سلسلة الأمن النووي رقم 17-T (التنقيح الأول) الصادرة عن الوكالة الدولية للطاقة الذرية

إرشادات تقنية

تقنيات الأمن الحاسوبي للمرافق النووية

IAEA
الوكالة الدولية للطاقة الذرية

سلسلة الأمن النووي الصادرة عن الوكالة

تعالج **سلسلة الأمن النووي الصادرة عن الوكالة** قضايا الأمن النووي المتعلقة بمنع وكشف الأفعال الإجرامية أو المتعمدة غير المأذون بها المنطوية على مواد نووية أو مواد مشعة أخرى أو ما يرتبط بذلك من مرافق أو أنشطة، أو المستهدفة لها، والتصدي لتلك الأفعال. وتتسق هذه المنشورات مع الصكوك الدولية المتعلقة بالأمن النووي، وتكمِّلها، مثل اتفاقية الحماية المادية للمواد النووية وتعديلها، والاتفاقية الدولية لقمع أعمال الإرهاب النووي، وقراري مجلس الأمن التابع للأمم المتحدة رقم 1373 و1540، ومدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها.

فئات سلسلة الأمن النووي الصادرة عن الوكالة

تصدر منشورات سلسلة الأمن النووي الصادرة عن الوكالة في الفئات التالية:

- **أساسيات الأمن النووي** التي تحدد هدف نظام أمن نووي لدولة ما والعناصر الأساسية لنظام من ذلك القبيل. وتوفر الأساس لتوصيات الأمن النووي.
- **توصيات الأمن النووي** التي تحدد التدابير التي ينبغي أن تتخذها الدول من أجل تحقيق وتعهّد نظام أمن نووي وطني فعّال يتّسق مع أساسيات الأمن النووي.
- **أدلة التنفيذ** التي تقدم إرشادات عن الوسائل التي يمكن للدول أن تنفذ من خلالها التدابير المحدّدة في توصيات الأمن النووي. وبهذا، تركِّز على كيفية العمل بالتوصيات المتعلقة بمجالات واسعة للأمن النووي.
- **الإرشادات التقنية** تقدّم إرشادات عن مواضيع تقنية محدّدة لاستكمال الإرشادات المحدّدة في أدلة التنفيذ. وهي تركِّز على تفاصيل كيفية تنفيذ التدابير الضرورية.

الصياغة والاستعراض

يشارك في إعداد منشورات سلسلة الأمن النووي واستعراضها أمانة الوكالة، وخبراء من الدول الأعضاء (الذين يساعدون الأمانة في صياغة المنشورات) ولجنة إرشادات الأمن النووي، التي تستعرض وتعتمد مسودّة المنشورات. وعند الاقتضاء، تُعقد أيضاً اجتماعات تقنية مفتوحة العضوية خلال عملية الصياغة من أجل إتاحة الفرصة للأخصائيين من الدول الأعضاء والمنظمات الدولية المعنية لاستعراض ومناقشة مسودّة النص. وإضافة إلى ذلك، ولضمان مستوى رفيع من الاستعراض وتوافق الآراء على الصعيد الدولي، تعرض الأمانة مسودّات النصوص على جميع الدول الأعضاء لفترة 120 يوماً لكي تستعرضها استعراضًا رسميًا.

وتُعِّد الأمانة لكل منشور الخطوات التالية، التي توافق عليها لجنة إرشادات الأمن النووي على مراحل متتالية ضمن عملية الإعداد والاستعراض:

- عرضًا وخطة عمل يصفان المنشور المتوخى الجديد أو المنقّح، وغرضه المستهدف ونطاقه ومحتواه؛
- مسودّة منشور لعرضها على الدول الأعضاء للتعليق عليها خلال فترة 120 يومًا الاستشارية؛
- صيغة نهائية لمسودّة المنشور مع مراعاة تعليقات الدول الأعضاء.

وتُراعى في عملية صياغة واستعراض المنشورات في سلسلة الأمن النووي الصادرة عن الوكالة اعتبارات السرية، ويسلم فيها بأن الأمن النووي يتصل اتصالاً متلازماً بشواغل الأمن الوطني العامة والمحددة.

وأحد الاعتبارات المستند إليها هو أن معايير أمان الوكالة وأنشطتها الرقابية ذات الصلة ينبغي أن توضع في الاعتبار في المضمون التقني للمنشورات. وعلى وجه التحديد، تقوم اللجان المعنية بمعايير الأمان ذات الصلة ولجنة إرشادات الأمن النووي باستعراض منشورات سلسلة الأمن النووي التي تعالج المجالات التي يوجد فيها ترابط مع الأمان المعروفة بوثائق الترابط ـ في كل مرحلة من المراحل المحدّدة أعلاه.

تقنيات الأمن الحاسوبي
للمرافق النووية

الدول الأعضاء في الوكالة الدولية للطاقة الذرية

الاتحاد الروسي
إثيوبيا
أذربيجان
الأرجنتين
الأردن
أرمينيا
إريتريا
إسبانيا
أستراليا
إستونيا
إسرائيل
إسواتيني
أفغانستان
إكوادور
ألبانيا
ألمانيا
الإمارات العربية المتحدة
أنتيغوا وبربودا
إندونيسيا
أنغولا
أوروغواي
أوزبكستان
أوغندا
أوكرانيا
إيران، (جمهورية – الإسلامية)
آيرلندا
آيسلندا
إيطاليا
بابوا غينيا الجديدة
باراغواي
باكستان
بالاو
البحرين
البرازيل
بربادوس
البرتغال
بروناي دار السلام
بلجيكا
بلغاريا
بليز
بنغلاديش
بنما
بنن
بوتسوانا
بوركينا فاسو
بوروندي

البوسنة والهرسك
بولندا
بوليفيا، (دولة - المتعددة القوميات)
بيرو
بيلاروس
تايلند
تركمانستان
تركيا
ترينيداد وتوباغو
تشاد
توغو
تونس
تونغا
جامايكا
الجبل الأسود
الجزائر
جزر البهاما
جزر القمر
جزر مارشال
جمهورية أفريقيا الوسطى
الجمهورية التشيكية
الجمهورية الدومينيكية
الجمهورية العربية السورية
جمهورية الكونغو الديمقراطية
جمهورية تنزانيا المتحدة
جمهورية كوريا
جمهورية لاو
الديمقراطية الشعبية
جمهورية مولدوفا
جنوب أفريقيا
جورجيا
جيبوتي
الدانمرك
دومينيكا
رواندا
رومانيا
زامبيا
زمبابوي
ساموا
سان مارينو
سانت فنسنت وجزر غرينادين
سانت كيتس ونيفس
سانت لوسيا
سري لانكا
السلفادور

سلوفاكيا
سلوفينيا
سنغافورة
السنغال
السودان
السويد
سويسرا
سيراليون
سيشيل
شيلي
صربيا
الصين
طاجيكستان
العراق
عُمان
غابون
غامبيا
غانا
غرينادا
غواتيمالا
غيانا
غينيا
فانواتو
فرنسا
الفلبين
فنزويلا، (جمهورية - البوليفارية)
فنلندا
فيجي
فييت نام
قبرص
قطر
قيرغيزستان
كابو فيردي
كازاخستان
الكاميرون
الكرسي الرسولي
كرواتيا
كمبوديا
كندا
كوبا
كوت ديفوار
كوستاريكا
كولومبيا
الكونغو
الكويت
كينيا

لاتفيا
لبنان
لختنشتاين
لكسمبورغ
ليبيا
ليبيريا
ليتوانيا
ليسوتو
مالطة
مالي
ماليزيا
مدغشقر
مصر
المغرب
مقدونيا الشمالية
المكسيك
ملاوي
المملكة العربية السعودية
المملكة المتحدة لبريطانيا العظمى وآيرلندا الشمالية
منغوليا
موريتانيا
موريشيوس
موزامبيق
موناكو
ميانمار
ناميبيا
النرويج
النمسا
نيبال
النيجر
نيجيريا
نيكاراغوا
نيوزيلندا
هايتي
الهند
هندوراس
هنغاريا
هولندا، (مملكة -)
الولايات المتحدة الأمريكية
اليابان
اليمن
اليونان

وافق المؤتمر المعني بالنظام الأساسي للوكالة الدولية للطاقة الذرية الذي عُقد في المقرِّ الرئيسي للأمم المتحدة في نيويورك، في 23 تشرين الأول/أكتوبر 1956، على النظام الأساسي للوكالة الذي بدأ نفاذه في 29 تموز/يوليه 1957. ويقع المقرُّ الرئيسي للوكالة في فيينا. ويتمثَّل هدف الوكالة الدولية للطاقة الذرية الرئيسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع"

العدد T-17 (التنقيح الأول) من سلسلة منشورات الأمن النووي الصادرة عن الوكالة

تقنيات الأمن الحاسوبي للمرافق النووية

إرشادات تقنية

الوكالة الدولية للطاقة الذرية
فيينا، 2024

ملاحظة بشأن حقوق النشر

طُبِع من قِبَل الوكالة الدولية للطاقة الذرية في النمسا

مايو 2024

STI/PUB/1921

ISBN 978-92-0-609923-0 (paperback : alk. paper) | ISBN 978-92-0-609323-8 (pdf) | ISBN 978-92-0-609423-5 (epub)

ISSN 2520-6923

تصدير

بقلم رافائيل ماريانو غروسي
المدير العام

توفِّر سلسلة الأمن النووي الصادرة عن الوكالة إرشادات قائمة على توافق الآراء الدولي بشأن جميع جوانب الأمن النووي من أجل دعم الدول الأعضاء في عملها الهادف إلى الوفاء بمسؤولياتها في مجال الأمن النووي. وتضع الوكالة هذه الإرشادات وتتعهدها كجزء من دورها المركزي المتمثّل في توفير الدعم والتنسيق على الصعيد الدولي فيما يتعلّق بالأمن النووي.

وأطلقت سلسلة الأمن النووي الصادرة عن الوكالة في عام 2006 وتقوم الوكالة بتحديثها تحديثاً مستمراً بالتعاون مع خبراء من الدول الأعضاء. وبصفتي المدير العام، ألتزم بكفالة أن تحافظ الوكالة على هذه المجموعة المتكاملة والشاملة والمتسقة من المنشورات الجيدة النوعية من إرشادات الأمن النووي المحدثّة والميسورة الاستخدام والملائمة للغرض، وأن تعمل على تحسينها. وينبغي أن يتيح التطبيق الصحيح لهذه الإرشادات في استخدام العلم والتكنولوجيا النوويين مستوى عاليا من الأمن النووي وأن يوفر الثقة اللازمة للسماح بالاستخدام المستمر للتكنولوجيا النووية لصالح الجميع.

والأمن النووي مسؤوليةٌ وطنية. وتكمل سلسلة الأمن النووي الصادرة عن الوكالة الصكوك القانونية الدولية المتعلقة بالأمن النووي، وهي بمثابة مرجع عالمي لمساعدة الأطراف على الوفاء بالتزاماتها. ومع أن إرشادات الأمن النووي ليست قانوناً ملزما للدول الأعضاء، فإنها تُطبّق على نطاق واسع. وقد أصبحت نقطة مرجعية وقاسما مشتركا لا غنىً عنهما بالنسبة للغالبية العظمى من الدول الأعضاء التي اعتمدت هذه الإرشادات لاستخدامها في اللوائح الوطنية لتعزيز الأمن النووي في توليد القوى النووية، ومفاعلات البحوث، ومرافق دورة الوقود، وكذلك في التطبيقات النووية في مجالات الطب، والصناعة، والزراعة، والبحوث.

وتستند الإرشادات الواردة في سلسلة الأمن النووي الصادرة عن الوكالة إلى الخبرة العملية للدول الأعضاء فيها، ويُتوصل إليها من خلال توافق الآراء الدولي. وتتسم مشاركة أعضاء لجنة إرشادات الأمن النووي وآخرين بأهمية خاصة، وأنا ممتن لجميع أولئك الذين يساهمون بمعرفتهم وخبراتهم في هذا المسعى.

وتستخدم الوكالة أيضا الإرشادات في سلسلة الأمن النووي الصادرة عن الوكالة عندما تقوم بمساعدة الدول الأعضاء من خلال بعثاتها الاستعراضية وخدماتها الاستشارية.

ويساعد ذلك الدول الأعضاء في تطبيق هذه الإرشادات ويتيح تقاسم الخبرات والرؤى والقيِّمة. وخلال التنقيح الدوري للإرشادات، تؤخذ في الحسبان التعقيبات الواردة من هذه البعثات والخدمات، والدروس المستخلصة من الأحداث والخبرات في استخدام إرشادات الأمن النووي وتطبيقها.

وأعتقد أن الإرشادات المقدمة في سلسلة الأمن النووي الصادرة عن الوكالة وتطبيقها يسهمان إسهاما قيما في ضمان مستوى عال من الأمن النووي في استخدام التكنولوجيا النووية. وأحث جميع الدول الأعضاء على تعزيز هذه الإرشادات وتطبيقها، وعلى العمل مع الوكالة من أجل المحافظة على جودتها، في الحاضر وفي المستقبل.

ملحوظة تحريرية

لا يتناول هذا التقرير مسائل تتعلق بالمسؤولية، قانونية كانت أم غير قانونية، عن أفعال أو الامتناع عن أفعال من جانب أي شخص.

والإرشادات الواردة في سلسلة الأمن النووي الصادرة عن الوكالة هي إرشادات غير مُلزمة للدول، ولكن يجوز أن تَستَخدِم الدول الإرشادات لكي تساعدها على الوفاء بالتزاماتها بمقتضى الصكوك القانونية الدولية وعلى الاضطلاع بمسؤولياتها المتصلة بالأمن النووي داخل الدولة. وتهدف الإرشادات المعبَّر عنها بجمل تبدأ بالفعل "ينبغي" إلى عرض الممارسات الدولية الجيدة والإشارة إلى إجماع دولي بأنَّ من الضروري أن تتخذ الدول الإجراءات الموصى بها أو ما يعادل ذلك من تدابير بديلة.

ويجب أن تُفهَم المصطلحات ذات الصلة بالأمن حسب تعريفها الوارد في المنشور الذي ترد فيه، أو في الإرشادات الأعلى درجة التي يدعمها المنشور. وفي غير ذلك من الحالات، فإنَّ الكلمات تُستَخدَم بمعانيها المتعارف عليها.

ويُعتبَر التذييل جزءًا لا يتجزأ من المنشور. ويكون للمواد الواردة في أي تذييل نفس صفة المتن. وتُستَخدم المرفقات لتوفير معلومات أو تفسيرات إضافية. ولا تُعتَبر المرفقات أجزاءً لا تتجزأ من النص الرئيسي.

وعلى الرغم من توخي قدر كبير من الحرص للحفاظ على دقة المعلومات الواردة في هذا المنشور، لا تتحمل الوكالة ولا دولها الأعضاء أي مسؤولية عن العواقب التي قد تنشأ عن استخدام تلك المعلومات.

واستخدام تسميات معيَّنة لبلدان أو أقاليم لا يعني ضمنًا إصدار أي حكم من جانب الناشر، أي الوكالة، بشأن الوضع القانوني لهذه البلدان أو الأقاليم أو سلطاتها ومؤسساتها أو تعيين حدودها.

وذكر أسماء شركاتٍ أو منتجاتٍ معيَّنة (سواء مع الإشارة إلى أنها مسجّلة أو دون تلك الإشارة) لا يعني ضمنًا وجود أي نية لانتهاك حقوق الملكية، كما لا ينبغي أن يُفسَّر على أنه تأييد أو توصية من جانب الوكالة.

المحتويات

1- مقدمة

الخلفية

1-1- يسعى الأمن النووي إلى منع الأعمال الإجرامية أو المتعمدة غير المأذون بها التي تنطوي على مواد نووية وغيرها من المواد المشعة والمرافق والأنشطة المرتبطة بها أو الموجهة ضدها، وإلى كشفها والتصدي لها. ويشمل الأمن النووي للمواد النووية والمرافق النووية الحماية المادية، والأمن المتصل بالموظفين (مثل تحديد الجدارة بالثقة، والتدابير المتخذة ضد التهديدات الداخلية) وأمن المعلومات.

1-2- وقد تستفيد الجماعات أو الأفراد الذين يخططون لعمل ضار ينطوي على مواد نووية أو مرفق نووي أو يرتكبون هذا العمل، من الوصول إلى المعلومات الحساسة والأصول المعلوماتية الحساسة المتعلقة بالمواد أو المرافق أو تدابير الأمن المطبقة.

1-3- وتؤكد أساسيات الأمن النووي [1] ومنشورات توصيات الأمن النووي [2–4] جميعها أهمية تأمين المعلومات الحساسة. ويُقدم العدد G-23 من سلسلة منشورات الأمن النووي الصادرة عن الوكالة، أمن المعلومات النووية [5]، إرشادات بشأن التدابير الملائمة لتحديد المعلومات الحساسة وتصنيفها وتأمينها من أجل تحقيق الأمن الفعال للمعلومات داخل منظومة الأمم النووي للدولة.

1-4- ويمكن أن تُساهم الهجمات على الفضاء الإلكتروني الموجهة ضد المرافق النووية في إحداث أضرار مادية بالمرفق و/أو تعطيل نُظمه الخاصة بالأمن أو الأمان (أي التخريب)، أو الحصول على معلومات نووية حساسة من دون إذن، أو إزالة المواد النووية من دون إذن. ولذلك فإن الأمن الحاسوبي أمر حيوي في المرافق النووي من أجل حماية الأمن النووي والأمان النووي على حد سواء.

1-5- ويوصى بحماية الأصول الرقمية الحساسة[1] في الفقرة 4-10 من المرجع [2]، التي

[1] الأصول الرقمية الحساسة هي أصول معلوماتية حساسة تُشكل نُظماً قائمة على الحاسوب (أو أجزاء من تلك من النُظم).

تنص على ما يلي:

"ينبغي أن تكون النُظم القائمة على الحاسوب والمستخدمة في الحماية المادية والأمان النووي وفي حصر المواد النووية ومراقبتها خاضعة للحماية من الضرر (كالهجمات الإلكترونية أو التلاعب أو التزوير) بما يتوافق مع تقييم التهديد أو التهديد المحتاط له في التصميم".

ويعترف المرجع [6] بالحاجة المحددة لحماية النُظم القائمة على الحاسوب من التهديدات الداخلية.

1-6- وترد إرشادات عامة بشأن الأمن الحاسوبي لأغراض الأمن النووي في العدد G-42 من سلسلة الأمن النووي الصادرة عن الوكالة، الأمن الحاسوبي لأغراض الأمن النووي [7]، وترد إرشادات أكثر تحديداً بشأن الأمن الحاسوبي لأغراض الأجهزة ونُظم التحكم في المرافق النووية في العدد T-33 من سلسلة الأمن النووي الصادرة عن الوكالة، الأمن الحاسوبي لنُظم الأجهزة والتحكم في المرافق النووية [8]. والغرض من هذا المنشور هو استكمال هذه الإرشادات بتقديم تفاصيل عن تقنيات الأمن الحاسوبي للنُظم الأخرى في المرافق النووية.

الهدف

1-7- الهدف من هذا المنشور هو مساعدة الدول الأعضاء على تطبيق الأمن الحاسوبي في المرافق النووية بهدف منع إزالة المواد النووية من دون إذن، وتخريب المواد النووية والوصول إلى المعلومات النووية الحساسة من دون إذن، والحماية من ذلك، ويعالج هذا المنشور الأمن الحاسوبي لدعم الأنشطة والمنظمات، مثل البائعين والمتعهدين والموردين. وبينما ينصب تركيز هذا المنشور على أمن المرافق النووية، فإن تطبيق هذه الإرشادات يمكن أن يكون مفيداً أيضاً للأمان والأداء التشغيلي في المرفق.

1-8- ويتناول هذا المنشور استخدام النهج القائم على إدراك المخاطر لوضع سياسات وبرامج وتدابير للأمن الحاسوبي وتعزيزها من أجل حماية الأصول الرقمية الحساسة وغيرها من الأصول الرقمية. ويعتمد المرفق النووي على الأصول الرقمية الحساسة وغيرها من الأصول الرقمية من أجل أمان المرفق وأمنه. ويصف هذا المنشور إدماج الأمن الحاسوبي في نظام إدارة المرفق أو تنظيمه، ويشمل إرشادات بشأن تحديد السياسات

والمتطلبات، وبشأن أنشطة وضع تدابير الأمن الحاسوبي التي تحمي المرفق من الهجمات على الفضاء الإلكتروني وتنفيذها والحفاظ على استدامتها وتعهدها وتقييمها وتحسينها باستمرار بما يتفق مع تقييم التهديدات أو التهديد المحتاط له في التصميم [9].

1-9- ويقدم هذا المنشور أيضاً إرشادات تقنية بشأن حماية الأصول الرقمية الأخرى في المرافق النووية.

1-10- ويوجه هذا المنشور إلى الهيئات الرقابية والسلطات المختصة الأخرى ومشغلي المرافق النووية والبائعين والمتعهدين والموردين.

النطاق

1-11- تنطبق الإرشادات الواردة في هذا المنشور على تنفيذ الأمن الحاسوبي لأغراض الأمن النووي في المرافق النووية وإدارته. وينطبق هذا المنشور على جميع مراحل عمر المرفق النووي [10].

1-12- والغرض من الأمن الحاسوبي في المرافق النووية هو حماية مجموعة من النُظم التي تُساهم في جوانب مختلفة من الأمن النووي، مثل الحماية المادية ونُظم حصر المواد النووية ومراقبتها. ولا يعالج هذا المنشور تصميم هذه النُظم ما لم يكن التصميم أو التشغيل متصلاً بحماية تلك النُظم من خلال تدابير الأمن الحاسوبي.

1-13- ويتناول هذا المنشور جميع الأصول الرقمية المرتبطة بالمرفق النووي، بما في ذلك نُظم الأجهزة والتحكم الخاصة بالمرفق. وترد في المرجع [8] إرشادات إضافية بشأن الاعتبارات الحاسوبية المحددة لنُظم الأجهزة والتحكم الخاصة بالمرفق التي توفِّر وظائف الأمان أو الأمن أو الوظائف المساعدة.

الهيكل

1-14- بعد هذه المقدمة، ترد في القسم 2 المصطلحات والمفاهيم الأساسية والعلاقات. ويصف القسم 3 الاعتبارات العامة للأمن الحاسوبي في المرافق النووية. ويقدم القسمان

4 و5 إرشادات بشأن إدارة مخاطر الأمن الحاسوبي في المرفق وعلى مستوى النُظم، على التوالي. ويُقدم القسم 6 إرشادات بشأن الاعتبارات المتعلقة بنظام إدارة مخاطر الأمن الحاسوبي للمرافق والنُظم ذات الصلة بمختلف المراحل في عمر المرفق. ويُقدم القسم 7 لمحة عامة عن برنامج للأمن الحاسوبي. ويُقدم القسم 8 مثالاً توضيحياً لتنفيذ بنية الأمن الحاسوبي الدفاعية وتدابير الأمن الحاسوبي المرتبطة بها.

1-15- ويُقدم التذييل إرشادات محددة بشأن مجموعة مختارة من عناصر برنامج الأمن الحاسوبي. ويقدم المرفق الأول أمثلة على سيناريوهات الهجمات التي يمكن استخدامها لتقييم الأمن الحاسوبي في المرافق النووية. ويقدم المرفق الثاني مثالاً على تخصيص مستويات الأمن الحاسوبي لمحطة قوى نووية. ويُقدم المرفق الثالث مثالاً على تطبيق مستويات ونطاقات الأمن الحاسوبي.

2- المفاهيم الأساسية والعلاقات

2-1- يوضح هذا القسم معنى المصطلحات المهمة المستخدمة في هذا المنشور.

الأمن النووي والأمن الحاسوبي

2-2- تنص أساسيات الأمن النووي [1] على أن الأهداف المتعلقة بالأمن النووي هي ما يلي:

> "المواد النووية، أو المواد المشعة الأخرى، أو المرافق ذات الصلة، أو الأنشطة ذات الصلة، أو المواقع أو الأشياء الأخرى التي يحتمل أن يستغلها تهديد الأمن النووي. وتشمل الأحداث العامة الرئيسية، والمواقع الاستراتيجية، والمعلومات الحساسة، وأصول المعلومات الحساسة".

وبالإضافة إلى المعلومات المخزّنة في الأصول الرقمية الحساسة، تشمل المعلومات الحساسة برامجيات على تلك الأصول الرقمية الحساسة، بما في ذلك برامجيات زمن

التشـغيل، والبرامـج الثابتـة المدمجـة، وأدوات التطويـر وأدوات الاختبـار، وبرامجيـات أدوات الصيانـة، ونُظـم التشـغيل.

2-3- وينـص المرجـع [1] علـى أن نظـام الأمـن النـووي هـو "مجموعـة متكاملـة مـن تدابيـر الأمـن النـووي". وفيمـا يلـي تعريـف تدابيـر الأمـن النـووي:

"تدابير يُقصد منها الحيلولة دون أن يؤدي تهديد الأمن النووي إلى إتمام أفعال إجرامية أو أفعال متعمدة غير مأذون بها تتعلق بمواد نووية، أو مواد مشعة أخرى، أو مرافق ذات صلة، أو أنشطة ذات صلة، أو أفعال موجهة نحو هذه المواد أو المرافق أو الأنشطة، أو يُقصد منها الكشف عن الأحداث المتصلة بالأمن النووي أو التصدي لها" [1].

2-4- وتنـص الإرشـادات العامـة بشـأن الأمـن الحاسـوبي [7] علـى أنـه: "ينبغـي أن تضـع الدولـة وتتعهـد اسـتراتيجية وطنيـة للأمـن الحاسـوبي فـي إطـار منظومـة الأمـن النـووي الخاصة بهـا". وبالنظـر إلـى أن المرافـق النوويـة تدخـل ضمـن نطـاق منظومـة الأمـن النـووي، ينبغـي أن يُـدرج الأمـن الحاسـوبي لهـذه المرافـق فـي تلـك الاسـتراتيجية الوطنيـة المتعلقـة بالأمـن الحاسـوبي. ويتعيّـن حمايـة وظائـف المرفـق التـي تدعـم الأمـان والأمـن مـن الخصـوم. وعندمـا تسـتخدم وظائـف المرفـق هـذه التقنيـات الرقميـة أو تعتمـد عليهـا أو تدعمهـا، فـإن الأمـن النـووي مطلـوب لحمايـة هـذه الوظائـف.

2-5- ويتعلـق الأمـن الحاسـوبي بالنُظـم القائمـة علـى الحاسـوب، ولا سـيما النُظـم التـي تـؤدي وظائـف المرافـق المهمـة أو المتصلـة بالأمـن النـووي والأمـان النـووي (أي الأصـول الرقميـة) أو تدعمهـا. ويوفِّـر الأمـن الحاسـوبي تقنيـات وأدوات للدفـاع ضـد الهجمـات علـى الفضـاء الإلكترونـي وضـد الإجـراءات أو أوجـه التقصيـر البشـرية التـي قـد تؤثـر علـى الأمـن.

وظائف المرفق ومستويات الأمن الحاسوبي ونطاقات الأمن الحاسوبي

2-6- يتمثـل النهـج المعتـاد المتبـع فـي حمايـة النُظـم بطريقـة منظمـة وفقـاً لنهـج متـدرج فـي اسـتخدام مفاهيـم مسـتويات الأمـن الحاسـوبي ونطاقـات الأمـن الحاسـوبي. ويعتمـد مسـتوى الأمـن الحاسـوبي المخصـص لمنطقـة أمـن حاسـوبي علـى أعلـى درجـة مـن الحمايـة الأمنيـة التـي تتطلبهـا أي وظيفـة يؤديهـا نظـام فـي المرفـق داخـل ذلـك النطـاق. ويُعيّـن نفـس مسـتوى الأمـن الحاسـوبي لجميـع النُظـم داخـل ذلـك النطـاق. وعـادة مـا يتكـون نمـوذج منطقـة المرفـق النـووي مـن العديـد مـن النطاقـات المختلفـة، ويمكـن أن يخصـص للعديـد

مـن النطاقـات مسـتوى الأمـن الحاسـوبي نفسـه.

2-7- وتُمثـل وظيفـة المرفـق مجموعـة منسـقة مـن الإجـراءات والعمليـات التـي يتعيّـن أداؤهـا فـي مرفـق نـووي. وتشـمل وظائـف المرفـق وظائـف مهمـة أو متصلـة بالأمـن النـووي ووظائـف مهمـة للأمـن النـووي أو مرتبطـة بـه ووظائـف مهمـة للأمـان النـووي أو مرتبطـة بـه (أي وظائـف الأمـان).[2] وتـوزّع وظائـف المرفـق بيـن النُظـم[3]، ويـؤدي كل منهـا واحـدة أو أكثـر مـن هـذه الوظائـف.

2-8- ويشـير مسـتوى الأمـن الحاسـوبي إلـى درجـة الحمايـة الأمنيـة المطلوبـة لوظيفـة فـي المرفـق وبالتالـي للنظـام الـذي يـؤدي تلـك الوظيفـة. ويرتبـط كل مسـتوى مـن مسـتويات الأمـن الحاسـوبي بمجموعـة مـن المتطلبـات التـي يفرضهـا المشـغِّل لضمـان توفيـر المسـتوى الملائـم مـن الحمايـة للأصـول الرقميـة المعيّنـة لذلـك المسـتوى باسـتخدام نهـج متـدرج. وسـيحتاج كل مسـتوى مـن مسـتويات الأمـن الحاسـوبي إلـى مجموعـات مختلفـة مـن تدابيـر الأمـن الحاسـوبي لتلبيـة متطلبـات الأمـن الحاسـوبي لذلـك المسـتوى.

2-9- ونطـاق الأمـن الحاسـوبي هـو مجموعـة منطقيـة و/أو ماديـة مـن الأصـول الرقميـة التـي تعيّـن لنفـس مسـتوى الأمـن الحاسـوبي وتكـون لهـا متطلبـات أمـن حاسـوبي مشـتركة بسـبب الخصائـص المتأصلـة فـي النُظـم أو ارتباطهـا بنُظـم أخـرى (ومعاييـر إضافيـة عنـد الضـرورة). ويهـدف اسـتخدام نطاقـات الأمـن الحاسـوبي إلـى تبسـيط إدارة تدابيـر الأمـن الحاسـوبي وتعميمهـا وتطبيقهـا[4].

2-10- ويمكن أن تشمل المعايير الإضافية لتحديد نطاقات الأمن الحاسوبي ما يلي:

(أ) المسـؤوليات التنظيميـة، مثـل نطاقـات الأمـن الحاسـوبي المختلفـة للنُظـم التـي تقـع المسـؤولية عنهـا علـى الإدارات المختلفـة؛
(ب) الحاجـة إلـى الحفـاظ علـى الفصـل، مثـل مناطـق أمـن حاسـوبي مختلفـة للنُظـم الاحتياطيـة علـى نفـس مسـتوى الأمـن الحاسـوبي الـذي يـؤدي وظيفـة المرفـق نفسـها؛

---

[2] تشمل وظائف المرفق أيضاً الوظائف التشغيلية والإدارية (أو التنظيمية).
[3] يمكن أن تكون النُظم داخل الموقع أو خارجه أو سحابية.
[4] يمكـن تطبيـق مفهـوم نطاقـات الأمـن الحاسـوبي علـى المرافـق القائمـة والمرافـق القديمـة وكذلـك علـى التصاميـم الجديـدة.

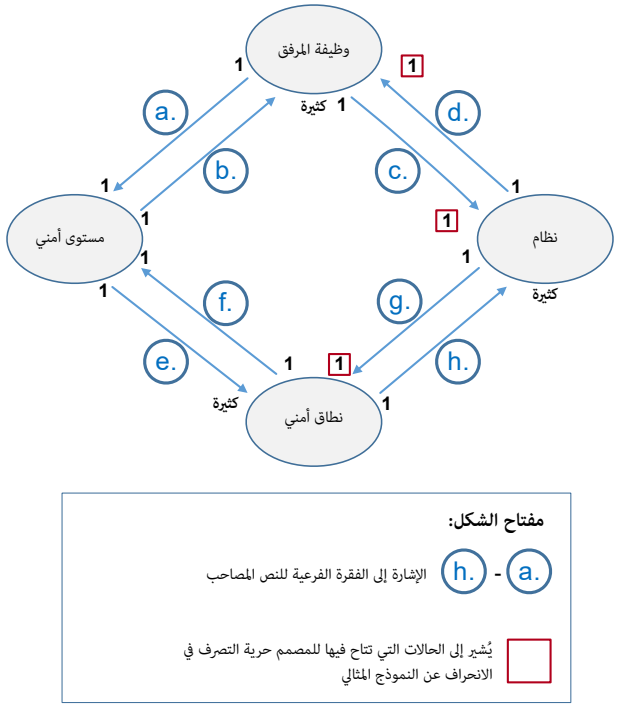
(ج) النطاقات المحددة بالفعل لأغراض أخرى، مثل نطاق الأمن الحاسوبي المحدد على سبيل التبسيط ليكون مماثلا للنطاق الذي أنشئ بالفعل لأغراض إدارية أو لأغراض الاتصال.

2-11- ويوضح الشكل - 1 العلاقات المثالية بين مفاهيم وظيفة (وظائف) المرفق، ومستوى (مستويات) الأمن الحاسوبي، والنظام (النُظم)، ونطاق (نطاقات) الأمن الحاسوبي.

2-12- يبين الشكل 1 كل علاقة من العلاقات المثالية، ويصف النص الوارد أدناه كل علاقة:

(أ) تُسند كل وظيفة من وظائف المرفق لمستوى أمن حاسوبي واحد.

(ب) يمكن تطبيق كل مستوى من مستويات الأمن الحاسوبي على واحد أو أكثر من وظائف المرفق.



الشكل -1- العلاقات المثالية بين وظيفة المرفق ومستوى الأمن الحاسوبي، والنظام ونطاق الأمن الحاسوبي

(ج) من المثالي تخصيص كل وظيفة من وظائف المرفق لنظام واحد، حيثما أمكن.[5]
(د) من المثالي أن يؤدي كل نظام وظيفة واحدة من وظائف المرفق، حيثما أمكن.[6]
(هـ) يمكن تطبيق كل مستوى من مستويات الأمن الحاسوبي على واحد أو أكثر من نطاقات الأمن.
(و) يعيَّن مستوى أمن حاسوبي واحد لكل نطاق من نطاقات الأمن الحاسوبي.
(ز) يوضع كل نظام داخل نطاق أمن حاسوبي واحد، حيثما أمكن.[7]
(ح) يمكن أن تتألف كل نطاق من نطاقات الأمن الحاسوبي من نظام واحد أو أكثر من نظام.

إدارة مخاطر الأمن الحاسوبي

2-13- يعالج نظام إدارة مخاطر الأمن الحاسوبي في المرفق (انظر القسم 4) وظائف المرفق، وهو الذي يحدد تخصيص هذه الوظائف لمستويات الأمن الحاسوبي ولنظام واحد أو لأكثر من نظام. وتنتقل إلى النُظم مستويات الأمن الحاسوبي المحددة للوظائف المخصصة لها.

2-14- ويُشكل نظام إدارة مخاطر الأمن الحاسوبي (انظر القسم 5) جزءاً من نظام إدارة الأمن الحاسوبي الخاص بالمرفق، ويعالج النُظم ويحدد (أ) حدود نطاقات الأمن الحاسوبي وفقاً لوظائف المرفق التي يؤديها والترابط بين النُظم وكذلك (ب) تدابير الأمن الحاسوبي التي سيجري تطبيقها لتلبية متطلبات مستوى الأمن الحاسوبي للنطاق.

2-15- وتعتمد مخرجات عمليات إدارة المخاطر في العادة على وضع السيناريوهات وتحليلها وفي بعض الحالات، على الأداء لزيادة الثقة في التقييمات النوعية. وهناك فئتان من السيناريوهات: وظيفية وتقنية. وتستخدم السيناريوهات الوظيفية بشكل عام

---

[5] وعلى سبيل المثال، قد تعيَّن وظيفة لنظامي إيقاف تشغيل مستقلين ومتنوعين.

[6] على سبيل المثال، العلاقة بين الإنسان والآلة. ومن المثالي، من منظور أمني، أن يؤدي نظام واحد وظيفة واحدة في المرفق، ولكن يمكن للمصممين تعيين أكثر من وظيفة من وظائف المرفق لنظام ما إذا كانوا يرون أن ذلك ضرورياً لدعم الأداء البشري أو التشغيلي أو أداء الأمان.

[7] من المثالي، من منظور أمني، أن يؤدي كل وظيفة من وظائف المرفق نظام واحد داخل نطاق أمن حاسوبي واحدة، ومن ثم يعيَّن له مستوى أمني واحد، ولكن المصممين قد يحيدون عن المستوى المثالي لاعتبارات أخرى، مثل نُظم الحماية من الحرائق أو نُظم الحماية المادية التي تغطي المرفق بأكمله (أو التي تغطي جزءاً كبيراً منه) وبالتالي يمكن أن تمر عبر مناطق مادية تحتوي على نطاقات معيّنة لمستويات أمنية مختلفة.

فـي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق، وتُسـتخدم السـيناريوهات التقنيـة فـي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للنظـم.

الطلبات المتزاحمة على البساطة والكفاءة والأمن الحاسوبي

2-16- يتعيّـن تحقيـق تـوازن بيـن الطلبـات المتزاحمـة علـى البسـاطة والكفـاءة والأمـن الحاسـوبي عنـد النظـر فـي الآتـي:

(أ) تحديد وظائف المرفق ووضع قائمة بها؛
(ب) تخصيص وظائف المرفق للنُظم؛
(ج) تطوير النُظم؛
(د) تحديـد متطلبـات الأمـن الحاسـوبي لمختلـف مسـتويات الأمـن الحاسـوبي علـى أسـاس نهـج متـدرج؛
(هـ) وضع حدود منطقية و/أو مادية لنطاقات الأمن الحاسوبي.

2-17- ويمكـن أن تـؤدي اعتبـارات البسـاطة إلـى تفضيـل تخصيـص وظيفـة واحـدة لنظـام واحـد. ويمكـن أن يسـفر ذلـك عـن بنيـة أمـن حاسـوبي دفاعيـة تسـمح بتكييـف تدابيـر الأمـن الحاسـوبي الفعالـة داخـل كل نطـاق لـكل وظيفـة مـن وظائـف المرفـق (بافتـراض وجـود علاقـة تناظريـة أُحاديـة بيـن النُظـم والوظائـف). ومـع ذلـك، سـتحتاج النُظـم إلـى ترابـط بينـي للتمكيـن مـن تحقيـق التكامـل بيـن الوظائـف المنفصلـة فـي المرفـق، وبالتالـي فـإن نظـام مسـتويات الأمـن الحاسـوبي ونطاقـات الأمـن الحاسـوبي قـد يصبـح أكثـر تعقيـداً بسـبب ازديـاد عـدد نطاقـات الأمـن الحاسـوبي والترابـط بيـن هـذه النطاقـات.

2-18- غيـر أن اعتبـارات الكفـاءة فـي أداء النُظـم لوظائـف المرفـق قـد تـؤدي إلـى تفضيـل تخصيـص وظائـف متعـددة لنظـام متكامـل واحـد. وفـي حيـن أن ذلـك قـد يسـفر عـن عـدد أقـل مـن نطاقـات الأمـن الحاسـوبي، قـد يـزداد تعقـد النظـام، ممـا يجعـل مـن الصعـب تطبيـق تدابيـر الأمـن الحاسـوبي الفعالـة فـي جميـع هـذه النطاقـات. وبالإضافـة إلـى ذلـك قـد يـزداد تراجـع الكفـاءة عندمـا يُحـدد لنطـاق الأمـن الحاسـوبي مسـتوى أمـن حاسـوبي مناسـب لأهـم وظيفـة فـي النظـام، إذ قـد يُطبـق مسـتوى حمايـة أعلـى مـن الـلازم علـى الوظائـف الأقـل أهميـة التـي تُشـكل جـزءاً مـن النظـام.

2-19- ويمكـن أن يشـمل أيضـاً التـوازن بيـن الكفـاءة والبسـاطة موازنـة أداء وظائـف المرفـق

مـن خـلال النُظـم حيـث تُسـند النُظـم إلـى نطاقـات الأمـن الحاسـوبي ومسـتويات الأمـن الحاسـوبي. ولذلـك، تشـمل إدارة مخاطـر الأمـن الحاسـوبي فـي العـادة عـدداً مـن الجـولات المتكـررة التـي تُحـدد فيهـا نطاقـات الأمـن الحاسـوبي وتدابيـر الأمـن الحاسـوبي المرتبطـة بهـا لإيجـاد التـوازن الأمثـل بيـن البسـاطة والكفـاءة. وسـتحتاج الجـولات المتكـررة إلـى إظهـار أن التعديـلات المقترحـة لتعاريـف نطاقـات الأمـن الحاسـوبي لـن تسـمح بالمسـاس بوظائـف المرفـق التـي مـن شـأنها أن تـؤدي إلـى عواقـب أسـوأ.

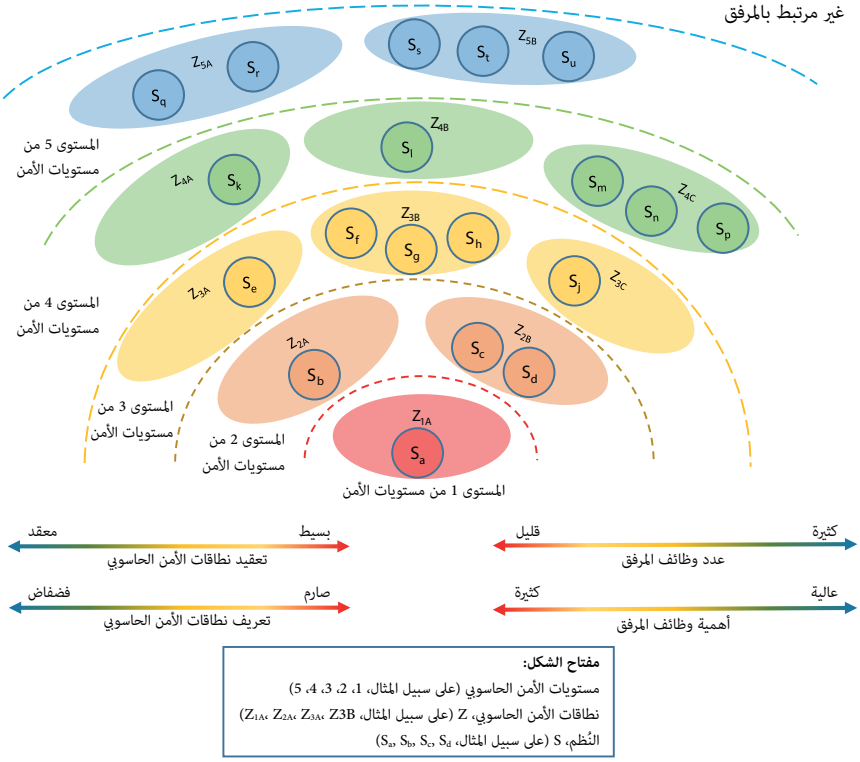
النموذج المفاهيمي لمناطق المرفق النووي

2-20- يبيـن الشـكل 2 مثـالاً علـى نمـوذج مفاهيمـي لنطاقـات مرفـق نـووي يتسـم بالخصائـص التاليـة:

(أ) يرتبـط المرفـق الـوارد فـي المثـال بعواقـب وخيمـة فـي حالـة إزالـة المـواد مـن دون إذن أو التخريـب.
(ب) يقتصـر عـدد مسـتويات الأمـن الحاسـوبي علـى خمسـة مسـتويات، يشـمل فيهـا المسـتوى 1 أكثـر متطلبـات الحمايـة صرامـة، ويشـمل المسـتوى 5 المتطلبـات الأقـل صرامـة.
(ج) يوضع كل نظام داخل نطاق أمن حاسوبي.
(د) يخصص لكل نطاق (بما في ذلك نُظمه) مستوى أمن حاسوبي.
(هـ) قد يخصص مستوى أمن حاسوبي لنطاق واحد أو أكثر من نطاق.

2-21- يوضـح الشـكل 2 التطبيـق المفاهيمـي للنُظـم ومسـتويات الأمـن الحاسـوبي ونطاقـات الأمـن الحاسـوبي. وفيمـا يلـي أثـر مسـتوى الأمـن الحاسـوبي المحـدد علـى متطلبـات وظائـف المرفـق ونظمـه ونطاقـات أمنـه الحاسـوبي:

(أ) يلـزم فـي العـادة مسـتويات أمـن حاسـوبي أعلـى (أكثـر صرامـة) للوظائـف الأقـل (وتُطبـق بالتالـي علـى نُظـم أقـل) مقارنـة بمسـتويات الأمـن الدنيـا. وفـي الشـكل 2، ينطبـق المسـتوى 1 مـن مسـتويات الأمـن علـى المجموعـة الدنيـا مـن الوظائـف الحاسـمة الأهميـة التـي مـن المثالـي تخصيصهـا لنظـام واحـد، فـي حيـن أن مسـتوى المسـتوى 5 مـن مسـتويات الأمـن يتيـح تخصيـص وظائـف كثيـرة لنظـام واحـد.
(ب) تكـون مسـتويات الأمـن الحاسـوبي الأعلـى (الأكثـر صرامـة) بصفـة عامـة أكثـر بسـاطة (أي أقـل تعقيـداً) مـن المسـتويات الدنيـا. وفـي الشـكل 2، يحتـوي النطـاق Z_{1A} علـى نظـام



الشكل -2- نموذج مفاهيمي لمستويات الأمن الحاسوبي ونطاقاته

قطعي واحد تُخفَّض تفاعلاته المنطقية والمادية مع النطاقات (والنُظم) الأخرى إلى أدنى حد قدر المستطاع، في حين أن النطاق Z_{5B} لا يُفرض على تفاعلاته مع النطاقات (والنُظم) الأخرى سوى قليل جداً من القيود.

(ج) يرتبط تعقد النطاقات في العادة بحجمها المادي والمنطقي. ومن ذلك على سبيل المثال أن من المحتمل، في النطاق Z_{1A}، أن تقتصر المواقع المادية للأصول الرقمية الحساسة على منطقة حيوية، وأما في النطاق Z_{3C}، فإن أي أصول رقمية قد تكون في أي مكان داخل المنطقة المحمية. ومن المحتمل أن تؤدي الزيادة في المساحة المادية من المنطقة الحيوية (Z_{1A}) إلى المنطقة المحمية (Z_{3C}) إلى زيادة عدد نقاط الوصول وعدد الأشخاص المأذون لهم الذين يحتاجون إلى الوصول، ويمكنهم بالتالي التفاعل مع الأصول الرقمية.

(د) يمكن التعبير عن الحجم المنطقي للنطاق باعتباره عدد الأصول الرقمية المثبتة القابلة للعنونة داخل نظام ما. وعلى سبيل المثال، قد يُحدد المدى المنطقي

للنطـاق Z_{3A} بحيـث يحتـوي علـى عـدد أصغـر مـن العناويـن القابلـة للإسـناد لسـعة محـدودة مـن الأصـول الرقميـة، فـي حيـن أن النطـاق Z_{5A} قـد يكـون لـه مـدى أوسـع ويشـمل عـدداً أكبـر مـن العناويـن المنطقيـة المتاحـة للأصـول الرقميـة الآن وفـي المسـتقبل.

(هـ) فـي هـذه الأمثلـة، يـزداد عـدد الأصـول الرقميـة المحتملـة القابلـة للعنونـة بطريقـة مماثلة لمـا فـي مثـال حجـم المنطقـة الماديـة فـي الفقـرة 2-21 (ج). ومـع ذلـك، يؤثـر تركيـب الأصـول الرقميـة الإضافيـة تأثيـراً كبيـراً علـى حجـم المنطقـة المنطقيـة ولكـن ليـس علـى حجـم المنطقـة الماديـة.[8] ويعنـي ذلـك أن عـدد التفاعـلات المنطقيـة المحتملـة لا يـزداد إلاّ عندمـا تُركـب أصـول رقميـة إضافيـة داخـل منطقـة مـا ويـزداد بالتالـي عـدد هـذه التفاعـلات وتعقدهـا داخـل المنطقـة وداخـل حدودهـا.

2-22- وقـد تعتمـد الدقـة التـي تُحـدد بهـا نطاقـات الأمـن الحاسـوبي علـى مسـتويات الأمـن المعيّنـة لهـذه النطاقـات. وعلـى سـبيل المثـال، فيمـا يتعلـق بالنطـاق Z_{1A}، تُحـدد الحـدود الماديـة والمنطقيـة تحديـداً دقيقـاً، فـي حيـن أن النطـاق Z_{5A} قـد تحتـاج فقـط إلـى تحديـد صـارم للحـدود المنطقيـة، وقـد تكـون الحـدود الماديـة فضفاضـة بدرجـة أكبـر (علـى سـبيل المثـال، داخـل مركـز بيانـات أو خدمـة سـحابية أو مكتـب شـركة).

2-23- ويمكـن أن تكـون حـدود النظـام (النطـاق والماديـة) مفيـدة فـي تحديـد حـدود نطـاق الأمـن الحاسـوبي. وفـي الممارسـة العمليـة، قـد تشـمل المنطقـة نظامـاً واحـداً أو أكثـر مـن نظـام، ويتألـف كل نظـام أو يدعمـه واحـد أو أكثـر مـن الأصـول الرقميـة لأداء وظيفـة المرفـق المعيّنـة أو دعمهـا.[9]

2-24- وتحتـوي حـدود نطـاق الأمـن الحاسـوبي بصفـة عامـة علـى تحكـم مـادي فـي الوصـول (مثـل الخزائـن المقفلـة، والحواجـز، وبرامجيـات تعطيـل المنافـذ)، وآليـات فصـل تدفـق البيانـات (علـى سـبيل المثـال)، مرشـحات الـرُزم، وجـدران الحمايـة، وصمامـات البيانـات) لمنـع الهجمـات علـى الفضـاء الإلكترونـي أو غيـر ذلـك مـن أشـكال الوصـول غيـر المـأذون بـه ولمنـع

[8] عـادة مـا يكـون الحجـم المـادي لمنطقـة حيويـة أكبـر بعـدة مـرات مـن حجـم الأصـول الرقميـة الموجـودة داخـل حدودهـا، وبالتالـي لا يُشـكل قيـداً علـى عـدد الأصـول الرقميـة التـي قـد تكـون موجـودة داخلهـا.

[9] قـد تتطلـب بعـض النُظـم التناظريـة التـي تـؤدي وظائـف المرفـق (انظـر الفقـرة 2-3) تعيينهـا لمسـتوى أمـن حاسـوبي ووضعهـا داخـل منطقـة أمـن حاسـوبي. ويُفتـرض أن النُظـم التناظريـة تدعمهـا أصـول رقميـة، علـى سـبيل المثـال، أداة رقميـة لمعايـرة النظـام التناظـري.

انتشار الأخطاء من نطاق إلى آخر (وخاصة من نطق ذي متطلبات حماية أقل صرامة إلى نطاق ذي متطلبات أكثر صرامة).

2-25- ويوفِّر نموذج النطاقات نهجاً متدرجاً ودفاعاً في العمق. وسيحتاج الهجوم على الفضاء الإلكتروني الذي ينشأ خارج المرفق إلى التغلب على عدة طبقات من تدابير الأمن الحاسوبي أو تجاوزها قبل أن تتاح له الفرصة للإخلال بنظام مزوَّد بمستوى الأمن الحاسوبي 1 أو 2 أو 3. ويمكن أن تُساهم تدابير المستويين 4 و5 من مستويات الأمن الحاسوبي أيضاً في حماية مستويات الحماية الأعلى.[10] وعلى سبيل المثال، يفيد توفير قدرات الكشف المبكر داخل النطاقات المعيّنة للمستوى 4 أو 5 من مستويات الأمن في إتاحة الفرصة لاحتواء الهجوم على الفضاء الإلكتروني والتخفيف من حدته قبل أن يكون له أي أثر على الأُصول الرقمية الحساسة في المستويات 1 أو 2 أو 3.

تدابير الأمن الحاسوبي

2-26- في النهج المتدرج، تتناسب قوة تدابير الأمن الحاسوبي الموضوعة لحماية وظيفة المرفق تناسباً مباشراً مع العواقب الأسوأ المحتملة لتعرض وظيفة المرفق للخطر.

2-27- وتُستخدم تدابير الأمن الحاسوبي لما يلي:

(أ) منع الأعمال الإجرامية أو الأعمال المتعمدة غير المأذون بها الأخرى وكشفها وعرقلتها والتصدي لها؛
(ب) التخفيف من عواقب هذه الأعمال؛
(ج) التعافي من عواقب هذه الأعمال.

2-28- ويمكن أيضاً استخدام تدابير الأمن الحاسوبي لما يلي:

(أ) تقليل تأثر الأصول الرقمية بالأفعال الضارة؛

[10] قد تكون بعض المناطق الواردة في الشكل 2 معزولة من دون اتصال دائم بالشبكة. ومع ذلك، سيكون لمثل هذه المناطق التي تحتوي على أصول رقمية في جميع الحالات شكل ما من التبعية المعلوماتية المتقطعة - على سبيل المثال، التحديثات باستخدام قرص مدمج أو ناقل تسلسلي عام - وهو ما يمثل فرصة للخصم.

(ب) منع الأعمال غير الضارة من إضعاف الأمن النووي.

2-29- ويمكن تخصيص تدابير الأمن الحاسوبي لواحدة من ثلاث فئات: تدابير التحكم التقني؛ أو تدابير التحكم المادي، أو تدابير التحكم الإداري (انظر المرجع [7]).

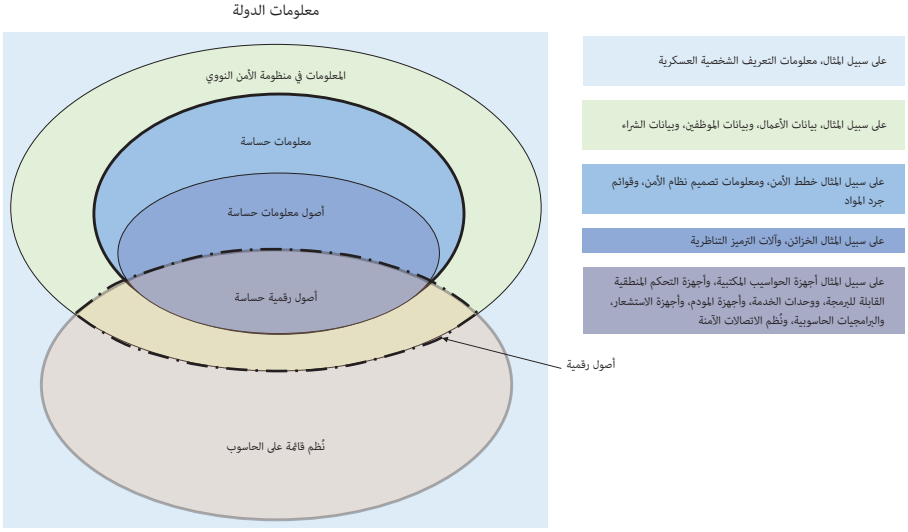
2-30- وقد تُساهم تدابير الأمن الحاسوبي أيضاً في اتخاذ تدابير أخرى للحماية المادية وللأمن المتصل بالأفراد وأمن المعلومات أو قد تدعمها تلك التدابير. ويُقدم القسم 8 مثالاً على تطبيق تدابير الأمن الحاسوبي في إطار إدارة مخاطر الأمن الحاسوبي التي تشمل خمسة مستويات.

النُظم القائمة على الحاسوب والأصول الرقمية (بما فيها الأصول الرقمية الحساسة)

2-31- تستفيد النُظم القائمة على الحاسوب من التكنولوجيات الرقمية أو تعتمد عليها أو تدعمها تلك التكنولوجيات. وتؤدي النُظم القائمة على الحاسوب دوراً متزايداً باستمرار في أداء الوظائف المهمة للمرافق النووية والعمليات المرتبطة بها. وتُشكل النُظم القائمة على الحاسوب بصورة متزايدة جزءاً لا يتجزأ من التصاميم الجديدة، ويمكن إدخالها في المرافق القائمة أثناء التحديث أو لزيادة الإنتاجية أو العولية.

2-32- والنُظم القائمة على الحاسوب هي التكنولوجيات التي تُنشئ المعلومات الرقمية أو تتيح الوصول إليها أو تعالجها أو تحوسبها أو تنقلها أو تخزنها، أو التي تؤدي خدمات تنطوي على هذه المعلومات أو تقدم خدمات من هذا القبيل أو تتحكم فيها. ويمكن أن تكون هذه النُظم مادية أو افتراضية. وتشمل **هذه النُظم الحواسيب المكتبية والنقالة واللوحية وغيرها من الحواسيب الشخصية؛ والهواتف الذكية، والحواسيب الكبيرة؛ ووحدات الخدمة؛ والحواسيب الافتراضية؛ والتطبيقات البرامجية؛ وقواعد البيانات؛ ووسائط التخزين القابلة للنقل؛ ونظم الأجهزة والتحكم الرقمية؛ وأجهزة التحكم المنطقية القابلة للبرمجة، والطابعات، وأجهزة الشبكات، والمكونات والأجهزة المدمجة**. ويمكن برمجة بعض النُظم القائمة على الحاسوب، مما يوفِّر خيار تعديل خطوات المعالجة من دون تغيير الأجهزة. ويمكن أن تتعرض النُظم القائمة على الحاسوب لهجمات على الفضاء الإلكتروني.

2-33- وفي سياق هذا المنشور، يُشير مصطلح 'الأصول الرقمية' إلى نظام قائم على الحاسوب مرتبط بمرفق نووي. وسيعتبر أي أصل رقمي مهم لأمان المرفق النووي أو أمنه



الشكل -3- نُظم المعلومات والنُظم القائمة على الحاسوب في الدولة وفي منظومة الأمن النووي.

أصلاً رقمياً حساساً.[11]

2-34- ويتعلق الأمن الحاسوبي بحماية النُظم القائمة على الحاسوب من المساس بها.[12] ويمثل الأمن الحاسوبي مجموعة فرعية من أمن المعلومات (كما هو محدد، على سبيل المثال، في سلسلة المعايير الدولية ISO/IEC 27000 [11]) ويشترك في العديد من الأهداف والمنهجيات والمصطلحات نفسها. وتُعتبر مصطلحات مثل 'أمن تكنولوجيا المعلومات' و'أمن الفضاء الإلكتروني' مترادفة مع 'الأمن الحاسوبي'، ولا تُستخدم في هذا المنشور.

2-35- ويبين الشكل 3 العلاقة بين أمن المعلومات، والمعلومات الحساسة، وأصول المعلومات الحساسة، والأصول الرقمية، والأصول الرقمية الحساسة.

[11] تستخدم بعض الدول الأعضاء تسميات مماثلة للأصول الرقمية الحساسة، مثل 'الأصول الرقمية الحرجة'، أو أصول الفضاء الإلكتروني الأساسية'. وهذه المصطلحات قد لا تكون مرادفة بصورة مباشرة للأصول الرقمية الحساسة.

[12] تعتبر مصطلحات مثل "أمن تكنولوجيا المعلومات" و "أمن الفضاء الإلكتروني" مرادفات لمصطلح "الأمن الحاسوبي" ولا تستخدم في هذا المنشور.

الهجوم على الفضاء الإلكتروني

2-36- الهجوم على الفضاء الإلكتروني هو عمل ضار بقصد سرقة هدف محدد أو تغييره أو منع الوصول إليه أو تدميره من خلال الوصول من دون إذن إلى (أو من خلال إجراءات داخل) نظام قابل للتأثر [8] ويمكن تنفيذ هجوم على الفضاء الإلكتروني من جانب أفراد أو مؤسسات، ويمكن أن يستهدف معلومات حساسة أو أصول معلومات حساسة. وتتميَّز الهجمات على الفضاء الإلكتروني بالخصائص الخاصة التالية:

(أ) يمكن أن تكون مخفية.
(ب) يمكن تأخير تنفيذها أو يمكن أن تكون معتمدة على الحالة أو يمكن الشروع فيها عن بُعد.
(ج) يمكن خداع الموظفين (مثل المهندسين والحراس وموظفي العمليات والصيانة والمتعهدين) لدعم الهجوم عن غير قصد.

2-37- وقد يوفِّر المساس بالأصول الرقمية مسارات للهجمات على الفضاء الإلكتروني التي تستهدف الأصول الرقمية الحساسة أو يُسهلها أو يُساعد فيها، مع ما يترتب على ذلك من أثر سلبي على الأمن النووي والأمان النووي. ولذلك، من الضروري توفير حماية مناسبة - بالاستناد إلى نهج متدرج ودفاع في العمق - لجميع الأصول الرقمية المرتبطة بالمرفق من أجل منع استخدامها في المساس بالأصول الرقمية الحساسة. ومن شأن المساس بالأصول الرقمية الحساسة أن يؤدي إلى إضعاف الأمن النووي، وقد يسفر عن حدث متصل بالأمن بالنووي[13] تنشأ عنه عواقب عواقب تتراوح في شدتها (من الأفضل إلى الأسوأ) على النحو التالي:

(أ) من دون أي عواقب؛
(ب) عواقب لا تكاد تُذكر؛
(ج) عواقب محدودة (بما في ذلك العواقب التي تؤثر على الأمان، مثل واقعة تشغيلية متوقعة، وتأثيرات تشغيلية، مثل أداء المحطة)؛
(د) عواقب معتدلة (على سبيل المثال، تدهور القدرة على منع أحداث الأمن النووي وكشفها والتصدي لها)؛
(هـ) عواقب كبيرة (مثل إفشاء معلومات حساسة من دون إذن أو فقدانها)؛

[13] يمكن أن يكون لأحداث الأمن النووي عواقب تؤثر على الأمن النووي أو الأمان النووي أو كليهما.

(و) عواقب وخيمة (مثل العواقب الإشعاعية غير المقبولة الناجمة عن التخريب أو إزالة مواد نووية أو مواد مشعة أخرى من دون إذن).

2-38- وقد تشمل قدرات الخصوم المحتملين فعالية استخدام الهجمات على الفضاء الإلكتروني. ولذلك فإن الأصول الرقمية الحساسة تكون أهدافاً نظراً لما لها من تأثير على وظائف المرفق وباعتبارها وسيلة يستخدمها الخصوم لتسهيل وتحقيق أهدافهم، وقد تكون مستهدفة تحديداً.

الترابط مع الأمان

2-39- تُعرَّف وظيفة الأمان بأنها "غرض محدد يجب تحقيقه من أجل الأمان" [12]. وتُعد وظائف الأمان ضرورية "لكي يمنع المرفق أو النشاط أو يُخفف من العواقب الإشعاعية للتشغيل العادي والوقائع التشغيلية المتوقعة وظروف الحوادث" [12].

2-40- وعلى سبيل المثال، فيما يلي وظائف الأمان الأساسية المطلوبة لجميع حالات المحطة (المتطلب 4 من العدد SSR-2/1 (الصيغة المنقحة Rev. 1) من سلسلة معايير الأمان الصادرة عن الوكالة، أمان محطات القوى النووية: التصميم [13]):

(أ) السيطرة على التفاعلية؛
(ب) إزالة الحرارة من المفاعل ومن مخزن الوقود؛
(ج) حجز المواد المشعة، والتدريع ضد الإشعاع ومراقبة الانبعاثات المشعة المخطط لها، فضلاً عن الحد من الانبعاثات المشعة العرضية.

2-41- وتُحدد الفقرة 3-46 من المرجع [2] وظائف الحماية المادية بأنها الكشف والعرقلة والتصدي. وتستخدم وظائف الحماية المادية الدفاع في العمق وتُطبق نهجاً متدرجاً لتوفير الحماية الفعالة المناسبة.

2-42- ولا ترتبط وظائف الحماية المادية ووظائف الأمان بالضرورة ببعضها البعض، مما يجعل من الصعب معالجة وظائف الأمان ووظائف الحماية المادية بصورة متسقة في منهجيات تقييم المخاطر. ولذلك فإن وصف وتخصيص وظائف المرفق المهمة أو المرتبطة بالأمن على نحو يماثل وظائف المرفق المهمة أو المرتبطة بالأمان (أي وظائف

الأمـان) سيُبسـط تحديـد أهميـة وظائـف المرفـق وسـيُمكِّن مـن معاملـة وظائـف الأمـان ووظائـف الأمـن المتماثلـة الأهميـة علـى قـدم المسـاواة. وفيمـا يلـي بعـض الأمثلـة علـى وظائـف المرفـق المهمـة للأمـن:

(أ) كشف الاقتحام (بما في ذلك تقييمه) في نقطة الكشف الحرجة؛
(ب) مراقبة وصول الأشخاص والمعدات إلى المواد من الفئة الأولى أو المناطق الحيوية؛
(ج) الاتصالات لتنسيق قوات التصدي أثناء أحداث الأمن النووي.

3- اعتبارات عامة بشأن الأمن الحاسوبي

تحديد وظائف المرفق

3-1- ينص المرجع [7] على ما يلي:

> "ينبغي أن تكون الخطوة الأولى في العملية المنهجية المذكورة [لتطبيق تدابير الأمن الحاسوبي لأغراض الأمن النووي] هي تحديد الوظائف التي توفِّر دعماً مباشراً لجانب واحد أو أكثر من جوانب الأمن النووي (مثل الحماية المادية، وحصر المواد النووية ومراقبتها، وإدارة المعلومات الحساسة) والأمان النووي. وبعد ذلك ينبغي تحديد ما يدعم هذه الوظائف من النُظم الحاسوبية والأصول الرقمية المكونة لها [أي الأصول الرقمية]".

والأصـول الرقميـة فـي المرفـق النـووي هـي النُظـم القائمـة علـى الحاسـوب التـي تحتـاج إلـى حمايـة مـن المسـاس بهـا، علـى النحـو الموصـى بـه فـي الفقـرة 4-10 مـن المرجـع [2]، والأصـول الرقميـة الحساسـة التـي يتناولهـا هـذا المنشـور.

3-2- وينبغـي أن يُحـدد المشـغِّل وظائـف المرفـق بأكملـه ويضـع قائمـة بهـا علـى نحـو متسـق لضمـان إمكانيـة تقييـم المجموعـة المحـددة مـن وظائـف المرفـق بصـورة شـاملة.

وينبغـي أن يقـدم المشـغِّل قائمـة بوظائـف المرفـق المحـددة إلـى السـلطة المختصـة[14] بمـا يتسـق مـع اللوائـح الوطنيـة. وينبغـي النظـر فـي متطلبـات الأمـن الحاسـوبي[15] لهـذه الوظائـف الخاصـة بالمرفـق، أيـاً كانـت وسـيلة أداء الوظائـف (علـى سـبيل المثـال، التكنولوجيـا المحـددة المسـتخدمة، سـواء كانـت تناظريـة أو رقميـة).

3-3- وسـيكون أداء وظائـف المرفـق معتمـداً علـى المعلومـات الحساسـة ذات الصلـة وأصـول المعلومـات الحساسـة والأصـول الرقميـة الأخـرى المرتبطـة بهـا أو سـيكون مدعومـاً بهـا.

حماية المعلومات الحساسة والأصول الرقمية

4-3- ينبغـي أن يطبـق المشـغِّل تدابيـر الأمـن الحاسـوبي لضمـان الحمايـة المناسـبة (بمـا فـي ذلـك الاقتفائيـة) للمعلومـات الحساسـة وأصـول المعلومـات الحساسـة والأصـول الرقميـة الحساسـة. ويتحقـق الأمـن الحاسـوبي مـن خـلال تدابيـر لضمـان السـرية والنزاهـة والتوافـر، وكذلـك لتلبيـة أي متطلبـات أخـرى تُحددهـا السـلطة المختصـة.

5-3- وينبغـي أن يحـدد المشـغِّل المعلومـات الحساسـة، مـع مراعـاة تأثيـرات المسـاس بهـا، ومتطلبـات الدولـة فيمـا يتعلـق بأمـن المعلومـات الحساسـة. ويوفِّـر المرجـع [5] إرشـادات مفصلـة لوضـع متطلبـات الدولـة بشـأن المعلومـات الحساسـة.

6-3- ويمكـن تحديـد المعلومـات الحساسـة مباشـرة مـن خـلال النظـر فـي العواقـب المحتملة المرتبطـة بالإفشـاء مـن دون إذن (كمـا هـو موضـح فـي المرجـع [5])، علـى سـبيل المثـال، لمعلومـات متعلقـة بالترتيبـات الأمنيـة، وهـي معلومـات يمكـن أن يسـتخدمها الخصـوم فـي التخطيـط لعمـل ضـار. وعـادة مـا تكـون السـرية هـي السـمة الأشـد احتياجـاً إلـى الحمايـة فـي حالـة هـذا النـوع مـن المعلومـات. ويمكـن أيضـاً تحديـد المعلومـات الحساسـة بطريقـة غيـر مباشـرة مـن خـلال النظـر فـي مغزاهـا الوظيفـي (أي أهميتهـا لتوفيـر وظيفـة للمرفـق أو

---

[14] تعنـي 'السـلطة المختصـة' فـي هـذا المنشـور السـلطة التـي تكلفهـا الدولـة بالمسـؤولية عـن الأمـن الحاسـوبي فـي سـياق الأمـن النـووي. وهـذه السـلطة يمكـن أن تكـون السـلطة المختصـة بالأمـن النـووي أو السـلطة المختصـة بالأمـن الحاسـوبي.

[15] تشـمل متطلبـات الأمـن الحاسـوبي فـي هـذا المنشـور متطلبـات مكتوبـة تفرضهـا السـلطة المختصـة ذات الصلـة أو يفرضهـا المشـغِّل للامتثـال لمتطلبـات الأمـن الحاسـوبي التـي تحددهـا السـلطة المختصـة أو للمتطلبـات الرقابيـة.

أداء هـذه الوظيفـة)، علـى سـبيل المثـال، البيانـات الدقيقـة والمناسـبة التوقيـت عـن ضغـط المرجـل، التـي قـد يسـتغلها الخصـم علـى الأرجـح عـن طريـق التعديـل أو التدميـر. وفـي هـذا النـوع مـن المعلومـات، قـد تكـون سـلامة المعلومـات وتوافرهـا علـى الأقـل بنفـس أهميـة السـرية.

3-7- ويمكـن تصنيـف المعلومـات المتضمنـة فـي خطـة أمـن الموقـع إلـى معلومـات حساسـة، ويمكـن تنفيـذ تدابيـر لحمايـة سـريتها لمـدة زمنيـة ممتـدة، نظـراً لأن المعلومـات سـتظل حساسـة طـوال الفتـرة التـي تسـري عليهـا خطـة أمـن الموقـع.

3-8- وفيمـا يتعلـق بنظـام الأجهـزة والتحكـم وبيانـات عملياتـه، قـد يُعطـي المشـغِّل الأولويـة لهـذه التدابيـر التـي تضمـن توافـر النظـام وسـلامته علـى التدابيـر التـي تضمـن السـرية. وفـي هـذه الحالـة، تكـون بيانـات العمليـات مهمـة لسـلامة أداء الوظيفـة وتوافرهـا، ولا تكـون حساسـة إلاّ خـلال الفتـرات الزمنيـة الفاصلـة المحـدودة جـداً التـي يقـوم فيهـا نظـام الأجهـزة والتحكـم بتنفيـذ إجـراء متعلـق بالتحكـم بنـاءً علـى البيانـات. ومـع ذلـك، حالمـا تصبـح بيانـات العمليـات غيـر مهمـة لأداء الوظيفـة وتوافرهـا (أي لـم يعـد مـن الممكـن أن تُشـكل أساسـاً للإجـراء المتعلـق بالتحكـم)، لا يكـون لبيانـات العمليـات التاريخيـة أي قيمـة إلّا بنـاءً علـى حساسـيتها. ولذلـك، ينبغـي الموازنـة بيـن الفائـدة الأمنيـة الناشـئة عـن زيـادة ضمـان السـرية (لحمايـة حساسـية المعلومـات) والفائـدة الأمنيـة الناشـئة عـن حمايـة السـلامة والتوافـر.

3-9- وفـي حيـن أن حمايـة سـرية بيانـات العمليـات المتولـدة مـن هـذه النُظـم قـد لا تحتـاج إلـى تدابيـر صارمـة، فـإن فقـدان سـرية البيانـات الأخـرى المتعلقـة بالنُظـم، مثـل كلمـات مـرور الإدارة ورمـز المصـدر والتفاصيـل الرئيسـية الأخـرى، سـيوفِّر للخصـم ميـزة كبيـرة فـي تخطيـط وتنفيـذ الهجمـات علـى الفضـاء الإلكترونـي التـي تسـتهدف النظـام قـد تفضـي إلـى الحاجـة إلـى اتخـاذ تدابيـر أقـوى. وبالإضافـة إلـى ذلـك، قـد يكـون تصنيـف بيانـات العمليـات التاريخية (علـى سـبيل المثـال بيانـات التسـجيل) لتقييـد توزيعهـا (مثـل تطبيـق الرقابـة الإداريـة) ضرورياً لتقليـل مخاطـر الإفشـاء مـن دون إذن إلـى مسـتوى مقبـول.

نهج إدراك المخاطر

3-10- ينبغـي تنفيـذ الأمـن الحاسـوبي باسـتخدام نهـج قائـم علـى إدراك المخاطـر. ويعـرض الشـكل 4 مـن المرجـع [7] لمحـة عامـة عـن نهـج إدراك المخاطـر حيـال تدابيـر الأمـن

الحاسـوبي.

3-11- وتُمثـل المخاطـر، فـي سـياق الأمـن الحاسـوبي، المخاطـر المرتبطـة بخصـم يسـتغل الثغـرات فـي أصـل رقمـي أو مجموعـة مـن الأصـول الرقميـة لارتـكاب عمـل ضـار أو تسـهيل ارتكابـه. ويُعبـر عـن هـذا الخطـر كمزيـج مـن احتمـال حـدوث هجـوم ناجـح وشـدة عواقبـه فـي حـال حدوثـه.

تقييم المخاطر وإدارتها

3-12- ينبغـي أن يضـع المشـغِّل عمليـة لإدارة مخاطـر الأمـن الحاسـوبي وتنفيذهـا (مـا لـم تكـن السـلطة المختصـة تتولـى إجـراء عمليـة الإدارة). ويمكـن للسـلطة المختصـة أن تُحـدد متطلبـات السياسـة الواجـب اتباعهـا، ويمكـن أن تشـترط اسـتخدام منهجيـة محـددة لتقييـم المخاطـر، أو يمكـن أن توافـق علـى اسـتخدام منهجيـة المشـغِّل [7]. ويمكـن لعمليـة التقييـم فـي مرفـق مـا أن تتبـع نمـوذج تقييـم مخاطـر الأمـن الحاسـوبي التنظيمـي كمـا هـو موضـح فـي الفقـرات مـن 7-10 إلـى 7-16 مـن المرجـع [7].

3-13- وينبغـي أن تشـمل عمليـة إدارة مخاطـر الأمـن الحاسـوبي عمليـة دوريـة للتحسـين المسـتمر[16] فـي إدارة المخاطـر المرتبطـة بالهجمـات علـى أمـن الفضـاء الإلكترونـي التـي يتعـرض لهـا المرفـق.

3-14- وتُسـتخدم تقييمـات المخاطـر الدوريـة والتكراريـة لدعـم اتخـاذ القـرار فـي إطـار عمليـة إدارة المخاطـر. وعـادة مـا تكـون تقييمـات مخاطـر الأمـن الحاسـوبي نوعيـة، وتشـمل مقاييـس نسـبية (علـى سـبيل المثـال، عاليـة ومتوسـطة ومنخفضـة)، ولكـن يمكـن أن تكـون كميـة إذا توافـرت بيانـات يمكـن التعويـل عليهـا بالقـدر الكافـي.[17] وستُسـاعد نتائـج تقييمـات المخاطـر فـي تحديـد متطلبـات الأمـن الحاسـوبي المناسـبة.

3-15- وينبغـي أن يُجـري المشـغِّل إدارة لمخاطـر الأمـن الحاسـوبي للمرفـق للامتثـال للمتطلبات الرقابيـة. ويُشـير المرجـع [7] إلـى أن ذلـك يمكـن أن يشـمل تقييميـن تكميلييـن، أحدهمـا على

[16] من أمثلة العملية الدورية للتحسين المستمر دورة التخطيط والعمل والتحقق والتنفيذ.

[17] لا توجـد أثنـاء إصـدار هـذا المنشـور منهجيـة مقبولـة دوليـاً تُطبـق قيمـاً كميـة لتقييـم المخاطـر الأمنيـة.

المستوى التنظيمي والآخر على مستوى النُظم، وينبغي الأخذ بهذا النهج في المرافق المعقدة والشديدة الخطورة، مثل المرافق النووية. ويفترض بالتالي في الإرشادات الواردة في هذا المنشور أن تشمل إدارة مخاطر الأمن الحاسوبي لأي مرفق نووي (إدارة مخاطر الأمن الحاسوبي للمرفق) مرحلة محددة لتقييم المخاطر وإدارتها على مستوى النُظم (إدارة مخاطر الأمن الحاسوبي للنُظم) (انظر الشكل 4). ويشمل ذلك مرحلتين:

(أ) تقييم مخاطر الأمن الحاسوبي المجمعة لوظائف المرفق بأكمله وإدارتها. وسيضمن ذلك قيام المشغِّل بإجراء تقييم كامل للمرفق وتزويد السلطة المختصة بالوسائل الأوّلية لتقييم الفعالية العامة لإدارة مخاطر الأمن الحاسوبي في المرفق. ويُقدم القسم 4 إرشادات بشأن إجراء إدارة مخاطر الأمن الحاسوبي للمرفق.

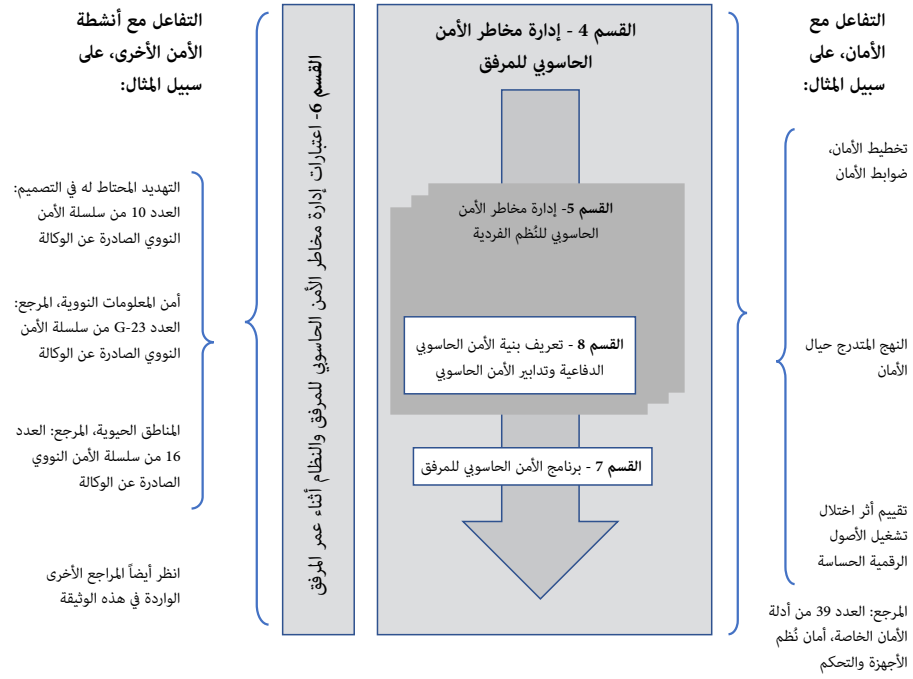
(ب) تقييم وإدارة المخاطر المرتبطة بكل نظام يؤدي وظائف المرفق أو يدعمها. وسيضمن ذلك قيام المشغِّل بإجراء تقييم مفصل لكل نظام يؤدي وظيفة في المرفق أو يدعمها. ويمكن أن تطلب السلطة المختصة إجراء تقييمات مفصلة كوسيلة لاستعراض فعالية حالات محددة من حالات إدارة مخاطر الأمن الحاسوبي في المرفق. ويقدم القسم 5 إرشادات بشأن إجراء إدارة مخاطر الأمن الحاسوبي للنُظم.

3-16- وينبغي أن يضمن المشغِّل استقلال الأفرقة المسؤولة عن إجراء إدارة مخاطر الأمن الحاسوبي بشكل عام لتحديد متطلبات الأمن الحاسوبي للمرفق، والأفرقة التي تُنفذ المتطلبات، والأفرقة التي تتحقق من استيفاء المتطلبات.

3-17- ومن المهم إجراء إدارة للمخاطر في جميع مراحل عمر المرفق وطوال دورات حياة النُظم للاسترشاد بها في وضع تدابير الأمن الحاسوبي وتنفيذها وتعهدها. ويُحدد القسم 6 أنشطة إدارة المخاطر طوال عمر المرفق.

3-18- وينبغي إجراء استعراض لتقييم المخاطر، وتحديث تقييم المخاطر بحسب ما تقتضيه الضرورة، في الحالات التالية:

(أ) ظهور معلومات جديدة أو نتائج مهمة يمكن أن تُبطل الافتراضات الواردة في سياسة الأمن الحاسوبي الراهنة، أو برنامج الأمن الحاسوبي، أو بنية الأمن الحاسوبي الدفاعية، أو تقييم التهديدات الخاصة بالموقع.



الشكل -4- الهيكل العام للإرشادات بشأن إدارة مخاطر الأمن الحاسوبي في هذا المنشور.

(ب) اكتشاف ثغرة تعطل تدابير الأمن الحاسوبي أو الافتراضات المحددة في تقييم مخاطر النظام.

(ج) وقوع حادث متصل بالأمن الحاسوبي في المرفق.

(د) تعديل بيان التهديد الوطني أو التهديد المحتاط له في التصميم (وكون التعديلات ذات صلة بالخصوم الذين يستخدمون هجمات على الفضاء الإلكتروني أو هجمات مختلطة). ويمكن أن يُعبِّر ذلك عن تهديدات جديدة أو قدرات أو موارد معززة لدى الخصم قد تزيد من احتمالات نجاح الهجمات على الفضاء الإلكتروني.

(هـ) حدوث تغيير في وظيفة المرفق أو لنظام أو الأصول الرقمية الحساسة أو تدابير الأمن الحاسوبي. وينبغي أن يشمل ذلك إدخال أي معدات أو برامجيات أو إجراءات جديدة أو أي تغيير رئيسي في مجموعات المهارات لدى موظفي التشغيل. ويمكن أن يسترشد مستوى الجهد المبذول لتحديث تقييم المخاطر بمستوى الحماية المخصص للأصل الرقمي الحساس (مثل مستوى الأمن الحاسوبي).

(و) تغيير المتطلبات الرقابية.

(ز) حلول موعد إجراء استعراض دوري وفقاً لعملية التحسين المستمر لضمان استمرار سريان التقييم.

3-19- وينبغي أن تشمل الأنشطة الرقابية المتصلة بأمن المرفق، مثل الترخيص والتفتيش والإنفاذ، بإيلاء المراعاة المناسبة للأمن الحاسوبي. وينبغي أن تكون السجلات المستمدة من عملية إدارة المخاطر والقرارات والإجراءات الناتجة عنها متاحة للاستعراض من جانب السلطة المختصة بناءً على طلبها لتمكينها من تقييم ما إذا كان قد جرى استيفاء المتطلبات الرقابية.

3-20- وينبغي أن يشمل الهيكل العام والنهج المتبع في عملية إدارة المخاطر ما يلي:

(أ) إدارة مخاطر الأمن الحاسوبي للمرفق:
'1' تحديد نطاق إدارة مخاطر الأمن الحاسوبي؛
'2' تحديد خصائص المرفق؛
'3' تحديد خصائص التهديدات؛
'4' تحديد المتطلبات؛
'5' التحقق والتثبت؛
'6' القبول من جانب السلطة المختصة.
(ب) إدارة مخاطر الأمن الحاسوبي للنظم:
'1' تحديد حدود النظام؛
'2' تحديد الأصول الرقمية (بما فيها الأصول الرقمية الحساسة)؛
'3' متطلبات الأمن الحاسوبي للنظام؛
'4' التحقق.

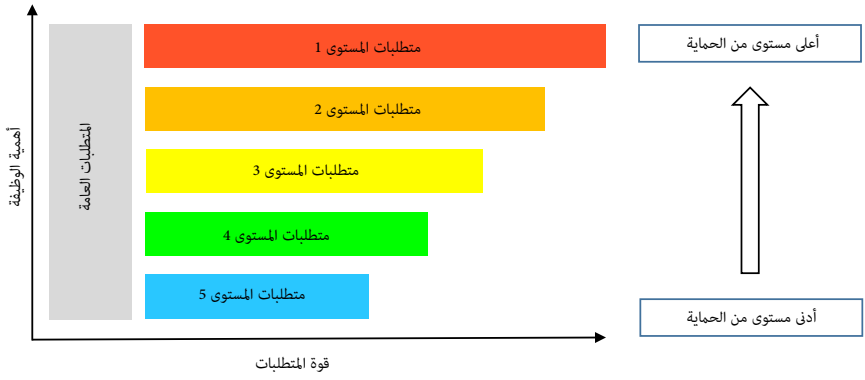
3-21- ويوجد العديد من الطرق لإجراء تقييم المخاطر (انظر على سبيل المثال [14] ISO/IEC 27005). ويتعيّن على المنظمات اختيار أسلوب وتكييفه مع بيئتها وأهدافها التنظيمية المحددة وفي الوقت نفسه ملاحظة الحاجة إلى إدارة منفصلة للمخاطر على مستوى المرفق والنظام.

مستويات الأمن الحاسوبي بالاستناد إلى نهج متدرج

3-22- ينبغي أن تستند متطلبات الأمن الحاسوبي وتصميم التدابير وتنفيذها بهدف تلبية هذه المتطلبات، إلى نهج متدرج تُطبق على أساسه تدابير الأمن الحاسوبي بالتناسب المباشر مع العواقب المحتملة الناشئة عن المساس بوظيفة المرفق. وكما يبين القسم 2، تتمثل إحدى الطرق العملية لتطبيق نهج متدرج في تخصيص وظائف المرفق لمستويات الأمن الحاسوبي، حيث يتميَّز كل مستوى من مستويات الأمن الحاسوبي بمتطلبات أمن حاسوبي متدرجة، ويمكن اختيار تدابير الأمن الوقائية والحمائية لتلبية المتطلبات الخاصة بالمستوى ذي الصلة. ويوضح الشكل 5 النهج المتدرج باستخدام مستويات الأمن الحاسوبي.

3-23- في حين أن المتطلبات (مثل القيود الصريحة المفروضة على الاتصال بين الأصول الرقمية الحساسة المعيّنة للمستويات المختلفة) تُحدد تبعاً لمستويات الأمن الحاسوبي، ويمكن اختيار تدابير الأمن (مثل النوع المحدد لجدار الحماية المستخدم لتقييد هذه الاتصالات) لحماية الأصول الرقمية (بما فيها الأصول الرقمية الحساسة) وفقاً للبيئة البنيوية لمستوى الأمن الحاسوبي وتكنولوجيا الأصول الرقمية المحددة (بما فيها الأصول الرقمية الحساسة).

3-24- وفي النهج القائم على مستويات الأمن الحاسوبي، يتعيّن تحديد متطلبات الأمن



الشكل -5- توضيح النهج المتدرج باستخدام مفهوم مستويات الأمن الحاسوبي

الحاسوبي لكل مستوى بالاستناد إلى الاعتبارات التالية:

(أ) ينبغي تطبيق المتطلبات العامة بصورة واسعة على نطاق المرفق والمنظمة المشغِّلة، ويمكن تطبيقها على جميع الأصول الرقمية. وتتيح المتطلبات العامة تحسين ثقافة الأمن النووي من خلال زيادة الوعي بالأمن الحاسوبي. وتُحسِّن هذه المتطلبات أيضاً قدرة الأمن الحاسوبي على الصمود، وقد توفِّر دفاعاً إضافياً في العمق. ولا يمكن أن يُنسب إلى المتطلبات العامة أي فضل في توفير فائدة لمستوى أو نظام الأمن الحاسوبي المحدد لأن التدابير العامة تنطبق في العادة على مجموعة واسعة من الأصول الرقمية ولا يمكن التعويل على تطبيقها بصورة متسقة وفعالة.

(ب) تُعيَّن مستويات الأمن الحاسوبي، بدءاً من المستوى 5 (أقل حماية مطلوبة) إلى المستوى 1 (أكبر حماية مطلوبة) (انظر الشكل 5). وفي هذا النهج، تكون النُظم التي تشمل أصولاً رقمية حساسة داخلة ضمن مستويات الأمن الحاسوبي من 1 إلى 3، في حين أن النُظم في المستويين 4 و5 تشمل أصولاً رقمية أخرى.

(ج) تُحدد متطلبات الأمن الحاسوبي وتُطبق وفقاً لمستويات الأمن الحاسوبي المعيّنة بناءً على نهج متدرج. وينبغي أن تستند متطلبات الأمن الحاسوبي إلى الدفاع في العمق الذي لا تعتمد فيه الأصول الرقمية المعيّنة لمستويات الأمن التي توفِّر حماية أعلى فقط على الأصول الرقمية أو تدابير الأمن الحاسوبي المعيّنة لمستويات الأمن ذات الحماية المنخفضة أو تثق بها ضمنياً.

(د) ينبغي أن تراعي تدابير الأمن الحاسوبي المطبقة لتلبية المتطلبات لكل مستوى من مستويات الأمن الحاسوبي استقلالية التدابير وتنوعها من أجل الحد من الثغرات الشائعة التي يمكن أن تسمح بتجاوز طبقات متعددة من الدفاع في العمق أو التغلب عليها. ومع ذلك قد يكون من الضروري استخدام بعض تدابير الأمن الحاسوبي المطبقة في مستوى معيّن من مستويات الأمن الحاسوبي لتطبيقها في مستويات أخرى من مستويات الأمن الحاسوبي.

(هـ) يمكن لتدابير الأمن الحاسوبي المطبقة على المستويات الدنيا، عند استخدام نهج متعدد الطبقات والدفاع في العمق، أن تساعد في حماية المستويات العليا، وخاصة في الكشف المبكر عن الهجمات على الفضاء الإلكتروني.

(و) النُظم القائمة على الحاسوب الخارجة عن سيطرة برنامج الأمن الحاسوبي هي نُظم غير معيّنة، وينبغي ألّا يثق بها أي أصل من الأصول الرقمية على أي مستوى من مستويات الأمن الحاسوبي.

3-25- ويُقدم القسم 8 إرشادات بشأن متطلبات الأمن الحاسوبي لنهج متدرج باستخدام مثال لخمسة مستويات من مستويات الأمن الحاسوبي، بالإضافة إلى متطلبات الأمن الحاسوبي العامة.

4- إدارة مخاطر الأمن الحاسوبي للمرفق

4-1- تُمثل إدارة مخاطر الأمن الحاسوبي للمرفق عملية معقدة ينبغي أن يجريها فريق متعدد التخصصات مكون من أشخاص يتمتعون بالمهارات والكفاءات في مجال الأمن النووي والأمان النووي والعمليات والصيانة والأمن الحاسوبي والهندسة.[18] ويمكن أن يكون لهذا الفريق تكوين مماثل للتكوين المقترح لتقييمات الحماية المادية (انظر المرجع [15]). ويمكن أن تستخدم بعض الدول الأعضاء تسميات مثل 'فريق أمن الفضاء الإلكتروني' لتحديد الأفراد المطلوبين للأمن الحاسوبي.

4-2- وتُمثل إدارة مخاطر الأمن الحاسوبي للمرفق عملية تكرارية يتم إجراؤها على مراحل. وقد يكون من الضروري استعراض الافتراضات أو الاستنتاجات أو النتائج المستمدة من مرحلة سابقة وتعديلها على أساس نتائج مرحلة لاحقة. ويتوقع أن تُنفذ أنشطة للتحقق بين المراحل.

هدف إدارة مخاطر الأمن الحاسوبي للمرفق

4-3- يتمثل هدف إدارة مخاطر الأمن الحاسوبي للمرفق في تقييم وإدارة المخاطر المرتبطة بالهجمات على الفضاء الإلكتروني التي يمكن أن تتسبب في إضعاف الأمن النووي أو الأمان النووي للمرفق.

4-4- وينبغي أن تضمن إدارة مخاطر الأمن الحاسوبي للمرفق استيفاء المتطلبات الرقابية المتعلقة بالأمن الحاسوبي.

[18] قد تستخدم بعض الدول الأعضاء تسميات مثل "فريق الأمن السيبراني" للإشارة إلى الموظفين المطلوبين للأمن الحاسوبي.

4-5- وينبغي أن تأخذ إدارة مخاطر الأمن الحاسوبي للمرفق في الحسبان تقييم الخصوم المحددين الذين قد يهاجمون المرفق وما يسعون إلى تحقيقه من أهداف (على سبيل المثال، التخريب، أو إزالة مواد نووية أو مواد مشعة من دون إذن، أو الوصول من دون إذن إلى معلومات حساسة)، بما في ذلك تقييم جاذبية الأهداف[19] في المرفق بالنسبة لهؤلاء الخصوم. ويمكن توفير تقييم الدولة للتهديدات من خلال بيان التهديد الوطني أو التهديد المحتاط له في التصميم[20].

4-6- وينبغي أن تشمل إدارة مخاطر الأمن الحاسوبي للمرفق استنتاجاً بشأن أهمية كل وظيفة من وظائف المرفق وفقاً لأهمية الوظيفة بالنسبة لأهداف المشغِّل. ويمكن أن تتيح هذه الاستنتاجات وضع قائمة هرمية[21] بأحداث الأمن النووي المحتملة (بدءاً بالأحداث التي تنطوي على أشد العواقب وانتهاءً بالأحداث التي لا تنطوي على أي عواقب) الناشئة عن المساس بوظيفة في المرفق.[22] ويمكن استخدام الشكل 7 في المرجع [7] في وضع هذه القائمة الهرمية.

4-7- وينبغي أن تشمل إدارة مخاطر الأمن الحاسوبي للمرفق مراعاة وظائف المرفق، من دون النظر في تنفيذها التقني في النُظم والأصول الرقمية، لأن ذلك هو ما تأخذه في الاعتبار إدارة مخاطر الأمن الحاسوبي للنُظم (انظر القسم 5).

4-8- ومن شأن استخدام نهج متسق في إدارة مخاطر الأمن الحاسوبي لجميع المرافق داخل الدولة أن يساعد السلطات المختصة على توفير إشراف فعال فيما يتعلق بتطبيق الأمن الحاسوبي في المرافق النووية.

---

[19] يمكن تناول جاذبية الأهداف في تقييم التهديدات أو التهديد المحتاط له في التصميم، ويمكن تعزيزها بالمعلومات المقدمة من الدولة من خلال سلطاتها المختصة.

[20] يُستمد التهديد المحتاط له في التصميم من التقييم الراهن الذي تُجريه الدولة للتهديد، ويُشكل أساساً لوضع تدابير للأمن النووي. وتقع على المشغِّل المسؤولية الأولى عن توفير تدابير الأمن النووي ضد قدرات التهديدات المبيّنة في التهديد المحتاط له في التصميم. وتوفِّر بعض الدول الأعضاء بيان التهديد الوطني بدلاً من التهديد المحتاط له في التصميم.

[21] قائمة مرتبة تضع وظائف المرفق في مجموعات متماثلة تقريباً من حيث العواقب.

[22] يجوز للمشغِّل أيضاً إدراج وظائف أخرى محددة على أنها مهمة للمرفق بخلاف الأمان أو الأمن.

مدخلات لإدارة مخاطر الأمن الحاسوبي للمرفق:

4-9- ينبغي أن يستخدم المشغِّل ما يلي كمدخلات في إدارة مخاطر الأمن الحاسوبي للمرفق:

(أ) بيان التهديد الوطني أو التهديد المحتاط له في التصميم وما يرتبط بذلك من تحليل، إن وجد.
(ب) المتطلبات الرقابية المعمول بها والوثائق الأخرى. ويمكن أن تشمل متطلبات الدولة لتصنيف المعلومات.
(ج) تحليل الأمان للنُظم الحاسوبية في المرفق. ويمكن استخدام هذا التحليل في تحديد متطلبات الأمن الحاسوبي، ولكنه ليس كافياً لهذا الغرض لأنه لا يُعالج جميع حالات سوء التشغيل، ولا سيما ما ينشأ منها عن الأعمال الضارة.
(د) خطة أمن الموقع [15]. ويمكن استخدام خطة أمن الموقع في تحديد وظائف المرفق المهمة للأمن أو المرتبطة به وأهميتها في تحقيق أهداف المشغِّل. ويمكن أن تشمل خطة أمن الموقع برنامج الأمن الحاسوبي للمرفق أو جوانب من هذا البرنامج.
(هـ) سياسة الأمن الحاسوبي للمرفق.
(و) وثائق برنامج الأمن الحاسوبي الحالي والسابق للمرفق، بما في ذلك تفاصيل تخصيص وظائف المرفق للنُظم وتقييم التهديدات الخاصة بالمرفق.

مراحل إدارة مخاطر الأمن الحاسوبي للمرفق

4-10- فيما يلي مراحل إدارة مخاطر الأمن الحاسوبي للمرفق:

(أ) تحديد النطاق: تحديد نطاق لتقييم المخاطر، مع مراعاة أهداف المشغِّل المتعلقة بالمرفق (مثل الأمان والأمن والعمليات والتأهب لحالات الطوارئ)، والحدود المادية والمنطقية، ومرحلة عمر المرفق. وينبغي تحديد الشروط الأساسية المسبقة للتقييم ومدخلاته في هذه المرحلة.

(ب) تحديد خصائص المرفق: تحديد وظائف المرفق وتفاعلاتها وترابطاتها، وتحديد المعلومات الحساسة التي يمكن أن تكون مفيدة في التخطيط لهجوم ضد المرفق، وتحديد الأهداف على أساس وظائف المرفق المحددة والمعلومات الحساسة.

(ج) تحديد خصائص التهديد: تحليل تقييم التهديد الوطني أو التهديد المحتاط له في التصميم وأي معلومات أخرى ذات صلة أو تحليل التهديدات لتحديد الخطط والتقنيات والإجراءات المحددة إلى جانب مهارات الخصوم التي يمكن استخدامها في الهجمات على الفضاء الإلكتروني (بما في ذلك الهجمات المختلطة) على الأهداف في المرفق النووي. ويمثل تحديد خصائص التهديد نموذجاً يوضع من خلال تحليل الجوانب القابلة للتطبيق من المعلومات المتعلقة بالتهديد، للحصول على صورة تمثيلية للخصوم الذين يُشكلون أكبر خطر. وتُحدد مرحلة تحديد خصائص التهديد نطاق سيناريوهات الهجمات ذات المصداقية.

(د) تحديد متطلبات الأمن الحاسوبي: توليد متطلبات الأمن الحاسوبي على مستوى المرفق. وتشمل مرحلة التحديد ما يلي:

'1' وضع برنامج للأمن الحاسوبي وتوثيقة؛

'2' التوصية بأي تعديلات ضرورية على سياسة الأمن الحاسوبي؛

'3' تخصيص وظائف المرفق المحددة لمستويات الأمن الحاسوبي؛

'4' وضع متطلبات بنية الأمن الحاسوبي الدفاعية أو تعديلها.

ويمكن أن يشمل ذلك تطبيق تقنيات التحليل (على سبيل المثال، تقييم الثغرات، وتقييم التهديدات) وأساليب التقييم (انظر الفقرة 98-4) لتوليد المتطلبات من مرحلتي تحديد خصائص المرفق وتحديد خصائص التهديد، ومن المتطلبات الرقابية.

(هـ) إدارة مخاطر الأمن الحاسوبي للنظم: يُطبق برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية على كل نظام. ويصف القسم 5 بصورة كاملة عملية إدارة مخاطر الأمن الحاسوبي للنظم. وقد يلزم إدخال تغييرات على برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية في ضوء الخبرة المكتسبة من تنفيذ برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية في كل نظام.

(و) تنفيذ النُظم وإدماجها في المرفق: لا ترد تفاصيل أخرى عن هذه المرحلة في هذا المنشور. وقد يلزم إدخال تغييرات على بنية الأمن الحاسوبي الدفاعية وبرنامج الأمن الحاسوبي في ضوء الخبرة الهندسية العملية المكتسبة من تنفيذ إدماج النُظم.

(ز) أنشطة الضمان: هذه الأنشطة ليست مجرد مرحلة من مراحل إدارة مخاطر الأمن الحاسوبي للمرفق، بل هي مجموعة من الأنشطة المستمرة التي تُنفذ أيضاً في كل عملية من عمليات إدارة مخاطر الأمن الحاسوبي للنظم. وتُستخدم ثلاثة أنواع من أنشطة الضمان:

'1' تقييم الامتثال لمتطلبات الأمن الحاسوبي؛

'2' التحقق من كل مرحلة من مراحل إدارة مخاطر الأمن الحاسوبي؛

'3' التحقق من الأمن الحاسوبي للمرفق.

وتُشكل السيناريوهات جزءاً حيوياً من التقييم والتحقق وأنشطة التثبت.

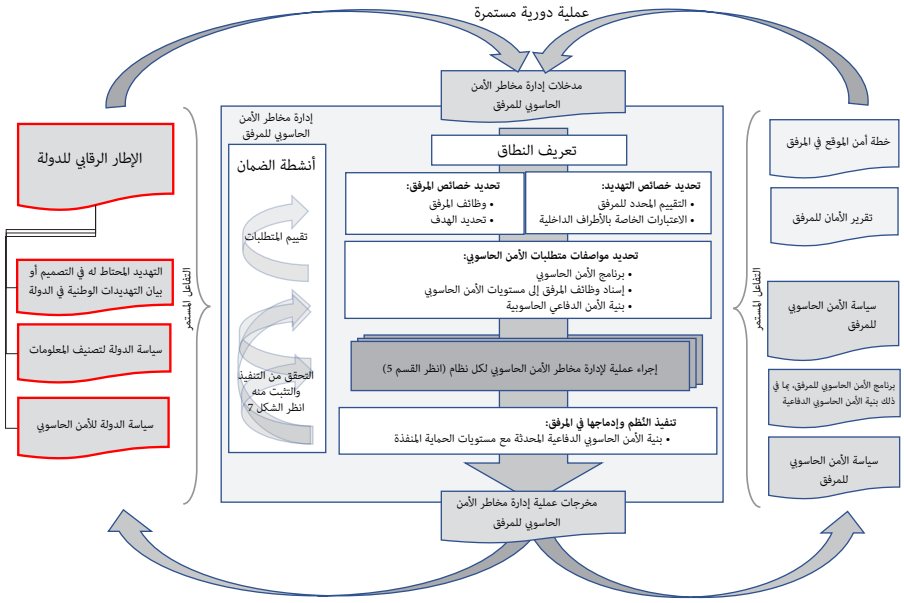
(ح) مخرجات إدارة مخاطر الأمن الحاسوبي للمرفق: تشمل هذه المخرجات برنامج الأمن الحاسوبي (المنقح) وبنية الأمن الحاسوبي الدفاعية، وتقييم التهديدات الخاصة بالموقع، وتقرير الامتثال لإدارة مخاطر الأمن الحاسوبي للمرفق. وسيخضع بعض هذه الوثائق أو جميعها لاستعراض لقبولها من جانب السلطة المختصة. ويمكن أن تكون مخرجات إدارة مخاطر الأمن الحاسوبي مدخلات تستفيد منها الدولة في مواصلة تطوير المتطلبات الرقابية.

4-11- وترد مراحل إدارة مخاطر الأمن الحاسوبي للمرفق في الشكل 6 الذي يُقدم لمحة عامة عن عملية إدارة مخاطر الأمن الحاسوبي للمرفق. وترد هذه المراحل بمزيد من التفصيل في الجزء المتبقي من هذا القسم.

4-12- وتوجد عملية إدارة واحدة لمخاطر الأمن الحاسوبي لكل مرفق، وتوجد داخلها عملية منفصلة لإدارة مخاطر الأمن الحاسوبي لكل نظام. وفيما يتعلق بالمواقع التي تحتوي على مرافق متعددة أو المنظمة التي تُشغل مرافق متعددة، يمكن أن تكون هناك عملية واحدة للموقع بأكمله أو للمنظمة بأكملها، مما يؤدي إلى واحدة أو أكثر من مجموعات مخرجات إدارة مخاطر الأمن الحاسوبي للمرفق. وفي هذه الحالة، يمكن للمشغِّل أن يحدد عدد مجموعات المخرجات المتولدة، ولكن ينبغي أن يضمن أن العملية تُطبق بصورة شاملة على كل مرفق.

تحديد النطاق

13-4- ينبغي أن يحدد المشغِّل نطاق عملية إدارة مخاطر الأمن الحاسوبي للمرفق، وهذا النطاق هو المدى المادي أو المنطقي لوظائف المرفق وما يرتبط بها من نُظم تهم الأمن النووي. ويمكن أن تشمل الاعتبارات المتعلقة بتحديد النطاق المحيط المادي للمرفق؛ وأماكن البائعين المعتمدين والمتعهدين والموردين؛ ومكاتب المنظمة المشغِّلة؛ ومراكز البيانات خارج الموقع؛ وأي مواقع استراتيجية أخرى. وقد يتفاوت نطاق التقييم أيضاً تبعاً لمرحلة عمر المرفق أو قدرة ونُضج المنظمة المشغِّلة (انظر الفقرات من 5-26 إلى 5-29 من المرجع [7]).



الشكل -6- لمحة عامة عن عملية إدارة مخاطر الأمن الحاسوبي للمرفق.

تحديد وظائف المرفق

4-14- ينبغي أن يحدد المشغِّل جميع وظائف المرفق من دون النظر في كيفية أداء هذه الوظائف. ومن شأن وجود أصول رقمية واستخدامها في المرفق وطوال عمره أن يجعل من المحتمل استخدام الأصول الرقمية لإجراء أو دعم غالبية المهام والأنشطة الرئيسية المرتبطة بوظائف المرفق.

4-15- وينبغي أن تؤخذ في الحسبان مرحلة عمر المرفق [10] عند تحديد خصائص المرفق وتحديد وظائفه. وستكون وظائ6 المرفق المختلفة ذات صلة في مختلف مراحل عمر المرفق، وقد تتغيَّر أهميتها النسبية.

4-16- وتتميّز وظائف المرفق بالعناصر التالية:

(أ) الأهمية الجوهرية: أهمية وظيفة المرفق للأمن النووي والأمان النووي والعواقب المحتملة على المرفق في عدم أداء الوظيفة بصورة صحيحة.[23] وهذه هي الخاصية الرئيسية.
(ب) التأثيرات المحتملة الناتجة عن التعرض للخطر: الطرق التي يمكن أن تفشل بها وظيفة المرفق في الأداء بصورة صحيحة.
(ج) الترابطات بين الوظائف: قد تنشأ أهمية وظيفة المرفق من الوظائف الأخرى التي تعتمد عليها.
(د) توقيت ودقة إجراء وظيفة المرفق.

[23] يمكن في كثير من الأحيان أن تكون أهمية الوظيفة للأمن النووي مرتبطة بعواقب عدم أداء الوظيفة بصورة صحيحة. وفيما يتعلق بالمرافق النووية، تتمثل العواقب التي تُعتبر أكثر أهمية في إزالة المواد النووية من دون إذن، والتخريب، مما يسفر عن عواقب إشعاعية غير مقبولة. ويمكن النظر في العواقب الأخرى، مثل إفشاء معلومات حساسة من دون إذن. وقد تكون العواقب الممكنة الأخرى مرتبطة بأهداف تنظيمية أخرى، مثل الحفاظ على السمعة أو الامتثال للوائح البيئية الأخرى. وترد في ISO 27005:2018 [14] قائمة بالعواقب المحتملة.

الأهمية الجوهرية لوظائف المرفق

4-17- ينبغي مقارنة أهمية جميع وظائف المرفق من أجل تجميع الوظائف المتماثلة الأهمية، يُستخدم فيها إن أمكن، مقياس مشترك يشمل اعتبارات الأمن والأمان على حد سواء.

4-18- وفيما يتعلق بوظائف المرفق المهمة للأمن النووي أو المرتبطة بها، ينبغي أن يُستخدم مخطط تصنيفي مستند إلى العواقب المترتبة على الأمن النووي، على النحو الموضح في الشكل 7 من المرجع [7].

4-19- وفيما يتعلق بوظائف المرفق المهمة للأمان النووي أو المرتبطة بها، يمكن استخدام مخطط تصنيفي قائم بالفعل لتصنيف الأمان من أجل تحديد أهمية الوظيفة. ومع ذلك، يمكن أن تتطلب اعتبارات الأمن إسناد أهمية أعلى مما يُشير إليه تصنيف الوظيفة من حيث الأمان.

4-20- وينبغي أن يراعي تحديد أهمية وظائف المرفق أن أداء وظائف الأمان (من خلال النُظم) قد يدعم الأمن وأن أداء وظائف الأمن قد يدعم وظائف الأمان. ونتيجة لذلك، يمكن أن تتفاوت الأهمية المخصصة لوظيفة الأمان في الأمن الحاسوبي عن فئتها المتعلقة بالأمان.

4-21- وعلى سبيل المثال، قد ينص أيضاً نظام يوفِّر وظيفة للكشف عن الإشعاعات من أجل حماية الموظفين (هدف مرتبط بالأمان) على كشف إزالة المواد النووية من دون إذن (هدف مرتبط بالأمن النووي). وعلى الرغم من أن تعطل وظيف الحماية من الإشعاعات من منظور الأمان قد تكون له عواقب محدودة فإن عواقب تعطلها من منظور الأمن قد تكون أشد حدة. ولذلك ستُسند لوظائف المرفق التي يوفرها النظام في هذا المثال قيمة مهمة على أساس أهمية تلك النُظم لأهداف الأمن النووي (وبدلاً من ذلك، يمكن للمشغِّل اختيار تنفيذ نُظم مستقلة للفصل بين الوظائف التي تدعم الأمان النووي والأمن النووي، وفي هذا المثال، يمكن تخصيص أهمية أقل للوظيفة الداعمة للأمان النووي).

التأثيرات المحتملة للمساس بنظام على وظيفة المرفق

4-22- بالإضافة إلى النظر في الأهمية الجوهرية لوظيفة المرفق، ينبغي أن ينظر المشغِّل في التأثيرات الواقعة على وظيفة المرفق بسبب المساس بالنظام المراد منه أداء تلك الوظيفة. وهذه التأثيرات هي كما يلي (مرتبة من الأسوأ إلى الأفضل):

(أ) أداء وظيفة المرفق غير محدد. ويعني ذلك أن من الممكن تغيير الوظيفة بأي شكل من الأشكال من دون اكتشاف أي مساس أوّلي بها.
(ب) يتغيَّر أداء وظيفة المرفق بطرق غير متوقعة (ويمكن تنفيذ إجراءات أخرى)، ولكن يمكن للمشغِّل ملاحظة هذه الحالات الشاذة.
(ج) تعطل أداء وظيفة المرفق.
(د) أداء وظيفة المرفق على النحو المتوقع، مما يعني أن المساس بها لا يؤثر سلباً على الوظيفة (أي أن النظام قادر على تحمل الأعطال).

4-23- قد يحدث خلل في النظام الذي يُقصد منه أداء وظيفة معيّنة في المرفق عند المساس به، وتعتمد آثار الخلل على الظروف والبيئة في الوقت الذي يحدث فيه مساس بالنظام، وطبيعة الهجوم على الفضاء الإلكتروني الذي يتسبب في المساس بالنظام، وأهمية وظيفة المرفق. وعلى سبيل المثال، قد يُستخدم نظام يؤدي وظيفة أقل أهمية في المرفق، من خلال ترابطات وتفاعلات بين الوظائف، لمهاجمة نظام يؤدي وظيفة أكثر أهمية.

4-24- ولكل نظام ولكل نوع من تأثيرات المساس بالنظام (أي اختلال التشغيل)، ستكون هناك عواقب مختلفة على المرفق. وينبغي معالجة هذه العواقب، وينبغي أن تكون الأهمية المحددة لوظائف المرفق مستندة إلى هذه العواقب المحتملة. وعند تقييم العواقب، ينبغي النظر في فقدان سرية المعلومات الحساسة أو سلامتها أو توافرها، وكذلك العواقب المتعلقة بإزالة المواد من دون إذن، أو تخريب المرفق.

4-25- وينبغي أن يأخذ في الحسبان عند تحديد أهمية وظيفة مرفق ما إذا كان يمكن تحديد وظيفة المرفق بطريقة تصلح لجميع الظروف أو الطرق الممكنة التي قد تعتمد عليها الوظيفة. وإذا لم يكن بالإمكان ربط وظيفة المرفق على هذا النحو، قد تكون قائمة العواقب غير كاملة، وقد يلزم إجراء تحليل إضافي أو قيمة أهم (باستخدام نهج محافظ).

أوجه الترابط بين وظائف المرفق

4-26- ينبغي أن يُراعى في تحديد أهمية وظيفة المرفق العواقب المحتملة الناشئة عن المساس بالوظيفة (أو اختلال تشغيلها) على سائر وظائف المرفق التي تعتمد على تلك الوظيفة. ومن أمثلة هذه التبعيات الوظيفية ما يلي:

(أ) تبعية المعلومات: توفِّر وظيفة المرفق معلومات لوظيفة أخرى في المرفق. وتشمل أمثلة اختلال التشغيل ما يلي:
'1' انقطاع تعليمات التحكم الآلي في عملية في المرفق؛
'2' المساس بالإنذارات المقدمة إلى ضباط الأمن؛
'3' عرض معلومات رصد غير صحيحة لموظفي التشغيل؛
'4' عدم تقديم معلومات للقائمين بالتصدي للطوارئ أو لضباط الأمن النووي؛
'5' فقدان الإجراءات أو التعليمات أو السجلات التي توثق نتائج هذه الإجراءات أو التلاعب بها.

(ب) تبعية الموارد الهندسية أو المادية: توفر وظيفة المرفق مورداً مادياً لوظيفة مرفق أخرى. ويشمل ذلك الموارد اللازمة لدعم وظيفة المرفق الأخرى بصورة مباشرة والموارد اللازمة لدعم تلك الموارد. وفيما يلي أمثلة على هذا الاختلال في التشغيل:
'1' انقطاع المياه أو القوى؛
'2' الظروف البيئية المحيطة غير المتوقعة؛
'3' فشل جدولة مهام الصيانة الوقائية؛
'4' فشل نُظم الحماية المادية (مثل التحكم في الدخول، وكشف الاقتحام).

(ج) التبعية السياساتية أو الإجرائية: يتطلب التغيير في وظيفة من وظائف المرفق تغييراً في وظيفة أخرى في المرفق. وعلى سبيل المثال، إذا كانت السياسة تتطلب توفير وظائف بالوعة حرارة أوّلية وثانوية عندما يكون المفاعل في حالة حرجة، ينبغي في هذه الحالة في حال عدم توافر إحدى بواليع الحرارة أن يوضع المفاعل في الحالة دون الحرجة.

(د) تأثيرات القرب: التأثيرات على وظيفة المرفق الناشئة عن اختلال التشغيل أو العطل المادي في النُظم الأخرى القريبة فعلياً من النُظم التي تؤدي وظيفة المرفق.

4-27- وقد يكشف تحليل التفاعلات وأوجه الترابط بين وظائف المرفق أن وظيفة مهمة

مـن وظائـف المرفـق قـد اسـتُبعدت مـن نطـاق التقييـم. وقـد تمتـد التبعيـات إلـى مـا وراء المرفـق، مثـل توفيـر الميـاه أو الطاقـة للمرفـق. وقـد يلـزم النظـر فـي بعـض الوظائـف التـي تقدمهـا المنظمـات الخارجيـة عنـد تحليـل تبعيـات وظائـف المرفـق. وفـي هـذه الحالـة، قـد يكـون مـن الضـروري تنقيـح نطـاق التقييـم ليشـمل تلـك التبعيـات أو لإجـراء تغييـرات فـي المرفـق لإزالـة التبعيـات.

4-28- وقـد يـؤدي الفصـل بيـن النُظـم التـي تـؤدي وظائـف المرفـق للحـد مـن التفاعـلات وأوجـه الترابـط فيمـا بينهـا إلـى تبسـيط مواصفـات مسـتويات الأمـن الحاسـوبي ومتطلباتـه، وقـد يُحسـن فعاليـة تدابيـر الأمـن الحاسـوبي وكفاءتهـا.

التوقيت والدقة اللازمان لأوجه الترابط بين وظائف المرفق

4-29- وقـد يراعـي تحديـد أهميـة وظائـف المرفـق أيضـاً التوقيـت والدقـة اللذيـن تسـتجيب بهمـا وظيفـة المرفـق لوظيفـة أخـرى. ويمكـن النظـر فـي التوقيـت مـن حيـث متطلبـات توافـر المعلومـات الحساسـة، ويمكـن النظـر فـي الدقـة مـن حيـث متطلبـات سـلامة هـذه المعلومـات:

(أ) يعنـي توافـر المعلومـات، علـى سـبيل المثـال، أن الإنـذارات التـي تقدمهـا إحـدى وظائف المرفـق تُقـدم فـوراً للسـماح بـأداء وظائـف المرفـق الأخـرى، مثـل تقييـم الإنـذارات والاسـتجابة لهـا.

(ب) تعنـي سـلامة المعلومـات، علـى سـبيل المثـال، أن وظيفـة المرفـق توفّـر بيانـات دقيقـة عـن المتغيـرات البيئيـة (علـى سـبيل المثـال، درجـة الحـرارة، والضغـط، والتواتـر، والمسـتوى) التـي تعتمـد عليهـا وظائـف المرفـق الأخـرى.

تحديد الهدف

4-30- يُعرَّف الهدف في المرجع [1] على النحو التالي:

> "المواد النووية، والمواد المشعة الأخرى، أو المرافق ذات الصلة، أو الأنشطة ذات الصلة، أو المواقع أو الأشياء الأخرى التي يُحتمل أن يستغلها تهديد الأمن النووي، وتشمل الأحداث العامة الرئيسية، والمواقع الاستراتيجية، والمعلومات الحساسة، وأصول المعلومات الحساسة."

4-31- وستكون بعض النُظم التي تؤدي وظائف للمرفق أهدافاً وينبغي تحديدها من قائمة وظائف المرفق التي يتم إصدارها أثناء إجراء عملية إدارة مخاطر الأمن الحاسوبي للمرفق، باستخدام تعاريف المناطق الحيوية [16] والمعلومات الحساسة [5]. وسواءً كان ذلك النظام يُعتبر هدفاً فإنه لا يُغيِّر أهمية وظيفة المرفق، ولكنه اعتبار إضافي عند تحديد متطلبات الأمن الحاسوبي.

4-32- وينبغي تحديد الأهداف المرتبطة بوظائف مهمة لأمان المرفق وأمن المرفق باعتبارها أصولاً رقمية حساسة من خلال العملية المبيّنة في الفقرات من 3-6 إلى 3-9. وينبغي أيضاً تحليل هذه الأصول الرقمية الحساسة لمعرفة القيمة المحتملة لأي معلومات حساسة مرتبطة بها. وسيضمن ذلك أن الأصول الرقمية الحساسة وما يرتبط بها من معلومات تُعتبر واقعة داخل برنامج أمن المعلومات وبرنامج الأمن الحاسوبي للمرفق ومنحها المستوى المناسب من الحماية.

توثيق وظائف المرفق

4-33- ينبغي أن يوثق المشغِّل جميع وظائف المرفق التي يتم تحديدها وتقييمها أثناء عملية إدارة مخاطر الأمن الحاسوبي للمرفق.

4-34- ويعتمد تحديد الوظائف داخل المرفق على وجود سجلات كاملة ودقيقة تصف التفاعلات وأوجه الترابط بين الوظائف. وستتيح هذه السجلات تقييم هذه الوظائف التي يمكن أن يكون لها أثر سلبي على الوظائف الأخرى إذا لم يتم أداؤها بصورة صحيحة.

4-35- وقد تكون التفاعلات وأوجه الترابط لوظيفة المرفق داخلية أو خارجية، وقد تكون دائمة أو مؤقتة. وعلى سبيل المثال، أثناء تطوير النُظم، قد يلزم حدوث تفاعل بين بيئة التطوير والبيئة التشغيلية من خلال النقل المادي للبرامجيات الحاسوبية الجديدة أو البيانات أو الأجهزة، ولكن هذه التفاعلات يمكن إزالتها عندما تدخل النُظم طور التشغيل.

4-36- وينبغي أن ينظر المشغِّل، عند تحليل عواقب أي هجوم موجه ضد وظيفة من وظائف المرفق، في إمكانية أن يكون جزءاً من هجوم يؤثر على وظائف متعددة في المرفق أو أن يكون جزءاً من هجوم مختلط (أي هجوم مشترك على الفضاء الإلكتروني

وهجـوم مـادي).

4-37- وقـد يلـزم أن يشـمل التحليـل تقييمـاً تكراريـاً لـكل وظيفـة مـن وظائـف المرفـق، حيـث يتـم إجـراء تقييـم لتحديـد الأهميـة الجوهريـة للوظيفـة، ويتـم إجـراء تحليـل آخـر لتحديـد الأهميـة علـى أسـاس التفاعـلات وأوجـه الترابـط مـع سـائر وظائـف المرفـق. وينبغـي اسـتخدام المسـتوى الأعلـى مـن هذيـن المسـتويين مـن مسـتويات الأهميـة.

4-38- وينبغـي إعطـاء وظائـف المرفـق التـي لهـا علاقـة مباشـرة بيـن الوظيفـة التـي لا يتـم أداؤهـا بشـكل صحيـح والعواقـب الأكثـر خطـورة (علـى سـبيل المثـال، وظائـف المرفـق المرتبطـة ارتباطـاً وثيقـاً بوظائـف الأمـان الأساسـية الثـلاث للتحكـم فـي الحرجيـة، وإزالـة الحـرارة، واحتـواء المـواد [12])[24] المسـتوى الأكبـر مـن الأهميـة. وفـي هـذه الحـالات، ينبغـي ألّا يؤخـذ فـي الاعتبـار عنـد تحديـد الأهميـة أي بارامتـرات أو عوامـل أخـرى.

تحديد خصائص التهديد

4-39- يتوقـف تحديـد خصائـص التهديـد علـى عمليتيـن مسـتمرتين منفصلتيـن ولكنهمـا مترابطتـان:

(أ) تقييـم الدولـة للتهديـدات وتطويـر بيـان التهديـد الوطنـي أو التهديـد المحتـاط لـه فـي التصميـم وتعهـده باسـتخدام المصـادر الاسـتخباراتية؛
(ب) تقييـم التهديـدات الخاصـة بالمرفـق، مـع مراعـاة تحليـل المعلومـات الخاصـة بالمرفـق والمعلومـات المتعلقـة بالخصـوم المحدديـن.

مصادر المعلومات المتعلقة بالتهديد

4-40- تنص الفقرة 3-34 من المرجع [2] على ما يلي:

"ينبغي أن تحدد السلطات المعنية في الدولة التهديد وما يتصل به من قدرات، باستخدام مصادر معلومات موثوقة، وذلك في شكل تقييم التهديد والتهديد المحتاط له في

[24] انظـر العلاقـات بيـن الوظائـف التـي يعـود لهـا الفضـل عنـد تحليـل الأحـداث البادئـة المفترضـة وفئـات الأمـان فـي الجـدول 1 مـن المرجـع [17].

التصميم، عند الاقتضاء. ويتم تحديد التهديد المحتاط له في التصميم من خلال تقييم تجربة الدولة للتهديد الذي يثيره السحب دون إذن والتخريب."

ويمكن الرجوع إلى معلومات إضافية عن التهديد المحتاط له في التصميم في المرجع [9].

4-41- ينبغي أن يضع المشغِّل تدابير لتحديد المعلومات المحددة[25] المتعلقة بالهجمات المحتملة على الفضاء الإلكتروني والخصوم المحتملين والاحتفاظ بها وإدارتها (مثل رسائل الانتحال الإلكتروني وعينات البرامجيات الخبيثة) للسماح بتحليل لمتابعة دعم تحديد خصائص التهديد. وينبغي أن يضمن المشغِّل تنفيذ هذه التدابير على نحو لا يؤثر سلباً على الأمن النووي أو الأمان النووي.

4-42- وقد تشمل خصائص التهديد التي يحددها المشغِّل عناصر من تقييمات التهديدات التي تجريها منظمات أخرى (مثل التقييمات التي يُجريها المشغِّل نفسه، والتقارير المعتمدة على معلومات مستمدة من مصادر علنية).

4-43- وتُشجَّع السلطة المختصة ذات الصلة على تقديم تحليل للمعلومات المحددة التي يحصل عليها المشغِّل في الوقت المناسب وبطريقة تعاونية، ودعم تبادل هذا التحليل والمعلومات المهمة الأخرى، بما يتفق مع متطلبات الدولة بشأن المعلومات الحساسة [5]. ويمكن أن يكون قيام المشغِّل دورياً بالإبلاغ عن الحادثات إلى السلطة المختصة ذات الصلة ذا قيمة كتحليل للتهديد، ويمثل تحديد الخصائص نشاطاً مستمراً يتطلب معلومات مواكبة لآخر المستجدات.

4-44- وأثناء وضع بيان التهديد الوطني، ينبغي أن يكون لدى السلطة المختصة وغيرها من سلطات الدولة ذات الصلة (أو ينبغي أن تتاح لها إمكانية الوصول إلى) الخبرة والمعرفة فيما يتعلق بحادثات الأمن الحاسوبي المحتملة (على سبيل المثال، الهجمات على الفضاء الإلكتروني) في المرافق النووية.

4-45- ويُقدم المرجع [7] إرشادات بشأن تقييم تهديدات الفضاء الإلكتروني التي تتعرض

[25] يمكن للمشغِّل أو السلطة المختصة أو منظمة حكومية أخرى تحديد هذه المعلومات. ويمكن أن تكون هذه المعلومات سرية، ويتعيّن بالتالي الامتثال لمتطلبات الدولة بشأن تحديد المعلومات الحساسة والتعامل معها.

لهـا منظومـة الأمـن النـووي وكذلـك وصـف مفصّـل للمصـادر المحتملـة للهجـوم ومـا يرتبـط بـه مـن آليـات الهجـوم ذات الصلـة بالمرافـق النوويـة، والمنهجيـات المسـتخدمة لتقييـم التهديـدات وتحديدهـا.

تحديد خصائص التهديدات الخاصة بالمرفق

4-46- ينبغـي أن يُجـري المشـغِّل عمليـة لتحديـد خصائـص التهديـدات الخاصـة بالمرفـق وتعهـد تلـك العمليـة لدعـم تقييـم مخاطـر الأمـن الحاسـوبي علـى المرفـق. وينبغـي أن يشـمل ذلـك تحليـلاً لبيـان التهديـد الوطنـي أو التهديـد المحتـاط لـه فـي التصميـم لتحديـد خصائـص التهديـدات الخاصـة بالأمـن النـووي التـي تُسـاهم فـي مخاطـر الأمـن الحاسـوبي للمرفـق. وينبغـي أن يصـف هـذا التحليـل الأهـداف والقـدرات والأسـاليب والتقنيـات المحتملـة للتهديـدات ذات الصلـة، ممـا يُشـكل الأسـاس لصياغـة سياسـة للأمـن الحاسـوبي وبرنامـج للأمـن الحاسـوبي للمرفـق أو التحقـق مـن فعاليـة السياسـة والبرنامـج.

4-47- وينبغي أن يُجري المشغِّل عملية لتحديد خصائص التهديدات في الحالات التالية:

(أ) يجـري المشـغِّل تقييمـاً لمخاطـر الأمـن الحاسـوبي للمرفـق. ويمكـن أن يكـون ذلـك فـي بعـض الأحيـان تحليـلاً أقـل كثافـة للتحقـق مـن التحليـل السـابق والافتراضـات.
(ب) تُصـدر السـلطة المختصـة بيانـاً جديـداً تُحـدد فيـه التهديـد المحتـاط لـه فـي التصميـم أو بيـان تهديـد وطنـي جديـداً.
(ج) يتلقى المشغِّل معلومات يحتمل أن تُبطل الافتراضات الواردة في التحليل الراهن.

4-48- ينبغـي أن يصـف تحديـد خصائـص التهديـدات الـذي يجريـه المشـغِّل المعرفـة والقـدرات والتمويـل، بالإضافـة إلـى الحمـلات والأهـداف والأسـاليب والتقنيـات والإجـراءات المحتملـة للخصـوم المحتمليـن والمحدديـن، وأي سـمات إضافيـة ذات أهميـة خاصـة. وتـرد فـي الفقـرة 5-19 مـن المرجـع [9] قائمـة بالسـمات الإضافيـة المحتملـة لعمليـة تحديـد خصائـص التهديـدات.

4-49- وينبغـي أن تُحـدد عمليـة تحديـد خصائـص التهديـدات التـي يجريهـا المشـغِّل مجموعـة محتملـة مـن الأسـاليب والتقنيـات التـي يمكـن اسـتخدامها فـي الهجـوم، مثـل الإجـراءات المنسـقة التـي تُنفـذ عـن بُعـد أو عـن قـرب، أو اسـتخدام عناصـر داخلية وخصـوم خارجييـن، أو الهجمـات المختلطـة التـي تجمـع بيـن الهجمـات علـى الفضـاء الإلكترونـي والهجمـات الماديـة.

وينبغـي أن تشـمل عمليـة تحديـد خصائـص التهديـدات إمكانيـة شـن هجمـات متتاليـة أو متوازيـة علـى الفضـاء الإلكترونـي تترتـب عليهـا عواقـب تراكميـة، وتشـمل خصمـاً واحـداً أو عـدة خصـوم، فضـلاً عـن الحـالات التـي لا توجـد فيهـا مؤشـرات علـى تواطـؤ بيـن الخصـوم المختلفيـن (هجمـات غيـر تعاونيـة).

4-50- وينبغـي أن تتيـح عمليـة تحديـد خصائـص التهديـدات التـي يجريهـا المشـغِّل إدراج أنـواع الهجمـات ذات المصداقيـة وتقييمهـا. وستُشـكل هـذه القائمـة أسـاس متطلبـات الأمـن الحاسـوبي ومواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة.

4-51- وينبغـي أن تُشـير عمليـة تحديـد خصائـص التهديـدات إلـى مـا إذا كانـت لـدى الخصـم قـدرات تمكنـه مـن تنفيـذ نـوع معيّـن مـن الهجمـات، ومـا إذا كان الخصـم يسـتطيع أن يُعـرِّض للخطـر نظامـاً يـؤدي وظيفـة فـي المرفـق علـى نحـو يجعـل سـلوكه غيـر محـدد (أي خـارج عـن النطـاق المحتـاط لـه فـي التصميـم).

اعتبارات إضافية للتهديدات الداخلية

4-52- ينبغـي أن تشـمل عمليـة تحديـد خصائـص التهديـدات النظـر فـي التهديـدات الداخليـة. وتـرد إرشـادات محـددة فـي المرجـع [6]. وفيمـا يتعلـق بالأمـن الحاسـوبي، يمكـن تصنيـف التهديـدات الداخليـة علـى النحـو التالـي:

(أ) تهديـد داخلـي كامـن: عنصـر داخلـي لديـه الدافـع للتمكيـن مـن ارتـكاب أعمـال ضـارة ولكـن دون الشـروع فيهـا. وقـد تعتمـد تدابيـر الأمـن الحاسـوبي لمواجهـة التهديـد الداخلـي الكامـن علـى تدابيـر وقائيـة، بمـا فـي ذلـك وجـود ثقافـة أمـن قويـة. والتهديـد الداخلـي الكامـن لا تردعـه فـي العـادة تدابيـر الكشـف لأن وصـول العناصـر الداخليـة إلـى المعلومـات والنُظـم أمـر مشـروع، بـل تسـعى هـذه العناصـر الداخليـة، إلـى تجنـب تحديدهـا علـى أنهـا تتصـرف بصـورة ضـارة.

(ب) تهديـد داخلـي نشـط: عنصـر داخلـي لديـه الدافـع للشـروع فـي أعمـال ضـارة. ومـن المحتمـل أن يكـون هنـاك عـدد أقـل مـن التهديـدات الداخليـة النشـطة مقارنـة بالتهديـدات الداخليـة الكامنـة. ويتعيّـن أن تكـون ضوابـط الأمـن الحاسـوبي لمواجهـة التهديـد الداخلـي النشـط أكثـر شـمولاً مـن ضوابـط الأمـن الحاسـوبي الخاصـة بمواجهـة التهديـدات الداخليـة الكامنـة، وينبغـي أن تشـمل تدابيـر حمائيـة، مثـل الفصـل بيـن الواجبـات، وتجزئـة المعلومـات، أو الوصـول المـادي أو امتيـازات النظـام.

(ج) تهديد داخلي عن غير قصد: عنصر داخلي ليس له دافع لارتكاب عمل ضار ولا يُدرك استغلاله من جانب الخصم. ومن ذلك على سبيل المثال أن التهديد الداخلي عن غير قصد في أي هجوم على الفضاء الإلكتروني قد لا يكون على دراية بأن بعض الإجراءات يمكن أن توفر للخصم معلومات أو إمكانية الوصول بصورة رسمية صحيحة، وذلك على سبيل المثال عن طريق النقر فوق رابط ضار في رسالة بريد إلكتروني متنكرة في شكل مصدر موثوق.

4-53- وتختلف مسارات الخصم والجداول الزمنية المرتبطة بالتهديدات الداخلية عن سائر التهديدات بسبب ما يتاح للعناصر الداخلية من إمكانية الوصول بإذن. ويتيح هذا الوصول للعناصر الداخلية، على سبيل المثال، استخدام سلسلة غير مستمرة من المهام التي تُنفذ خلال مدة زمنية ممتدة. وعلى سبيل المثال، يمكن أن تُجمع أوراق الاعتماد الإدارية (إما من خلال الهندسة الاجتماعية أو الإخلال بالنُظم) للتغلب على تدابير مثل ضوابط الوصول أو الفصل بين الواجبات خلال عدة أسابيع أو أشهر أو سنوات.

تحديد متطلبات الأمن الحاسوبي

سياسة الأمن الحاسوبي وبرنامج الأمن الحاسوبي

4-54- تُحدد سياسة الأمن الحاسوبي الخاصة بالمشغِّل[26] الأهداف والمتطلبات الرفيعة المستوى للأمن الحاسوبي في المرفق، مع تطبيق نهج متدرج ودفاع في العمق. ويُحدد المشغِّل هذه المتطلبات الرفيعة المستوى وفقاً للمتطلبات الرقابية المعمول بها، وتُطبق من دون أي استثناءات. وتُمثل سياسة الأمن الحاسوبي أحد المدخلات في عملية إدارة مخاطر الأمن الحاسوبي للمرفق، ويمكن لعملية إدارة مخاطر الأمن الحاسوبي للمرفق أن توسِّع سياسة الأمن الحاسوبي للمرفق وتحسنها.

4-55- ينبغي أن يقوم المشغِّل بوضع وتوثيق برنامجه الخاص بالأمن الحاسوبي[27] كجزء من عملية إدارة مخاطر الأمن الحاسوبي للمرفق. ويُشكل برنامج الأمن الحاسوبي إطاراً لتنفيذ سياسة الأمن الحاسوبي للمرفق التي ستُستخدم طوال عمر المرفق. ويصف القسم 7 محتويات برنامج نموذجي للأمن الحاسوبي، ويشمل مجموعة من متطلبات الأمن

[26] قد تشير بعض المنظمات إلى سياسة الأمن الحاسوبي باسم 'استراتيجية الأمن الحاسوبي'.
[27] قد تشير بعض المنظمات إلى برنامج الأمن الحاسوبي باسم 'خطة الأمن الحاسوبي'.

الحاسوبي المحددة للمرفق، بالإضافة إلى المتطلبات المحددة من خلال نهج قائم على إدراك المخاطر.

4-56- وينبغي أن يقوم المشغِّل بتحديد متطلبات الأمن الحاسوبي في برنامج الأمن الحاسوبي لما يلي، وهو ما يصفه القسم 7 بمزيد من التفصيل:

(أ) الأدوار والمسؤوليات التنظيمية؛
(ب) تقييم المخاطر والثغرات والامتثال؛
(ج) إجراءات الأمن التنظيمية؛
(د) تصميم أمن النُظم وإدارته؛
(هـ) إدارة الأصول وتشكيل الأنساق؛
(و) إدارة الأفراد.

4-57- وينبغي أن يُحدد المشغِّل داخل برنامج الأمن الحاسوبي تدابير الأمن الحاسوبي الأساسية الإلزامية لكل مستوى من مستويات الأمن الحاسوبي. ويرجح أن تتألف هذه التدابير من متطلبات تمثل السياسات والعمليات التنظيمية وستترجم إلى إجراءات.

4-58- وينبغي تحديد وتعريف المتطلبات المتعلقة بقوة تدابير الأمن الحاسوبي لكل مستوى من مستويات الأمن الحاسوبي بما يتسق مع المتطلبات التنظيمية (إن وجدت). ويُحبذ بشدة ألّا تكون هناك أي استثناءات من تطبيق تدابير محددة داخل مستوى الأمن الحاسوبي، وينبغي تبرير أي استثناءات من هذا القبيل وتوثيقها في إطار عملية إدارة مخاطر الأمن الحاسوبي للمرفق.

4-59- وتتمثل المخرجات الرئيسية من مرحلة تحديد المواصفات في إطار عملية إدارة مخاطر الأمن الحاسوبي للمرفق في توثيق برنامج الأمن الحاسوبي (أو برنامج الأمن الحاسوبي المنقح) وتقرير عن الامتثال يُقدم إلى السلطة المختصة ويبين كيفية ضمان تلبية المتطلبات الرقابية من خلال تنفيذ برنامج الأمن الحاسوبي. ويمكن أن تكون وثائق برنامج الأمن الحاسوبي وثيقة واحدة أو مجموعة من الوثائق المنفصلة التي ينبغي أن

تشـمل مـا يلـي:

(أ) بيـان يُشـير إلـى مسـتوى حمايـة الأمـن الحاسـوبي لـكل مسـتوى مـن مسـتويات الأمـن الحاسـوبي. ويمكـن أن يكـون هـذا البيـان نوعيـاً أو كميـاً، ولكـن ينبغـي أن يكـون قابـلاً للتحقـق.

(ب) اشـتراط إجـراء وتوثيـق الاسـتعراضات الدوريـة للأمـن الحاسـوبي وتقييمـات المخاطـر فـي كل مرحلـة مـن مراحـل عمـر المرفـق.

(ج) تحديد للأدوار والمسؤوليات اللازمة لدعم الأمن الحاسوبي.

(د) تحديـد مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة بحيـث تجمـع بيـن متطلبـات الأمـن الحاسـوبي المسـتمدة مـن تطبيـق المشـغّل لنهـج قائـم علـى إدراك المخاطـر وأي متطلبـات يفرضهـا القانـون الوطنـي أو اللوائـح الوطنيـة علـى المرفـق. وينبغـي أن تشـمل مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة مـا يلـي:

'1' متطلبـات تقضـي بتطبيـق نهـج متـدرج (علـى سـبيل المثـال عـدد مسـتويات الأمـن الحاسـوبي)؛

'2' متطلبات الدفاع في العمق؛

'3' أي متطلبـات إضافيـة (علـى سـبيل المثـال، صحـة البيانـات، وعـدم التنصـل، والاقتفائيـة) ضروريـة لتلبيـة المسـتوى الـلازم مـن الحمايـة لـكل مسـتوى مـن مسـتويات الأمـن الحاسـوبي؛

'4' متطلبـات توفِّـر وتحافـظ علـى القـدرة علـى منـع الهجمـات علـى الفضـاء الإلكترونـي وكشـفها وعرقلتهـا والتخفيـف مـن آثارهـا والتعافـي منهـا؛

'5' المتطلبـات المحـددة لتدابيـر الأمـن الحاسـوبي لـكل مسـتوى مـن مسـتويات الأمـن الحاسـوبي التـي سـتُطبق علـى نطاقـات الأمـن الحاسـوبي المعنيـة.

(هـ) سـجل يشـمل السـيناريوهات الوظيفيـة أو طـرق التقييـم الأخـرى المسـتخدمة فـي التحليـل لوضـع المتطلبـات. ومـن المهـم وضـع سـيناريوهات أخـرى مسـتقلة لتوفيـر قـدر أكبـر مـن الضمـان فـي المتطلبـات (أي زيـادة الثقـة). ويـرد فـي الفقـرات مـن 4-116 إلـى 4-122 وصـف أكثـر تفصيـلاً لاسـتخدام السـيناريوهات مـن أجـل زيـادة الثقـة فـي مخرجـات مرحلـة تحديـد المواصفـات.

4-60- وينبغـي أن يُقـدّم المشـغِّل وثائـق برنامـج الأمـن الحاسـوبي لاسـتعراضها مـن جانـب السـلطة المختصـة إلـى جانـب تقريـر الامتثـال.

تخصيص النُظم التي تؤدي وظائف المرفق لمستويات الأمن الحاسوبي

4-61- ينبغي أن تشمل عملية إدارة مخاطر الأمن الحاسوبي للمرفق استخدام قائمة بوظائف المرفق محددة الأولويات ومرتبة حسب أهمية وظيفة المرفق، كأساس لتطبيق نهج متدرج لتوفير أعلى مستوى من ضمان الحماية للوظائف التي لديها أعلى إمكانية للتسبب في أشد العواقب.

4-62- ويهدف نهج مستويات الأمن الحاسوبي إلى تبسيط تطبيق النهج المتدرج. وتحدد مستويات الأمن الحاسوبي مجموعات من متطلبات الأمن الحاسوبي التي تُنفذ لتوفير المستوى المناسب من الحماية للنظام الذي يؤدي وظيفة في المرفق.

4-63- وينبغي أن يحدد المشغِّل عدد مستويات الأمن الحاسوبي التي سيجري استخدامها، مع مراعاة المتطلبات الرقابية الواجبة التطبيق. وعلى سبيل المثال، يمكن أن يختار المشغِّل تطبيق مستوى أمن حاسوبي مختلف لكل وظيفة من وظائف المرفق. ومع ذلك، يزداد تعقيد تطبيق النهج بازدياد عدد مستويات الأمن الحاسوبي. ويتيح الحد من عدد مستويات الأمن الحاسوبي تطبيق نُهج وأساليب مشتركة على نُظم مختلفة. ولذلك، قد يختار المرفق استخدام عدد مستويات أقل. وينبغي الموازنة بين فائدة البساطة في خفض عدد المستويات والتكلفة في الموارد وكفاءة تطبيق تدابير أكثر صرامة على وظائف المرفق مما هو ضروري بصورة مطلقة في جميع الحالات.

4-64- وينبغي أن يضمن المشغِّل تخصيص كل وظيفة من وظائف المرفق لمستوى واحد من مستويات الأمن الحاسوبي.

4-65- وفي بعض الحالات، قد لا تُحدد بالقدر الكافي وظائف المرفق المهمة للأمن أو المرتبطة به للسماح بتمييزها بوضوح عن الوظائف الأخرى. ومن شأن عدم القدرة على الفصل بين وظائف المرفق أن يزيد من التعقيد في تحديد أهمية وظائف المرفق. ولذلك ينبغي أن تكون وظائف المرفق متميزة ومستقلة عن بعضها البعض قدر الإمكان. ويمكن أن ينظر المشغِّل في تعديل وظائف المرفق بهدف تبسيط تطبيق النهج المتدرج، وقد يكون ذلك من جانبه مفيداً أيضاً في تطبيق الدفاع في العمق.

4-66- وينبغي أن يُدرج المشغِّل ما يلي في وثائق برنامج الأمن الحاسوبي:

(أ) عدد مستويات الأمن الحاسوبي ومتطلبات تدابير الأمن الحاسوبي المرتبطة بتلك المستويات؛
(ب) القائمة المرتبة التي تشمل وظائف المرفق وتُشير إلى كيفية تخصيص الوظائف لمستويات الأمن الحاسوبي.

تحديد مواصفات بنية الأمن الحاسوبي الدفاعية

4-67- ينبغي أن يقوم المشغِّل بتصميم وتنفيذ بنية أمن حاسوبي دفاعية تسند فيها لجميع النُظم التي تؤدي وظائف المرفق مستويات أمن حاسوبي، وتتم حمايتها وفقاً لمتطلبات الأمن الحاسوبي المحددة في ذلك المستوى.

4-68- وينبغي أن يحدد المشغِّل تدابير الأمن الحاسوبي الأساسية الإلزامية لكل مستوى من مستويات الأمن الحاسوبي داخل بنية الأمن الحاسوبي الدفاعية. ويمكن أن تشمل التدابير الأساسية تدابير تحكم تقني وإداري ومادي.

4-69- وينبغي تصميم بنية الأمن الحاسوبي الدفاعية لإزالة المسارات المحتملة للهجوم على الفضاء الإلكتروني أو الحد منها (كما هو محدد في تحديد خصائص التهديدات) التي يمكن أن يستغلها الخصم للإخلال بالنُظم التي تؤدي وظائف المرفق. وترد في المرجع [16] تفاصيل عن العمليات المماثلة للحد من المسارات المادية المتاحة للخصم.

4-70- وينبغي وضع حدود للأمن الحاسوبي[28] بين النُظم التي تؤدي وظائف المرفق المختلفة من حيث مستويات أمنها الحاسوبي.

متطلبات في عملية تحديد مواصفات بنية الأمن الحاسوبي الدفاعية لتطبيق نهج متدرج

4-71- ينبغي أن تشمل مواصفات بنية الأمن الحاسوبي الدفاعية متطلبات عامة (بما في ذلك عدد مستويات الأمن الحاسوبي)، وينبغي أن تشمل قوة تدابير كل مستوى

[28] تُعرَّف 'حدود الأمن الحاسوبي' في هذا المنشور بأنها الحدود المنطقية لنظام أو لمجموعة من النُظم داخل مستوى الأمن نفسه، ويمكن بالتالي تأمينها من خلال تطبيق تدابير أمنية مشتركة (مثل نطاقات الأمن الحاسوبي).

مـن مسـتويات الأمـن الحاسـوبي، وقـوة التدابيـر المتخـذة بيـن مختلـف مسـتويات الأمـن الحاسـوبي، وقواعـد الاتصـال بيـن المناطـق فـي مختلـف مسـتويات الأمـن الحاسـوبي.

4-72- وينبغـي أن يضمـن تحديـد مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة تخصيـص وظائـف المرفـق الأعلـى أهميـة لمسـتوى الأمـن الحاسـوبي الأكثـر صرامـة. وينبغـي تحديـد متطلبـات الاتصـالات بيـن النُظـم المخصصـة لمختلـف وظائـف المرفـق. وينبغـي التحكـم فـي تدفـق البيانـات بيـن وظائـف المرفـق المختلفـة مـن حيـث مسـتويات الأمـن الحاسـوبي وفقـاً لنهـج قائـم علـى إدراك المخاطـر.

4-73- وينبغـي أن تضمـن عمليـة تحديـد مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة تقليـل تعقـد النُظـم حيثمـا أمكـن مـن أجـل تبسـيط تنفيـذ تدابيـر الأمـن الحاسـوبي. ويمكـن أن يـؤدي تقليـل تعقـد تدابيـر الأمـن الحاسـوبي إلـى زيـادة الأداء والموثوقيـة.

متطلبات في عملية تحديد مواصفات بنية الأمن الحاسوبي لتطبيق الدفاع في العمق

4-74- وينبغـي أن تشـترط مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة تطبيـق الدفـاع فـي العمـق مـن خـلال طبقـات متتاليـة[29] مـن تدابيـر الأمـن الحاسـوبي التـي يتعيّـن علـى الخصـم التغلـب عليهـا أو تجاوزهـا مـن أجـل الإخـلال بالنُظـم التـي تـؤدي وظائـف المرفـق.

4-75- وينبغـي أن تشـترط مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة وضـع مزيـج مـن تدابيـر التحكـم التقنـي والمـادي والإداري لتوفيـر دفـاع فـي العمـق.

4-76- وينبغـي أن تشـترط مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة تصميمـاً يضمـن ألّا يـؤدي الإخـلال بتدبيـر واحـد مـن تدابيـر الأمـن النـووي أو تعطلـه إلـى عواقـب غيـر مقبولـة.

4-77- وينبغـي أن تشـترط مواصفـات بنيـة الأمـن الحاسـوبي الدفاعيـة اسـتخدام تدابيـر مسـتقلة ومتنوعـة لضمـان أن وجـود ثغـرة مشـتركة لا تتيـح للخصـم الإخـلال بطبقـات الدفـاع فـي العمـق المتعـددة أو تجاوزهـا بأسـلوب تكتيكـي واحـد.

---

[29] يشـير مصطلـح 'الطبقـات' فـي هـذا المنشـور إلـى طبقـات الدفـاع فـي العمـق. وفيمـا يتعلـق بالأمـن الحاسـوبي، يتحقـق ذلـك فـي العـادة مـن خـلال ترتيـب نطاقـات الأمـن الحاسـوبي (بمـا فـي ذلـك تدابيـر الأمـن الحاسـوبي) التـي توضـع وفقـاً لمتطلبـات مسـتويات الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة.

4-78- وينبغي أن تشترط مواصفات بنية الأمن الحاسوبي الدفاعية تطبيق الدفاع في العمق بين الطبقات وداخل كل طبقة. ويمكن أن تستخدم طبقات الدفاع مجموعة من التدابير التي تُطبق على مستويات الأمن الحاسوبي المختلفة وتطبيقها على مختلف نطاقات الأمن الحاسوبي. وفيما يتعلق بالعواقب الأكثر شدة (أي العواقب الإشعاعية الوخيمة بسبب التخريب أو إزالة مواد نووية من الفئة الأولى من دون إذن)، ينبغي تنفيذ تدابير الأمن الحاسوبي في طبقات مستقلة متعددة بهدف توفير سلوك قطعي ومحصن من الأعطال للنُظم في حالة وقوع هجوم على الفضاء الإلكتروني.[30]

4-79- وينبغي دعم عملية تحديد مواصفات بنية الأمن الحاسوبي الدفاعية بتقرير تحليلي لتحديد تدابير الأمن الحاسوبي المحصنة من الأعطال والقطعية في إطار تطبيق الدفاع في العمق. ويمكن أن تطلب السلطة المختصة هذا التقرير لاستعراضه.

الدفاع في العمق بين الطبقات

4-80- ينبغي أن تشترط عملية تحديد مواصفات بنية الأمن الحاسوبي الدفاعية حماية كل طبقة من طبقات الدفاع في العمق من الهجمات على الفضاء الإلكتروني الناشئة في الطبقات المجاورة. وينبغي أن تمنع الطبقات وتدابير الأمن الحاسوبي المرتبطة بها تقدم الهجمات أو تعرقلها.

4-81- وينبغي أن تشترط عملية تحديد مواصفات بنية الأمن الحاسوبي الدفاعية اختيار تدابير الأمن الحاسوبي المستخدمة في طبقة وتشغيلها بطريقة متنوعة ومستقلة عن تدابير الأمن الحاسوبي المستخدمة في طبقة مجاورة من أجل التخفيف من أعطال آليات الحماية المشتركة الأسباب المستخدمة في العزل بين الطبقات. ووفقاً لمبدأ النهج المتدرج، ينبغي أن تكون هذه المتطلبات أكثر صرامة للطبقات التي تتطلب حماية أكثر صرامة (أي المستويين 1 2 من مستويات الأمن الحاسوبي).

الدفاع في العمق داخل الطبقة نفسها

4-82- ينبغي أن تشترط عملية تحديد مواصفات بنية الأمن الحاسوبي الدفاعية استخدام مجموعة من تدابير الأمن الحاسوبي داخل كل طبقة لتقليل احتمالات تمكن إخلال واحد

[30] يعني مصطلح 'آمن من الأعطال' أن يؤدي إخفاق تدبير ما إلى حالة تحافظ على أمن الوظيفة التي يهدف التدبير إلى حمايتها.

مـن التغلـب علـى تدابيـر متعـددة أو تجاوزهـا. ووفقـاً لمبـدأ النهـج المتـدرج، ينبغـي أن تكـون هـذه المتطلبـات أكبـر بالنسـبة للطبقـات التـي تتطلـب حمايـة أكثـر صرامـة (أي المسـتويين 1 و2 مـن مسـتويات الأمـن الحاسـوبي، وتزويـد المسـتوى 1 بأعلـى مسـتوى مـن الحمايـة).

نموذج الثقة

4-83- ينبغـي أن يكـون تطبيـق النهـج المتـدرج والدفـاع فـي العمـق متسـقاً مـع نمـوذج ثقـة قابـل للتطبيـق. وتشـمل نمـاذج الثقـة التـي يمكـن تطبيقهـا مـا يلـي:

(أ) جدارة الموظفين بالثقة (أي الحماية ضد التهديدات الداخلية) [6]؛
(ب) حمايـة المعلومـات الحساسـة (أي السـرية) (علـى سـبيل المثـال نمـوذج بيل-لابـادولا (Bell–LaPadula)[31])؛
(ج) حماية السلامة (أي نموذج بيبا (Biba)، ونموذج كلارك-ويلسون (Clark–Wilson)[32])

العلاقة بإدارة مخاطر الأمن الحاسوبي للنظم - يتم إجراؤها لكل نظام

4-84- وبعـد تحديـد متطلبـات الأمـن الحاسـوبي، يمضـي تنفيـذ هـذه المتطلبـات علـى النحـو الموضـح فـي الشـكل 6 (انظـر أيضـاً الشـكل 7). ويتطلـب تنفيـذ المتطلبـات فهـم الطـرق التـي تـؤدي بهـا الأصـول الرقميـة وظائـف المرفـق.

4-85- وتحـدث تفاعـلات مهمـة بيـن عمليـات إدارة المخاطـر فـي المرفـق وعمليـة إدارة مخاطـر الأمـن الحاسـوبي للنظـم (انظـر الشـكلين 6 و7). وتشـمل إدارة مخاطر الأمن الحاسـوبي للمرفـق تخصيـص واحـدة أو أكثـر مـن وظائـف المرفـق لنُظـم فرديـة وبالتالـي تحديـد النطـاق لـكل عمليـة مـن عمليـات إدارة مخاطـر الأمـن الحاسـوبي لـكل نظـام، ولكـن إدارة مخاطـر الأمـن الحاسـوبي للمرفـق قـد تتأثـر أيضـاً بمخرجـات عمليـة إدارة مخاطـر الأمـن الحاسـوبي

[31] يفـرض نمـوذج بيل-لابـادولا السـرية: لكـي يتمكـن شـخص أو عمليـة مـن الوصـول إلـى المعلومـات، ينبغـي أن تكـون لديهـم حاجـة واضحـة للمعرفـة، وينبغـي أن يـؤذن لهـم بالوصـول إلـى تصنيـف المعلومـات الحساسـة علـى الأقـل.

[32] يحمـي نمـوذج بيبـا ونمـوذج كلارك-ويلسـون سـلامة المعلومـات: يمنـع نمـوذج بيبـا تعديـل البيانات مـن جانـب أطـراف غيـر مـأذون لهـم، ولكنـه لا يمنـع التعديـل مـن دون إذن مـن جانـب الأطـراف المـأذون لهـم (أي الأطـراف الداخليـة)، فـي حيـن يمنـع نمـوذج كلارك-ويلسـون كليهمـا.

للنظـم فـي أي عمليـة تكراريـة. وعلـى سـبيل المثـال، فـي نُظـم الحمايـة الماديـة، يمكـن تخصيـص عـدة وظائـف لنظـام واحـد بسـبب عـدم توافـر نُظـم منفصلـة الوظائـف. ويُقيِّـد ذلـك القـدرة علـى فصـل النظـام إلـى نطاقـات منفصلـة وبالتالـي يجعـل نمـوذج النطـاق مقصـوراً علـى حـدود ماديـة أو حـدود منطقيـة.

4-86- وفيمـا يتعلـق بالمرافـق أو النُظـم القديمـة، قـد لا تكـون هنـاك بعـض الهيـاكل والنُظـم والمكونـات القابلـة للتعديـل أو القابلـة للتغييـر. وقـد يعنـي ذلـك فـي مرحلـة إدارة مخاطـر الأمـن الحاسـوبي للنظـم عـدم إمكانيـة تلبيـة بعـض المتطلبـات المحـددة فـي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق، وقـد يحتـاج المشـغِّل إلـى مراجعـة عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق لتحديـد مواصفـات برنامـج الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة المناسـبة لتلبيـة متطلبـات الأمـان.

4-87- وينبغـي اسـتعراض إدارة مخاطـر الأمـن الحاسـوبي للمرفـق وللنظـام وقـد يتعيَّـن تنقيحهمـا فـي الحـالات التاليـة:

(أ) تنقيح إدارة مخاطر الأمن الحاسوبي للمرفق أو تحليل أمان المرفق.
(ب) عـدم امتثـال النظـام امتثـالاً كامـلاً للمتطلبـات المحـددة فـي مخرجـات عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق.
(ج) إجراء تعديلات للنظام يمكن أن تؤثر على إدارة مخاطر الأمن الحاسوبي للمرفق.
(د) وقوع أحداث أو حادثات أمنية ذات صلة.
(هـ) تحديد تهديدات أو ثغرات جديدة أو متغيرة.

4-88- ويتعيّـن إدراج اسـتعراض إدارة مخاطـر الأمـن الحاسـوبي للمرفـق والنظـام علـى حـد سـواء فـي عمليـة إدارة تغييـرات المرفـق لضمـان اتسـاق كل منهـا مـع الآخـر ومواكبتهـا لآخـر المسـتجدات. وتُسـاعد هـذه التحليـلات أيضـاً فـي وضـع المتطلبـات (علـى سـبيل المثـال، تحديـد مسـتويات الأمـن الحاسـوبي) للنُظـم الجديـدة أو عمليـات التنفيـذ.

4-89- وينبغـي أن تُقيَّـم دوريـاً اتجاهـات الجـولات المتكـررة المتتاليـة فـي عمليـة إدارة مخاطر

الأمـن الحاسـوبي للمرفـق وللنظـام لتحديـد أنـواع الأنمـاط الضـارة التالية:

(أ) مخاطـر تكشـف عـن نمـط واضـح مـن الزيـادة التـي تصـل إلـى عتبـة المخاطـر غيـر المقبولـة أو تتجاوزهـا. وفـي هـذه الحالـة، ينبغـي إيـلاء المراعـاة لسُـبل منـع حـدوث تجـاوز لعتبـة المخاطـر.

(ب) مخاطـر تصـل إلـى العتبـة أو تتجاوزهـا. وفـي هـذه الحالـة، سـيلزم اتخـاذ الإجـراءات المناسـبة (مثـل إبـلاغ السـلطة المختصـة وتنفيـذ تدابيـر تعويضيـة متسـقة مـع الحاجـة الملحـة المحـددة مـن خـلال بيانـات اتجاهـات المخاطـر).

4-90- وينبغـي تحليـل الاتجاهـات المرتبطـة بالنُظـم الفرديـة مـن أجـل ضمـان عـدم تسـبب الاتجـاه فـي إبطـال مخرجـات عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق. وعلـى سـبيل المثـال، يمكـن إجـراء تقييمـات لمراقبـة النُظـم باسـتمرار، ويمكـن بعـد ذلـك الموافقـة بصـورة دوريـة علـى تقاريـر رصـد أداء النُظـم. وينبغـي أن تسـتعرض عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق مخرجـات مـا يقابلهـا مـن إدارة لمخاطـر الأمـن الحاسـوبي للنُظـم مـن أجـل ضمـان عـدم حـدوث أي تغييـر فـي المخاطـر الشـاملة للمرفـق.

أنشطة الضمان

4-91- هناك ثلاثة أنواع من أنشطة الضمان:

(أ) التقييـم الـذي يوفِّـر الثقـة فـي مخرجـات المراحـل التـي يتعـذر فيهـا التحقـق (مثـل تحديـد خصائـص التهديـدات ومراحـل تحديـد مواصفـات متطلبـات الأمـن الحاسـوبي). ونظـراً لطبيعـة المعلومـات التـي تُضـع علـى أساسـها متطلبـات الأمـن الحاسـوبي (علـى سـبيل المثـال، تقديـرات التهديـد والافتراضـات المتعلقـة بأنمـاط إخفـاق وظائـف المرفـق بسـبب تعـرض النُظـم للخطـر)، لا يمكـن للمشـغِّل أن يكـون متأكـداً مـن صحـة المتطلبـات. ولذلـك، يلـزم إجـراء تقييـم لإعطـاء المشـغِّل ثقـة فـي مخرجـات مرحلـة تحديـد مواصفـات متطلبـات الأمـن الحاسـوبي، أي برنامـج الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة.

(ب) التحقـق، الـذي يوفِّـر تأكيـداً بـأن نتائـج مرحلـة مـا تفـي بالأهـداف والمتطلبـات المحـددة لتلـك المرحلـة. وتُنفـذ، حيثمـا أمكـن، أنشـطة التحقـق بيـن المراحـل المتتاليـة لعمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق وللنظـام. ويمكـن أن يشـمل ذلـك عـدداً

مـن الأسـاليب القائمـة علـى الأداء للتحقـق مـن مخرجـات كل مرحلـة قبـل اسـتخدامها كمدخـلات فـي مرحلـة لاحقـة.

(ج) التثبـت، وهـو عمليـة تحديـد مـا إذا كان الأمـن الحاسـوبي للمرفـق يوفِّـر حمايـة مناسـبة ضـد التهديـد (علـى النحـو المحـدد فـي عمليـة تحديـد خصائـص التهديـد) ويتوافـق مـع المتطلبـات الرقابيـة.

التقييم

4-92- ينبغـي أن يقيِّـم المشـغِّل برنامـج الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة للتحقـق مـن أن تنفيذهمـا سـيكون فعـالاً فـي تقليـل فرصـة الخصـوم فـي تقويـض النُظـم التـي تـؤدي وظائـف المرفـق، وتحديـداً مـن خـلال مـا يلـي:

(أ) تحديد وتخصيص الوظائف لمستويات الأمن الحاسوبي؛

(ب) تخصيص تدابير الأمن الحاسوبي لهذه المستويات؛

(ج) مواصفات تدابير الأمن الحاسوبي.

4-93- وينبغـي أن يشـمل تقييـم برنامـج الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة اختبـار الوظائـف والأداء بطريقـة تُلبـي المتطلبـات الرقابيـة. وينبغـي أن يشـمل التقييـم النظـر، حسـب الاقتضـاء، فـي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق وللنظـام علـى حـد سـواء، وكامـل عمـر المرفـق.

4-94- وينبغـي أن ينظـر المشـغِّل فـي الاسـتعانة بخبـراء مسـتقلين لاسـتعراض برنامـج الأمـن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعيـة.

4-95- وينبغـي أن يُبـرر المشـغِّل جميـع الافتراضـات المتعلقـة باحتمـالات حـدوث هجمـات أو نجاحهـا (مثـل الثغـرة والتعـرض والفرصـة) المسـتخدمة فـي التقييـم وينبغـي افتـراض أن الاحتمـال هـو 1 بالنسـبة للسـيناريوهات المفترضـة التـي يمكـن أن تسـفر عـن عواقـب إشـعاعية غيـر مقبولـة[33] أو إزالـة غيـر مـأذون بهـا للمـواد النوويـة (أي تقويـض الأصـول الرقميـة الحساسـة).

[33] ترد في المرجع [8] إرشادات بشأن تعريف العواقب الإشعاعية غير المقبولة.

4-96- ويوفِّر بيان التهديد الوطني أو التهديد المحتاط له في التصميم وتقييم التهديدات الخاصة بالمرفق الأساس الذي يمكن أن يستند إليه المشغِّل في إجراء تحديد لتأكيد الافتراضات التي أُجريت أثناء تخصيص وظائف المرفق لمستوى الأمن الحاسوبي المناسب. ويمكن أن يتيح استخدام سيناريوهات وظيفية ذات مصداقية (الفقرة 4-120 (أ)) بمستوى ضمان أعلى في جودة التقييم (انظر أمثلة السيناريوهات في المرفق الأول).

4-97- وتوفِّر تدابير الأمن الحاسوبي المستندة إلى برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية وظائف الحماية والعرقلة والتصدي من خلال تدابير التحكم المادي (مثل الهيكل)، والتقنية (مثل جدارة الحماية) والإدارية (مثل الأفراد والإجراءات). ومن شأن تفاعل هذه التدابير المتعلقة بالأمن الحاسوبي مع وظائف المرفق المهمة للأمان والأمن والنُظم المخصصة لها أن يجعل تقييم فعالية برنامج الأمن الحاسوبي مهمة صعبة.

4-98- ويتاح عدد من أساليب التقييم، بما في ذلك ما يلي:

(أ) تحليل شجرة الهجوم (يُشار إليه أيضاً باسم 'تحليل متجه الهجوم' و'تحليل الرسم البياني للهجوم'). ويشمل ذلك افتراض مجموعة من المسارات المختلفة الممكنة للخصم لتحديد ما إذا كانت هناك أي ضمانات كبيرة بأن كل هجوم سيكون مآله الإخفاق (أي أن من الممكن منع الخصم من اتباع المسار) أو كشفه والتصدي له قبل وصول الخصم إلى الهدف. ويمكن استخدام تحليل شجرة الهجوم، مع تحديد خصائص التهديد، لتقييم ما إذا كانت التدابير المستندة إلى برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية فعالة في القضاء على احتمالات قيام الخصم بالهجمات المفترضة بنجاح أو القضاء على تلك الاحتمالات.

(ب) يشمل ذلك عمليات محاكاة قائمة على الحاسوب تتناول عناصر برنامج الأمن الحاسوبي (بما في ذلك بنية الأمن الحاسوبي الدفاعية) وتمارين منضدية تتيح النظر في خطط الأمن وخطط الطوارئ وكذلك عملية اتخاذ القرار لدى الخصم والقائمين بالتصدي لحادثات الأمن النووي. وتستخدم هذه الأدوات للحكم على الأداء العام لبرنامج الأمن الحاسوبي، مع مراعاة جميع التدابير. ومن ذلك على سبيل المثال أن التمارين المنضدية قد تساعد في تحديد الفرص المتاحة للخصم على أساس قدراته وخصائصه (على سبيل المثال، ما إذا كان داخلياً) أو الثغرات في الوظيفة.

(ج) التمارين. يمكن أن تشمل اختبارات للأداء على مستوى المرفق وعلى مستوى النُظم (مثل اختبارات الإخلال) وكذلك تمارين محاكاة الاشتباك بين القوات (مثل

الهجمات المختلطة) في الظروف الميدانية أو في ظروف الاختبار. ويمكن أن تتناول هذه التمارين فعالية برنامج الأمن الحاسوبي في توفير الحماية للمرفق برمته أو لأجزاء من المرفق أو مجموعات محددة من النُظم أو مجموعات من التدابير ضد هجوم من الخصم تشمله عملية المحاكاة. وفي هذا النشاط التقييمي، تُجمع بيانات بشأن أداء تدابير الأمن الحاسوبي وتُستخدم لتقييم الفعالية العامة لبرنامج الأمن الحاسوبي.

4-99- ويتم إجراء عمليات المحاكاة والتمارين في العادة كجزء من التحليل القائم على السيناريوهات الذي تُحدد فيه الهجمات المفترضة (السيناريوهات) بالتفصيل وتتم محاكاتها أو استخدامها كأساس للتمارين. ويعتمد التحليل القائم على السيناريوهات في العادة على تحليل شجرة الهجوم من خلال النظر في الأساليب التكتيكية وتقنيات الخصم المحددة للتغلب على تدابير الأمن الحاسوبي.

4-100- ويمكن تقييم فعالية برنامج الأمن الحاسوبي أو بنية الأمن الحاسوبي الدفاعية أو تدابير الأمن الحاسوبي الفردية كمياً أو نوعياً أو كليهما. ويمكن للسلطة المختصة أن تُحدّد أساليب التقييم القطعية التي ستُستخدم مع أنواع مختلفة من الأهداف والتهديدات والسيناريوهات. ويقترح تعريف الفعالية العامة لبرنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية بصورة متحفظة على أنها أدنى فعالية لا تزال تلبي الأهداف الرقابية عند النظر في جميع الأساليب التكتيكية وتقنيات الخصم والسيناريوهات ذات المصداقية.

التحقق

4-101- الهدف من التحقق في هذا السياق هو تقييم جودة المخرجات الناتجة عن مرحلة ما مقابل المواصفات قبل استخدام تلك المخرجات في مرحلة لاحقة.

4-102- وينبغي، حيثما أمكن، إجراء التحقق بين المراحل المتتالية لعملية إدارة مخاطر الأمن الحاسوبي للمرفق أو للنظام.

4-103- وقد تفضي نتائج التحقق إلى اتخاذ المشغِّل الإجراءات التالية:

(أ) معالجة أي قصور في تصميم تدابير الأمن الحاسوبي أو تنفيذها لتلبية المتطلبات؛

(ب) تحديد التحسينات التي قد تكون ضرورية لمعالجة أوجه القصور المحددة وتحسين الأداء وتحليل تلك التحسينات وتنفيذها.

4-104- وقد تشمل أنشطة التحقق أساليب تقييمية، بما فيها التدريبات أو اختبارات الأداء أو المحاكاة أو التحليل (مثل تقييم الثغرات) (انظر الفقرة 4-98).

4-105- وعلى سبيل المثال، يشمل تقييم المخرجات على أساس تحليل شجرة الهجوم النظر في تدفق المعلومات بين النُظم والأجهزة والشبكات والمواقع. ويمكن لتبادل المعلومات بين النُظم أن يسمح للخصوم باستغلال هذه المسارات، ويمكن أن يؤدي إلى تقويض النُظم وبالتالي وظائف المرفق. ويأخذ تحليل شجرة الهجوم أثناء هذه المرحلة في الاعتبار المسارات العامة بهدف التقليل إلى أدنى حد من إمكانية وصول الخصم إلى هذه المسارات أو القضاء على هذه الإمكانية.

4-106- وينبغي أن يستخدم المشغِّل نهجاً متدرجاً عند تحديد مستوى الجهد المطلوب تطبيقه على التحقق والتثبت. وينبغي تطبيق أكبر مستوى من الجهد على الوظائف أو النُظم المخصصة لمستويات الأمن الحاسوبي الأكثر صرامة (أي تلك التي تتطلب أعلى مستوى من الحماية).

4-107- وينبغي تكرار التحقق بانتظام (على سبيل المثال، سنوياً) أو حسب الاقتضاء، لمراعاة أي تغييرات في الأهداف أو في متطلبات برنامج الأمن النووي.

التثبت

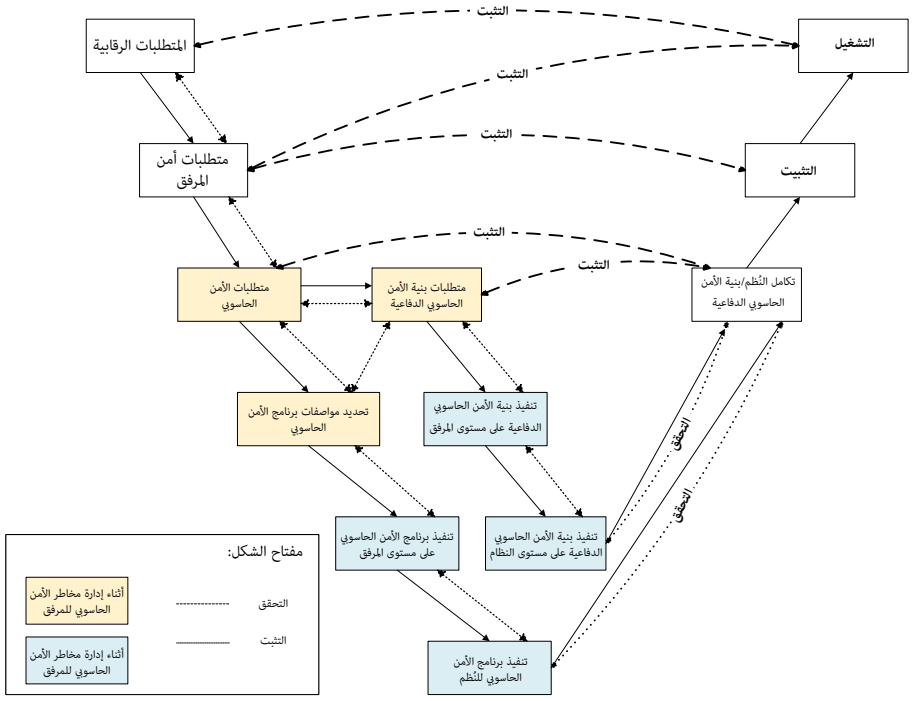
4-108- ينبغي أن يتثبت المشغِّل من أن النُظم، عند إدماجها معاً، تحصل على المستوى المناسب من الحماية لتلبية متطلبات الأمن الحاسوبي على النحو المحدد في برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية. ويوضح الشكل 7 أنشطة التحقق والتثبت في إطار عملية إدارة مخاطر الأمن الحاسوبي، وبرنامج الأمن الحاسوبي، وبنية الأمن الحاسوبي الدفاعية.

4-109- وينبغي أن يتثبت المشغِّل من أن النُظم المثبتة في المرفق تحصل على المستوى المناسب من الحماية التي يوفرها الأمن الحاسوبي لكي تؤدي وظائفها من أجل تلبية المتطلبات على النحو المحدد في متطلبات أمن المرفق.

4-110- وينبغي أن يتثبت المشغِّل من أن مستوى الحماية التي يوفرها الأمن الحاسوبي يكفي لضمان تلبية تشغيل المرفق بالمتطلبات الرقابية أو متطلبات المشغِّل على النحو المحدد في متطلبات أمن المرفق.

4-111- وعندما تُشير عملية التثبت إلى أن مستوى الحماية غير كافٍ، ينبغي أن يُنقح المشغِّل برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية لزيادة الحماية. ويمكن أن يخفض المشغِّل مستوى الحماية من دون موافقة السلطة المختصة.

4-112- وينبغي أن يتثبت المشغِّل من مخرجات عمليتي إدارة مخاطر الأمن الحاسوبي للمرفق وللنُظم. وينبغي التثبت من مخرجات عملية إدارة مخاطر الأمن الحاسوبي للمرفق مقابل متطلبات المشغِّل والمتطلبات الرقابية. وينبغي أن تكون مخرجات عملية إدارة مخاطر الأمن الحاسوبي للنظم متوافقة مع متطلبات برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية.



الشكل -7- لمحة عامة عن أنشطة التحقق والتثبت في عملية إدارة مخاطر الأمن الحاسوبي.

4-113- وينبغي أن يقوم المشغِّل بتجميع مستوى مخاطر المرفق، بما في ذلك الإشارة إلى المتطلبات الرقابية والتصميمية. وينبغي أن يشمل ذلك مستوى مخاطر كل نظام يحتوي على أصول رقمية حساسة.

4-114- وينبغي أن يتثبت المشغِّل من تقييمات المخاطر على مستوى النُظم مقابل بيان التهديد الوطني أو التهديد المحتاط له في التصميم باستخدام سيناريوهات تشمل هجمات تؤثر على نُظم متعددة وعلى البنية العامة. وتختلف هذه السيناريوهات عن السيناريوهات المستخدمة في عملية إدارة مخاطر الأمن الحاسوبي للنُظم (الفقرة 5-5 (ي)) والسيناريوهات المحددة في بيان التهديد الوطني أو التهديد المحتاط له في التصميم. وقد تشمل هجمات مختلطة تنطوي على تقويض لعدد من النُظم المنفصلة بهدف تحديد الثغرات في مكان ما في المرفق.

4-115- وينبغي أن يشمل التثبت الكامل من نتائج إدارة مخاطر الأمن الحاسوبي للمرفق وإدارة مخاطر الأمن الحاسوبي للنُظم النظر في السيناريوهات التقنية والوظيفية على النحو المبيّن أدناه.

تحديد السيناريوهات ووضعها

4-116- ينبغي أن يقوم المشغِّل بتحديد ووضع سيناريوهات على أساس التقييم الذي تجريه الدولة للتهديدات على النحو المبيّن بالتفصيل في بيان التهديد الوطني أو التهديد المحتاط له في التصميم وعند الاقتضاء، تقييم التهديدات الخاصة بالمرفق. ويُشجَّع المشغِّلون بشدة على إشراك الخبراء المتخصصين في الهجمات على الفضاء الإلكتروني وقدرات التهديدات المرتبطة بها في وضع هذه السيناريوهات. ويمكن الحصول على هذه الخبرة من السلطات المختصة ودوائر المعلومات الاستخباراتية ووكالات إنفاذ القانون. وقد يلزم من المشغِّل توفير هذه السيناريوهات المفصلة للسلطة المختصة لاستعراضها وقبولها.

4-117- وقد يوفِّر تحليل السيناريوهات أفكاراً تساعد على فهم النقاط الأكثر ضعفاً داخل المرفق والعمليات وبنية النُظم والإجراءات. وقد يلزم إجراء مزيد من التحليل لتحديد تدابير الأمن الحاسوبي الموضوعة بالفعل أو تدابير الأمن الحاسوبي التي يتعيّن إضافتها لمعالجة الثغرات المحددة.

4-118- وينبغي استخدام السيناريوهات في التحقق من نتائج تقييم مخاطر الأمن الحاسوبي للمرفق، بما في ذلك تحليل الأساليب التكتيكية المحتملة للخصم واحتمالات وقوع هجوم والعواقب المحتملة.

4-119- وينبغي تقييم السيناريوهات دورياً لضمان كفايتها لتلبية أهداف الأمن في ضوء ما يطرأ من تغييرات في التهديدات.

4-120- وهناك فئتان من السيناريوهات:

(أ) السيناريوهات الوظيفية، وهي سيناريوهات تستند إلى تقييمات التهديدات وتُعبِّر عن التأثيرات المحتملة على وظائف المرفق المترتبة عن تفويض النُظم التي تؤدي هذه الوظائف. وتشمل هذه السيناريوهات تلك التي تنطوي على تخريب يسفر عن عواقب إشعاعية غير مقبولة وإزالة غير مأذون بها لمواد نووية. ويمكن أيضاً استخدام السيناريوهات الوظيفية لتحديد التبعيات الحرجة بين الوظائف أو النُظم.

(ب) السيناريوهات التقنية، وهي سيناريوهات تستند إلى التنفيذ التقني المحدد لتدابير الأمن الحاسوبي، وتشمل معلومات مفصلة عن التنفيذ الفعلي أو المحتمل للأصول الرقمية. ويمكن تقييم هذه السيناريوهات من خلال تمارين قائمة على الأداء أو تمارين منضدية، وهي تُشكل في العادة جزءاً من عمليات التحقق والتثبت من مخرجات عملية إدارة مخاطر الأمن الحاسوبي للمرفق وللنُظم.

4-121- وتوضع هذه السيناريوهات ويتم تحليلها بين مراحل عملية إدارة مخاطر الأمن الحاسوبي للمرفق وعملية إدارة مخاطر الأمن الحاسوبي للنُظم، وداخل عناصر عملية إدارة مخاطر الأمن الحاسوبي للمرفق عند الحاجة إليها لأغراض التحليل. وتُعد هذه السيناريوهات ضرورية لزيادة الثقة في مخرجات مرحلة تحديد مواصفات المتطلبات، ولكن يمكن استخدامها أيضاً لوضع هذه المتطلبات. ولا يمكن أن تكون مجموعة السيناريوهات المستخدمة في التحليل لوضع المتطلبات مماثلة لمجموعة السيناريوهات المستخدمة في أنشطة الضمان.

4-122- وينبغي أن تشمل السيناريوهات محل النظر مسارات هجوم متعددة (على سبيل المثال، من خلال شبكات ونُظم محلية مختلفة)، وهجمات تشمل أطرافاً داخلية وهجمات مختلطة. وينبغي أن تشمل أيضاً احتمالات وقوع هجمات متتالية على الفضاء الإلكتروني تضاعف العواقب ولكنها لا تُظهر أي مؤشرات على تواطؤ بين مختلف الخصوم

(هجمات غير تعاونية).

4-123- ويمكن أن تشمل السيناريوهات ما يلي:

(أ) هجمات قائمة بذاتها من جانب خصم واحد؛
(ب) هجمات منسقة من جانب مجموعة من الخصوم يعملون معاً؛
(ج) هجمات انتهازية ينشئ فيها خصوم مستقلون بفعالية هجوماً مشتركاً. ومن ذلك على سبيل المثال، أن ثغرة يكشف عنها خصم واحد، مما يتيح لخصوم آخرين باستهداف نُظم المرفق ومعداته؛
(د) قدرات تهديد محددة [9]؛
(هـ) هجمات مختلطة مصحوبة بعناصر إلكترونية ومادية منسقة؛

ويمكن أن يساعد تحليل شجرة الهجوم على تحديد سيناريوهات التهديد، وكذلك تحديد استراتيجيات الحماية.

4-124- وينبغي استعراض السيناريوهات وتحديثها دورياً في الحالات التالية:

(أ) عند تحديث بيان التهديد الوطني أو التهديد المحتاط له في التصميم؛
(ب) عند إجراء تعديل مهم في المرفق؛
(ج) عند حدوث تغييرات في عمليات الأمن والتدابير المضادة الحرجة والبنية؛
(د) عند تحديد مسارات هجوم ذات مصداقية؛
(هـ) عند إدخال متطلبات رقابية جديدة؛
(و) عند معرفة ثغرات حرجة جديدة[34]، وخاصة الثغرات التي تنطوي على تدابير أمن حاسوبي مهمة؛
(ز) عند حدوث تغييرات في خصائص التهديد.

4-125- وفيما يتعلق بالسيناريوهات الأكثر أهمية، ينبغي تحديد نواقل ومكونات الهجوم المحدد وتوثيق مخاطرها.

[34] على سبيل المثال، يُحدد الإصدار 3 من نظام قياس الثغرات المشتركة التي يمكن استغلالها في الشبكة على أنها 'حرجة' (أي تتراوح درجتها بين 9 و10)؛ وأنها تنطوي على مستوى منخفض من تعقيدات الهجوم؛ وأنها تسفر عن إخلال كامل بالسرية والسلامة والتوافر.

مخرجات إدارة مخاطر الأمن الحاسوبي للمرفق

4-126- ينبغي أن تصف وثائق برنامج الأمن الحاسوبي تدابير الأمن الحاسوبي المطلوبة للحفاظ على الحماية ضد الخصوم الذين شملهم التحليل أثناء التقييم.

4-127- وينبغي أن تشمل عملية إدارة مخاطر الأمن الحاسوبي للمرفق وثائق برنامج الأمن الحاسوبي للمرفق وتحديد مخاطر المرفق المجمعة بناءً على تقييم فعالية التدابير المحددة في برنامج الأمن الحاسوبي على أنها توفِّر الحماية ضد الخصوم الموصوفين في بيان التهديد الوطني أو التهديد المحتاط له في التصميم.

4-128- وينبغي أن يشمل تقرير إدارة مخاطر الأمن الحاسوبي للمرفق استعراضاً رفيع المستوى وتحليلاً لتصميم نظام الأمن وإدارة تشكيل الأنساق على النحو المبيّن بالتفصيل في برنامج الأمن الحاسوبي. وينبغي إجراء تحليل أكثر تفصيلاً أثناء عملية إدارة مخاطر الأمن الحاسوبي للنُظم.

4-129- وينبغي معالجة وظائف المرفق وما يقابلها من نُظم في مخرجات عملية إدارة مخاطر الأمن الحاسوبي للمرفق في تقييمات شاملة للمخاطر على مستوى النُظم كما هو موضح في القسم 5.

4-130- وينبغي تزويد السلطة المختصة بتقييم المشغِّل للمخاطر المرتبطة بمختلف الوظائف ومخاطر المرفق المجمَّعة.

5- إدارة مخاطر الأمن الحاسوبي للنُظم

اعتبارات عامة

5-1- ينبغي أن يضع المشغِّل عملية منهجية وتخضع لاستعراض دوري من أجل إدارة مخاطر الأمن الحاسوبي للأصول الرقمية، بما فيها الأصول الرقمية الحساسة، داخل النُظم

التي تؤدي وظائف المرفق المحددة في عملية إدارة مخاطر الأمن الحاسوبي للمرفق.[35]. وعادة ما يؤدي تقويض الأصول الرقمية الحساسة في العادة إلى عواقب وخيمة جداً أو وخيمة أو متوسطة الشدة (على النحو المبيّن في المرجع [7]). وينبغي أن تشمل عملية إدارة مخاطر الأمن الحاسوبي للمرفق إدارة مخاطر الأمن الحاسوبي لكل نظام على النحو المبيّن في هذا القسم. وينبغي أن تنظر عملية إدارة مخاطر الأمن الحاسوبي للنُظم في جميع الأصول الرقمية داخل النظام، بما فيها الأصول الرقمية الحساسة.

5-2- وينبغي أن يتولى فريق متعدد التخصصات إجراء عملية إدارة مخاطر الأمن الحاسوبي للنُظم على غرار الفريق الذي يتولى إجراء عملية إدارة مخاطر الأمن الحاسوبي للمرفق. ومع ذلك، قد يتم تصميم تكوين فريق إدارة مخاطر الأمن الحاسوبي للنُظم لمعالجة اعتبارات محددة مرتبطة بكل نظام.

5-3- وينبغي أن يستخدم المشغِّل نهج متدرجاً عند تحديد مستوى الجهد الذي سيجري تطبيقه على إدارة المخاطر لكل نظام. وينبغي تطبيق أكبر مستوى من الجهد على النُظم التي تؤدي أو تدعم وظائف المرفق المخصصة لمستويات الأمن الحاسوبي الأكثر صرامة (أي التي تتطلب أكبر مستوى من الحماية) على النحو المحدد في عملية إدارة مخاطر الأمن الحاسوبي للمرفق.

لمحة عامة

5-4- يتمثل الهدف الرئيسي لعملية إدارة مخاطر الأمن الحاسوبي للنُظم في تقييم وإدارة تدابير الأمن الحاسوبي من أجل ضمان توفيرها المستوى المناسب من الحماية للنظام المحدد (أي مستوى الحماية المطلوب لمستوى الأمن الحاسوبي ذي الصلة) وفقاً للمتطلبات المحددة في مخرجات عملية إدارة مخاطر الأمن الحاسوبي للمرفق.

5-5- ولتحقيق هذا الهدف، تشمل عملية إدارة مخاطر الأمن الحاسوبي للنُظم الخطوات

[35] قد يكون من المبرر توسيع نطاق هذا التحليل ليشمل نظماً أخرى مستبعدة من نطاق عملية إدارة مخاطر الأمن الحاسوبي للمرفق ولا تتصل اتصالاً مباشراً بأهداف الأمن النووي.

التاليـة:

(أ) تقييـم كل وظيفـة مـن وظائـف المرفـق، والنُظـم المعيّنـة لأداء الوظيفـة ومسـتوى الأمـن الحاسـوبي المطبـق علـى هـذه النُظـم - مـع مراعـاة وظائـف المرفـق الأخـرى التـي لهـا تفاعـلات وأوجـه ترابـط محـددة فـي مرحلـة تحديـد خصائـص المرفـق فـي إطـار عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق - لتخصيـص الحـدود الوظيفيـة للنُظـم.

(ب) تحديـد نطـاق كل نظـام، بمـا يشـمل النُظـم التـي تدعـم وظائـف المرفـق الأخـرى التـي تتفاعـل مـع الوظيفـة التـي يؤديهـا النظـام وتعتمـد عليهـا. ويمكـن أن يشـمل ذلـك إجـراء تحليـل لبنيـة النظـام الشـاملة لتحديـد المواقـع والحـدود والعلاقـات البينيـة ومسـارات الاتصـال للنُظـم التـي تحتـوي علـى أصـول رقميـة، بمـا فـي ذلـك الأصـول الرقميـة الحساسـة.

(ج) تحديد (وإنشاء قائمة جرد) للأصول الرقمية داخل هذه النُظم.

(د) تحديـد وإنشـاء نطاقـات أمـن حاسـوبي علـى أسـاس المتطلبـات المحـددة فـي برنامـج الأمـن الحاسـوبي للمرفـق وبنيـة الأمـن الحاسـوبي الدفاعيـة.

(هـ) تحديـد الأصـول الرقميـة الحساسـة والأصـول الرقميـة الأخـرى داخـل حـدود النطاقـات مـن خـلال تحليـل الأصـول، وهـو تقييـم للأصـول الرقميـة يُحـدد مـا إذا كانـت تلـك الأصـول حيويـة لأداء وظيفـة المرفـق.

(و) تخصيـص الأصـول الرقميـة، بمـا فيهـا الأصـول الرقميـة الحساسـة، لمسـتوى الأمـن الحاسـوبي المعيّـن فـي مخرجـات برنامـج إدارة الأمـن الحاسـوبي للمرفـق إلـى وظيفـة الأمـن أو الأمـان للمرفـق.

(ز) تطبيـق مسـتوى الأمـن الحاسـوبي الأكثـر صرامـة علـى كامـل النطـاق المخصـص لأي مـن الوظائـف التـي توفرهـا الأصـول الرقميـة داخـل المنطقـة، وتخصيـص جميـع الأصـول الرقميـة داخـل النطـاق لهـذا المسـتوى.

(ح) تطبيـق تدابيـر الأمـن الحاسـوبي الأساسـية (انظـر الفقرتيـن 4-58 و4-68) وتدابيـر الأمـن الحاسـوبي الإضافيـة علـى الأصـول الرقميـة الحساسـة والأصـول الرقميـة الأخـرى (بمـا يشـمل حـدود النطاقـات)، مـع مراعـاة مواصفـات المحـددة لتلبيـة متطلبـات مسـتويات الأمـن الحاسـوبي المعيّنـة.

(ط) توفيـر عمليـة لتحديـد تدابيـر التحكـم التقنـي أو تدابيـر التحكـم الإداري أو تدابيـر التحكـم المـادي التـي يمكـن تطبيقهـا لتنفيـذ تدابيـر الأمـن الحاسـوبي الأساسـية.

(ي) تحليـل طـرق الهجـوم المحـددة والسـيناريوهات والثغـرات للتحقـق مـن فعاليـة تدابيـر الأمـن الحاسـوبي المطبقـة.

(ك) تطبيق تدابير إضافية أو تعويضية لتقليل المخاطر إلى مستوى مقبول إذا أظهر التحليل أن تدابير الأمن الحاسوبي الأساسية لا توفر القدر الكافي من الحماية للنظام.
(ل) وضع تقرير عن إدارة مخاطر الأمن الحاسوبي للنُظم فيما يتعلق بالنظام المحدد.

5-6- ويمكن أن تسفر هذه العملية عن تحديد الأصول الرقمية التي تُشكل جزءاً من النُظم المخصصة لوظائف المرفق أثناء عملية إدارة مخاطر الأمن الحاسوبي للمرفق، أو التي جرى تحديدها على أنها خارجة عن حدود النظام أو النطاق أثناء عملية إدارة مخاطر الأمن الحاسوبي للنُظم. وفي هذه الحالات، ينبغي إجراء تحليل إضافي لضمان إدراج جميع الأصول الرقمية ذات الصلة في التقييم وبرنامج الأمن الحاسوبي.

5-7- وينبغي أن تشمل مخرجات إدارة مخاطر الأمن الحاسوبي للنظم تحديد أولويات المخاطر داخل النظام لتحديد التنفيذ المناسب لتدابير الأمن الحاسوبي. وينبغي أن تشمل العملية النظر في مكان المكونات التي تُشكل النظام، والثغرات، ومستويات الأمن الحاسوبي، والنطاقات، إذا حددت، بالإضافة إلى أهمية الأصول الرقمية الحساسة والأصول الرقمية الأخرى داخل النظام الذي يكون قيد التقييم.

عملية إدارة مخاطر الأمن الحاسوبي للنظم

5-8- ينبغي أن يجري المشغِّل عملية لإدارة مخاطر الأمن الحاسوبي للنظم في الحالات التالية:

(أ) عند إنشاء مرفق لأول مرة (لكل نظام)؛
(ب) عند تعديل المرفق (لكل نظام)؛
(ج) عند نشر نظام جديد أو أصول رقمية جديدة (لكل نظام متأثر)؛
(د) عند تعديل النظام أو الأصول الرقمية (لكل نظام متأثر)؛
(هـ) عند تنقيح عملية إدارة مخاطر الأمن الحاسوبي للمرفق (لكل نظام).

5-9- وينبغي تحديد المدخلات التالية وإتاحتها للاستخدام أثناء عملية إدارة مخاطر

الأمــن الحاســوبي للنظــم:

(أ) مخرجـات عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق (مثـل مواصفـات برنامـج الأمن الحاسـوبي وبنيـة الأمـن الحاسـوبي الدفاعية)؛
(ب) تقرير تحليل الأمان؛
(ج) خطة أمن الموقع؛
(د) سياسة الأمن الحاسوبي.

المتطلبات العامة لبنية الأمن الحاسوبي الدفاعية لأغراض الأمن الحاسوبي

5-10- ينبغـي أن يسـتخدم المشـغِّل متطلبـات بنيـة الأمـن الحاسـوبي الدفاعيـة المحـددة أثنـاء عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق مـن أجـل تصميـم تدابيـر الأمـن الحاسـوبي وتنفيذهـا وتعهدهـا للنُظـم والأصـول الرقميـة مـن أجـل منـع وقـوع هجمـات علـى الفضـاء الإلكترونـي وكشـفها وعرقلتهـا والتخفيـف منهـا والتعافـي منهـا.

5-11- وينبغـي أن تكـون تدابيـر الأمـن الحاسـوبي فعالـة طـوال عمـر المرفـق، وذلـك علـى سـبيل المثـال أثنـاء فتـرات الصيانـة والإخـراج مـن الخدمـة عندمـا يمكـن إدخـال تغييـرات مهمـة علـى شـكل الأنسـاق. وينبغـي ألّا توفـر أنشـطة الرصـد والصيانـة والتعافـي وسـائل يمكـن مـن خلالهـا للخصـم تجـاوز تدابيـر الأمـن الحاسـوبي، مثـل تجـاوز الحمايـة علـى مسـارات الاتصـال بيـن وظائـف المرفـق التـي لهـا مسـتويات مختلفـة مـن الأمـن الحاسـوبي.

5-12- وينبغـي تطبيـق حـدود الأمـن الحاسـوبي[36] بيـن نطاقـات الأمـن الحاسـوبي، وينبغـي حمايتهـا باسـتخدام تدابيـر الأمـن الحاسـوبي المختلفـة.

5-13- وينبغـي التحكـم فـي تدفـق البيانـات بيـن نطاقـات مسـتويات الأمـن الحاسـوبي المختلفـة وبيـن نطاقـات مسـتويات الأمـن الحاسـوبي نفسـها، باسـتخدام نهـج قائـم علـى إدراك المخاطـر، لضمـان اسـتمرار فعاليـة بنيـة الأمـن الحاسـوبي الدفاعيـة.

[36] تُعـرّف "حـدود الأمـن الحاسـوبي" فـي هـذا المنشـور بأنهـا الحـدود المنطقيـة والماديـة لنظـام أو مجموعـة مـن النظـم علـى نفـس مسـتوى الأمـن والتـي يمكـن بالتالـي تأمينهـا مـن خـلال تطبيـق تدابيـر المراقبـة الأمنيـة المشـتركة (أي نطاقـات الأمـن الحاسـوبي).

تحديد حدود النظام

5-14- تُحدد حدود النظام نطاق كل عملية من عمليات إدارة مخاطر الأمن الحاسوبي للنظم وتشمل النُظم المحددة بأنها توفِّر وظيفة معيّنة للمرفق على أساس الخصائص المحددة للمرفق. وينبغي أن يشمل ذلك اعتبارات الترابط بين وظائف المرفق ونُظم تلك الوظائف.

5-15- وينبغي أن تشمل عملية إدارة مخاطر الأمن الحاسوبي للنظم تحديد حدود النظام وتوثيقها. ويشمل ذلك جميع المكونات الرئيسية والمكونات الفرعية والعلاقات البينية والبيئات في النظام المعني أثناء جميع مراحل عمر المرفق، وكذلك ما يتعلق منها بسائر النُظم التي توفر وظائف الدعم أو المساعدة.

5-16- ويمكن استخدام الخطوات التالية لتحديد حدود النظام قيد التقييم:

(أ) تحديد جميع العلاقات البينية للنظام.

(ب) تحديد جميع النقاط التي تدخل فيها البيانات إلى النظام وتخرج منه (النقاط التي قد يحاول فيها الخصم إدخال تعليمات برامجية ضارة). وينبغي مراعاة أي وسيلة لحقن تعليمات برمجية ضارة في النظام أثناء تقييم مخاطر الأمن الحاسوبي للنظام. وعلى سبيل المثال، يمكن حقن التعليمات البرمجية الضارة من خلال وصلات الاتصال، أو المنتجات والخدمات المورَّدة، أو الأجهزة المحمولة التي تكون متصلة بصفة مؤقتة بالمعدات المستهدفة.

(ج) تحديد الإجراءات التي تنطوي على تفاعل مع النظام في ظروف التشغيل العادي والظروف المحددة (مثل إدخال تصحيحات).

(د) تحديد مسارات البيانات (إن وجدت) التي لا تستخدمها أي إجراءات أثناء تشغيل النظام وصيانته. وتمثل مسارات البيانات غير المستخدمة ثغرة مهمة.

(هـ) تحديد مستوى الأمن الحاسوبي المعيّن للنظام (من خلال مخرجات عملية إدارة مخاطر الأمن الحاسوبي للمرفق).

(و) إعداد قائمة بتدابير الأمن الحاسوبي المطبقة على النظام أو بيئته.

تعريف نطاقات الأمن الحاسوبي وإنشاؤها

5-17- تفرض مواصفات برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية التي يتم إعدادها أثناء عملية إدارة مخاطر الأمن الحاسوبي للمرفق متطلبات للأمن الحاسوبي على تنفيذ نموذج النطاقات. وسيشمل برنامج الأمن الحاسوبي أيضاً قائمة بوظائف المرفق والنُظم المخصصة لها.

5-18- وينبغي أن يُنفذ المشغِّل تدابير الأمن الحاسوبي لتلبية المتطلبات المحددة في مواصفات بنية الأمن الحاسوبي الدفاعية. وينبغي عند القيام بذلك إيلاء المراعاة أيضاً لتحقيق ما يلي [8]:

(أ) تُشكل النُظم التي تنتمي إلى النطاق نفسه مساحة موثوقة للاتصالات الداخلية بين هذه النُظم، ويمثل مستوى الأمن الحاسوبي المطبق في كامل النطاق الذي يحتوي على مساحة موثوقة المستوى الأكثر صرامة بين المستويات المعيّنة للنُظم المعنية.

(ب) الحفاظ على متطلبات بنية الأمان (على سبيل المثال، الاستحاطة، والتنوع، والفصل المادي والكهربائي، ومعيار العطل المفرد).

(ج) تطبيق الدفاع في العمق سواءً داخل كل نطاق من نطاقات الأمن الحاسوبي (عن طريق استخدام تدابير تحكم إداري ومادي وتقني متنوعة ومستقلة ومتداخلة) وبين نطاقات الأمن الحاسوبي.

(د) تدابير التحكم التقني لتوفير إجراءات للوقاية والحماية (أي إجراءات لا تتطلب أي تدخل بشري) لتكميل تدابير التحكم المادي أو الإداري (أي تتطلب تدخلاً بشرياً) عند الاقتضاء.

(ه) تزويد جميع الوصلات بين النطاقات بآليات فصل لتدفق البيانات بحيث تعمل وفقاً للقواعد التي تعتمد على النطاقات لمنع الوصول من دون إذن والتفاعلات غير المرغوبة بين النطاقات. ويشمل ذلك الوصلات الشبكية المستمرة والوصلات المتقطعة، وذلك على سبيل المثال باستخدام وسائط تخزين قابلة للنقل.

(و) اعتماد مستوى الفصل بين النطاقات على مستويات الأمن الحاسوبي في المنطقتين. وتشمل تدابير الفصل تدابير التحكم التقني، مثل مرشحات الرُزم، وجدران الحماية، وصمامات البيانات، عند حدود النطاق لتقييد تدفق البيانات والاتصال بين النطاقات المختلفة.

(ز) اتباع الاتصالات المسموح بها بين النطاقات عند مستويات الأمن المختلفة المتطلبات المحددة للمستويات المعنية في برنامج الأمن الحاسوبي. ويمكن أن يشمل وضع المتطلبات للاتصالات المسموح بها النظر في نماذج الثقة (انظر الفقرة 4-83).

(ح) إذا كانت المتطلبات المحددة في برنامج الأمن الحاسوبي تسمح باتصالات بين الأصول الرقمية الحساسة في النطاقات المعيّنة لمستويات أمن مختلفة، لا يُسمح بالتوصيل إلّا بواسطة أصل من الأصول الرقمية الحساسة المخصصة لمستوى أمن حاسوبي أعلى (أكثر صرامة). ولا تسمح الأصول الرقمية الحساسة التي تؤدي وظائف إدارة معلومات حساسة في العادة بحدوث اتصال من مستويات أعلى إلى مستويات أدنى (أي تدفقات المعلومات في الاتجاه العكسي)، وفقاً لنموذج الثقة بيل-لابادولا (انظر الفقرة 4-83).

(ط) إذا كان الاتصال الذي يبدأه أصل رقمي حساس خاضع لمستوى أمن حاسوبي أدنى[37] أمراً لا مفر منه ويُشكل انتهاكاً لنموذج الثقة الخاص به، تُستخدم آليات فصل صارمة بصفة استثنائية.

(ي) يُعامل الوصول المنطقي أو المادي إلى الأصول الرقمية في نطاق ما بواسطة الأجهزة المحمولة المسموح بها أو غيرها من المعدات المؤقتة باعتباره شكلاً من أشكال الاتصال المتقطع بهذا النطاق، ويخضع لتدابير الأمن الحاسوبي الخاصة بالنطاق المحدد والأجهزة المتصلة مؤقتاً. وتخضع هذه الأجهزة لتدابير أمن حاسوبي إضافية عندما تتصل بأكثر من نطاق.

(ك) يمكن تقسيم النطاقات إلى نطاقات فرعية لتحسين نسق المكونات ولمنع التفاعلات غير المرغوبة مع النُظم الأخرى.

5-19- وينبغي النظر في فصل الأصول الرقمية إلى نطاقات متميزة عند استيفاء أيٍ من الشروط التالية:

(أ) انتماء الأصول الرقمية إلى نُظم تؤدي وظائف مختلفة في المرفق.

(ب) تخصيص مستويات مختلفة من الأمن الحاسوبي للنُظم التي تُساهم في وظيفة المرفق نفسها.

---

[37] لا تسمح بعض الدول الأعضاء بهذا الاتجاه للاتصالات من المستويات الأدنى إلى المستويات الأعلى في المرافق التي تنطوي على عواقب وخيمة أو وخيمة جداً. وفي سائر أنواع المرافق (مثل مرافق دورة الوقود النووي، والمفاعلات النمطية الصغيرة)، يمكن للسلطة المختصة أن تسمح للمشغِّل بسلطة تقديرية في تطبيق المسارات الثنائية الاتجاه.

(ج) إدارة النُظم التي تُساهم في وظيفة المرفق نفسها ومستوى الأمن الحاسوبي نفسه من خلال وحدات تنظيمية مختلفة.

(د) اتصال الخوادم مع عملاء متعددين (مثل تلك المستخدمة مع نُظم التحكم الموزعة وأجهزة التحكم المنطقي القابل للبرمجة). وينبغي أن يحتوي النطاق الذي يتطلب الحماية الأكثر صرامة على الحد الأدنى الممكن من الأصول الفريدة.

(هـ) حاجة النُظم إلى الاتصال بمكونات البنية الأساسية المشتركة التي تستخدمها نُظم متعددة (مثل خدمات الدليل، وخوادم الوقت، ووحدات جميع سجلات الأمن) ولكن ليس مع بعضها البعض. وينبغي إجراء رصد ومراقبة للاتصالات بين النطاقات التي تحتوي على هذه الأنواع من النُظم والنطاقات التي تحتوي على مكونات البنية التحتية المشتركة.

(و) الحالات التي تكون فيها النُظم مخصصة للإدارة (ولا سيما عند استخدام النُظم نفسها لإدارة العديد من النُظم الوظيفية).

(ز) اشتراط اللوائح وجود نطاقات متميزة.

5-20- ويمكن النظر في تخصيص الأصول الرقمية لنطاقات مختلفة، على الرغم من تخصيصها لمستوى الأمن الحاسوبي نفسه، في الحالات التالية:

(أ) الأصول الرقمية موجودة في نُظم تؤدي وظائف مختلفة في المرفق. وفي هذه الحالات، يمكن أن يؤدي تخصيص الأصول الرقمية لنطاقات مختلفة إلى تحسين الفصل بين النطاقات والنُظم التي تُساهم في وظيفة المرفق.

(ب) الوحدات التنظيمية المختلفة مسؤولة عن أصول رقمية مختلفة.

(ج) وجود أصول رقمية معزولة، أو استضافة العديد من الأصول الرقمية لنفس النظام الوظيفي على شبكة معزولة.

(د) ضرورة تخصيص نُظم منفصلة احتياطية تؤدي نفس وظيفة المرفق لنطاقات فردية.

(هـ) تتطلب اللوائح فصل الأصول الرقمية.

5-21- وينبغي أن تقتصر وصلات الشبكة والتبادلات المحلية (على سبيل المثال عبر وسائط التخزين القابلة للنقل أو الأجهزة المحمولة) للبيانات بين النُظم في نطاقات مختلفة على تلك الضرورية فقط. وعندما تكون وصلات الشبكة عبر حدود النطاق ضرورية، ينبغي إنشاؤها من نطاق الأمن الحاسوبي الأعلى إلى نطاق الأمن الحاسوبي الأدنى. ويمكن تطبيق قيود باستخدام تدابير التحكم التقنية (مثل أجهزة الترشيح) أو تدابير التحكم الإداري (مثل قواعد استخدام وسائط التخزين القابلة للنقل على نظام محدد).

وينبغي توثيق وصلات الشبكة والأساليب المسموح باستخدامها في تبادل البيانات غير المتصل.

5-22- ولا يمكن أن يشمل نطاق معين سوى النُظم (والأصول الرقمية) من نفس مستوى الأمن الحاسوبي. ويُخصص للنطاق مستوى الأمن الحاسوبي المخصص للنُظم الواقعة داخل النطاق. ويمكن، بل وينبغي، تطبيق مستوى أمن حاسوبي معيّن على نطاقات مختلفة. ومع ذلك، قد يكون من الصعب في بعض الحالات فصل النُظم المخصصة لمستويات أمن حاسوبي مختلفة إلى نطاقات مختلفة. وفي هذه الحالات، يمكن أن تصبح بعض النُظم جزءاً من منطقة أُسند إليها مستوى أمن حاسوبي أكثر صرامة من احتياجاتها.

5-23- وينبغي السماح بالاتصالات فقط بين النطاقات من نفس مستوى الأمن الحاسوبي أو مستويات الأمن الحاسوبي المجاورة. وينبغي أن تقتصر الوصلات بين النطاقات التي لها مستويات أمن حاسوبي مختلفة على نقاط دخول نطاقات محددة (على سبيل المثال، نقطة دخول واحدة لترشيح الوصلات بين النطاقات التي يخصص لها المستوى 2 من مستويات الأمن الحاسوبي والنطاقات التي يخصص لها المستوى 3 من مستويات الأمن الحاسوبي). وينبغي تحديد تدابير الأمن لجميع نقاط الدخول بطريقة متسمة بالكفاءة ومتسقة لإنفاذ بنية أمن شاملة. وينبغي تطبيق عمليات تحقق محددة عند نقطة دخول منطقة ما، وذلك على سبيل المثال على محتوى البيانات (مثل النطاقات المقبولة لقيم البارامترات) الداخلة أو الخارجة، أو التوقيع الرقمي للبيانات.

تحديد الأصول الرقمية

5-24- ينبغي الرجوع إلى السجلات التالية عند تحديد الأصول الرقمية للنظام:

(أ) قاعدة بيانات أصول النظام (لجميع المكونات الرقمية)؛
(ب) قائمة جرد البرامجيات الحاسوبية والبرامج الثابتة؛
(ج) قوائم المعلومات الحساسة ذات الصلة بالنظام [5]؛
(د) شبكة النظام والمخططات البيانية للبنية؛
(هـ) وثائق تصميم المرفق، مثل تقرير تحليل الأمان أو تقارير الاختبار؛
(و) المخططات البيانية لتدفق البيانات؛
(ز) قائمة حسابات وامتيازات المستخدمين والنُظم؛
(ح) الإجراءات المرتبطة بالنظام المحدد.

5-25- ويمكـن أن تشـمل قائمـة الأصـول الرقميـة محدداتهـا، والمواصفـات والبيانـات التقنيـة الرئيسـية، وعلاقاتهـا البينيـة، والإشـارات إلـى تقييمـات المخاطـر علـى مسـتوى المرفـق وعلـى مسـتوى النُظـم، والكيانـات المسـؤولة عنهـا.

5-26- وينبغـي الاحتفـاظ بقائمـة الأصـول الرقميـة طـوال عمـر المرفـق وينبغـي اسـتعراضها دورياً. وينبغـي أيضـاً اسـتعراض القائمـة وتحديثهـا عنـد الضـرورة كلمـا أُجـري تقييـم للمخاطـر علـى مسـتوى النظـام.

5-27- وينبغـي أن تعامـل كأصـول رقميـة حساسـة كل الأصـول الرقميـة التـي تكـون أيضـاً أصـول معلومـات حساسـة. وينبغـي أيضـاً تحديـد الأصـول الرقميـة التـي قـد تُسـهِّل أو قـد تُسـاهم فـي إحـداث تأثيـر ضـار علـى وظيفـة الأصـول الرقميـة الحساسـة ومراعاتهـا فـي تحليـل الأصـول الرقميـة لتحديـد مـا إذا كان ينبغـي تعيينهـا كأصـول رقميـة حساسـة وفقـاً لبرنامـج الأمـن الحاسـوبي.

5-28- وينبغـي تصنيـف قائمـة الأصـول الرقميـة الحساسـة باعتبارهـا معلومـات حساسـة وينبغـي حمايتهـا.

بنية الأمن الحاسوبي للنُظم، بما في ذلك تحليل الأصول الرقمية

5-29- ينبغـي أن يُحـدد المشـغِّل المهـام والأنشـطة الرئيسـية الضروريـة لتوفيـر الأمـن الحاسـوبي للمرفـق. وينبغـي أن تكـون هـذه المهـام والأنشـطة مرتبطـة بمسـتويات الأمـن الحاسـوبي وتدابيـر الأمـن الحاسـوبي المقابلـة. وينبغـي أن يضمـن المشـغِّل توافـر المـوارد والقـدرات الضروريـة لأداء هـذه المهـام والأنشـطة.

5-30- وينبغـي أن تُحـدد عمليـة إدارة مخاطـر الأمـن الحاسـوبي للنظـم جميـع الأصـول الرقميـة الحساسـة. وقـد يتعيّـن أيضـاً مراعـاة الأصـول الرقميـة التـي ليسـت أصـولاً رقميـة حساسـة عنـد تحليـل تهديـدات محـددة أو أنـواع محـددة مـن الهجمـات إذا كان الإخـلال بهـا يمكـن أن يؤثـر تأثيـراً ضـاراً علـى أحـد الأصـول الرقميـة الحساسـة. وينبغـي أن يكـون مسـتوى الجهـد المرتبـط بتقييـم المخاطـر علـى مسـتوى النظـام متدرجـاً لضمـان أن النُظـم التـي يُخصـص لهـا أعلـى مسـتوى مـن الأمـن الحاسـوبي تخضـع أيضـاً لأدق تقييـم.

5-31- وبصفـة عامـة، ينبغـي أن يُخصـص مسـتوى الأمـن الحاسـوبي نفسـه للنُظـم التـي تـؤدي

الوظيفة نفسها في المرفق، بما في ذلك النُظم المستقلة والمتنوعة والاحتياطية. ولا يُنصح بشدة بتخصيص مستوى أمن حاسوبي أقل صرامة لأي من هذه النُظم، ولا يمكن النظر فيه إلاّ على أساس كل حالة على حدة إذا كان ذلك يؤيده تبرير محدد وتحليل للمخاطر الأمنية.

5-32- وينبغي أن يشمل تحليل الأصول الرقمية الحساسة النظر في المعلومات المتعلقة بالبرامج الثابتة والبرامجيات الحاسوبية للأصول الرقمية الحساسة التي يمكن استخدامها كمدخلات في تحليل الثغرات. ويمكن أن يؤدي تحليل الثغرات إلى التوصية باتخاذ إجراءات لتحديد خدمات أو منافذ أو علاقات بينية غير مطلوبة في النظام (أو الشبكة) للأصول الرقمية الحساسة أو تعطيلها أو إزالتها للحد من مساحة الهجوم (أي تقوية النظام؛ انظر الفقرة 64 من التذييل).

5-33- وينبغي تحليل الواجهات البينية لكل نظام (بما في ذلك أصوله الرقمية) وتصنيفها من حيث حدود النطاق. ويمكن استخدام الفئات التالية:

(أ) الاتصالات الداخلية الموثوقة: تشمل هذه الفئة الاتصالات داخل النُظم وفيما بينها أو داخل نطاق أو بين الأصول الرقمية داخل النظام، بما في ذلك المسارات الداخلية إلى الأجهزة عند حدود النطاق (مثل جدران الحماية، وصمامات البيانات). ولا توجد أي تدابير للأمن الحاسوبي يمكنها رصد أو حماية مسارات الاتصالات الداخلية الموثوقة بصورة فعالة ضد الهجمات على الفضاء الإلكتروني.

(ب) الاتصالات الخارجية المأذون بها: تشمل هذه الفئة الوصلات بين النطاقات من خلال المسارات المسموحة المأذون بها والأجهزة الحدودية. وتجري هذه الاتصالات في العادة بين نُظم منفصلة تؤدي وظائف مختلفة في المرفق. وتضمن تدابير الأمن الحاسوبي في شكل أجهزة حدودية رصد جميع مسارات الاتصالات، سواء كانت رقمية أو تناظرية، باستمرار، ولا يمكن استخدام سوى تلك المأذون بها.

(ج) الاتصالات المحتملة غير المأذون بها: تشمل هذه الفئة القدرة على إنشاء وصلات غير مأذون بها بين النطاقات، وذلك على سبيل المثال باستخدام كابلات الشبكة أو الوصلات اللاسلكية أو وسائط التخزين القابلة للنقل ويمكن إنشاء هذه المسارات غير المأذون بها بين النُظم أو الأصول الرقمية الموجودة في نطاقات مختلفة ولكنها في القرب المادي أو المنطقي، على سبيل المثال النُظم الموجودة فعلياً في المنطقة نفسها من دون وجود حواجز مادية تتحكم في الوصول فيما بينها.

5-34- وينبغـي أن يُخصـص لجميـع الأصـول الرقميـة التـي لهـا مسـارات اتصـالات داخليـة موثوقـة داخـل نطـاق مـا المسـتوى نفسـه مـن الأمـن الحاسـوبي، أي المسـتوى المحـدد للنطـاق.

5-35- وينبغـي تخصيـص أجهـزة حـدود النطـاق لمسـتوى أمـن حاسـوبي يعـادل المسـتوى الأعلـى (الأكثـر صرامـة) المطبـق علـى المعـدات التـي تهـدف هـذه الأجهـزة إلـى توفيـر الحمايـة لهـا. ومـن ذلـك علـى سـبيل المثـال أن جـدار الحمايـة بيـن منطقتيـن مختلفتيـن مـن حيـث مسـتوى الأمـن الحاسـوبي قـد يكـون لـه مسـار اتصـال داخلـي موثـوق مـع المنطقـة التـي يُخصـص لهـا أعلـى مسـتوى مـن مسـتويات الأمـن الحاسـوبي، ولكـن لا يكـون لـه سـوى مسـار اتصـال خارجـي مـأذون بـه مـع المنطقـة الأخـرى.

5-36- ومـن الأمثلـة الأخـرى علـى أجهـزة حـدود النطـاق محطـة كشـف البرامجيـات الضـارة، أو الماسـح المضـاد للفيروسـات، الـذي يُسـتخدم لمسـح وسـائط التخزيـن القابلـة للنقـل والأجهـزة المحمولـة قبـل الدخـول إلـى النطـاق والخـروج منـه. ويُخصـص لمحطـة كشـف البرامجيـات الضـارة أعلـى مسـتوى مـن الأمـن الحاسـوبي المطبـق علـى أي شـيء فـي النطـاق التـي تهـدف إلـى توفيـر الحمايـة لـه.[38] وفـي هـذه الحالـة، يتعيّـن علـى المشـغِّل أن يضمـن أن المحطـة لا توفِّـر طريقـاً مشـتركاً للإخـلال بالنُظـم المختلفـة فـي النطاقـات المختلفـة (علـى سـبيل المثـال، إيجـاد ثغـرة مشـتركة يمكـن اسـتغلالها للإخـلال بالنُظـم المختلفـة).

5-37- وينبغـي أن تتوافـق جميـع الأصـول الرقميـة، بمـا فيهـا الأصـول الرقميـة الحساسـة، المتصلـة عبـر مسـار اتصـال داخلـي موثـوق، مـع المتطلبـات العامـة لبنيـة الأمـن الحاسـوبي الدفاعيـة. وتحتـاج الاتصـالات الخارجيـة المسـموح بهـا إلـى تدابيـر أمـن حاسـوبي إضافيـة (انظـر الفقـرة 5-33 (ب)).

5-38- وقـد يُسـمح للأصـول الرقميـة الحساسـة أن تكـون علـى مقربـة (منطقيـة أو ماديـة) مـن أصـول رقميـة حساسـة أخـرى، بشـرط وجـود تدابيـر أمـن حاسـوبي لضمـان عـدم تفاعـل هـذه النُظـم مـن خـلال مسـارات اتصـالات محتملـة غيـر مـأذون بهـا. وقـد تكـون هـذه التدابير مجـرد تدابيـر تحكـم إداري. وتُسـند فـي العـادة للأصـول الرقميـة الحساسـة أعلـى مسـتويات

[38] قـد تكـون هـذه المحطـات غيـر مناسـبة لحمايـة النُظـم المشـمولة بالمسـتوى 1 أو المسـتوى 2 بسـبب الصعوبـات فـي تطبيـق متطلبـات الأمـن الحاسـوبي علـى محطـة قائمـة بذاتهـا. وبالإضافـة إلـى ذلـك، لا يمكـن لمحطـات كشـف البرامجيـات الضـارة المعتمـدة فقـط علـى 'القائمـة السـوداء' أو نُهـج التوقيـع، توفيـر مسـتوى عـال مـن الحمايـة.

الأمـن الحاسـوبي (علـى سـبيل المثـال، المسـتويات مـن 1 إلـى 3).

5-39- وينبغـي ألّا يُسـمح للأصـول الرقميـة غيـر المـأذون لهـا بالاتصـال بالأصـول الرقميـة الحساسـة بـأن تكـون علـى مقربـة منطقيـة أو ماديـة مـن الأصـول الرقميـة الحساسـة فـي الحـالات التـي مـن المحتمـل أن توجـد فيهـا مسـارات اتصـال غيـر مـأذون بهـا. وينبغـي أن تنص بنيـة الأمـن الحاسـوبي الدفاعيـة علـى وضـع تدابيـر أمـن حاسـوبي قويـة وتعهدهـا للتخلـص مـن هـذه المسـارات أو إنشـاء تدابيـر تعويضيـة لتقليـل إمكانيـة اسـتخدام تلـك المسـارات.

5-40- وينبغـي ألّا تكـون الأصـول الرقميـة غيـر المعيّنـة (أي التـي لـم يُخصـص لهـا مسـتوى أمـن حاسـوبي) قريبـة بـأي حـال مـن الأحـوال مـن الأصـول الرقميـة الحساسـة. ومـن ذلـك علـى سـبيل المثـال، ينبغـي التعامـل مـع معـدات البائـع أو الأجهـزة المحمولـة الشـخصية التـي لـم تُقيَّـم ولـم يتـم تعيينهـا، علـى أنهـا أجهـزة يُحتمـل أن تكـون ضـارة لأداء الأصـول الرقميـة الحساسـة، وينبغـي عـدم السـماح لهـا بـأن تكـون علـى مقربـة منطقيـة أو ماديـة مـن الأصـول الرقميـة الحساسـة للمرفـق.

5-41- وينبغـي أن يشـمل تحليـل الأصـول تقييـم تأثيـرات السـيناريوهات ذات المصداقيـة بشـأن الهجـوم علـى الفضـاء الإلكترونـي التـي يتعـرض لهـا النظـام والمخاطـر التـي يتعـرض لهـا المرفـق. وينبغـي أن يأخـذ التقييـم فـي الاعتبـار احتمـالات حـدوث هجمـات علـى الفضـاء الإلكترونـي خـلال أي مرحلـة مـن مراحـل عمـر المرفـق أو أي مرحلـة مـن دورة حيـاة النظـام.

5-42- وقـد تؤثـر الهجمـات ضـد الفضـاء الإلكترونـي علـى نظـام منفـرد أو علـى نُظـم متعـددة، ويمكـن اسـتخدامها بالاقتـران مـع أشـكال أخـرى مـن الأعمـال الضـارة التـي تسـبب أضـراراً ماديـة. وينبغـي أن يشـمل تقريـر التقييـم قائمـة بهـذه التفاعـلات المحتملـة علـى مسـتوى المكونـات وينبغـي تقييمهـا.

5-43- وينبغـي أن يشـمل التقييـم النظـر فـي الإجـراءات الضـارة التـي يمكـن أن تغيُّـر إشـارات العمليـات، وبيانـات نسـق المعـدات أو البرامجيـات الحاسـوبية.

5-44- وينبغـي أن يشـمل تحليـل الأصـول تحديـد المواقـع التـي تُخـزّن فيهـا المعلومـات، ومسـارات تدفقـات المعلومـات داخـل النظـام (بمـا فـي ذلـك أصولـه الرقميـة). وينبغـي أن يُحـدد التحليـل أيضـاً التدابيـر المتخـذة لحمايـة تدفقـات البيانـات والاتصـالات الضروريـة ون يبررهـأن يبررهـا، وينبغـي أن يحـدد أي ثغـرات متبقيـة ممكنـة. ويمكـن دعـم التحليـل بمـا

يلـي:

(أ) تحليل تدابير الأمن أو اختبارها؛
(ب) توثيق حالة التدابير، بما في ذلك تحديد نقاط التحسين الممكنة؛
(ج) فيما يتعلق بالنُظم المحددة، ضمان إخضاع البرامجيات الحاسوبية لتقييم يتناول الثغرات.

5-45- ومن ذلك على سبيل المثال، ينبغي أن يؤخذ في الاعتبار تبادل البرامجيات الحاسوبية (على سبيل المثال رمز المصدر، ورمز الهدف) بين البيئة التطويرية ونظام الأمن. وفي حال عدم اتخاذ أي تدابير للأمن الحاسوبي، يُخصص النظام في هذه الحالة (الأجهزة والبرامجيات الحاسوبية) للنطاق نفسه (ومستوى الأمن الحاسوبي) المحددين لنظام الأمن نفسه، نظراً لعدم وجود أي حدود. ومع ذلك، في حال تطبيق تدابير الأمن على الحدود بين أداة البرمجة والنظام - على سبيل المثال، اختبار سلامة البيانات وتحديد أي ثغرات في الرمز الناتجة عن أداة البرمجة - يمكن وضع أداة البرمجة في نطاق منفصل وتخصيصها لمستوى أمن حاسوبي مختلف عن المستوى المخصصة للنظام نفسه. وتُستخدم التدابير المطبقة على مخرجات أداة البرمجة لحماية النظام، وبالتالي سيُخصص لها المستوى نفسه المخصصة للنظام الذي توفر له الحماية.

5-46- وينبغي أن ينتج عن تحليل الأصول الرقمية قائمة ووصف لتدابير الأمن الحاسوبي المحددة التي تُنفذ لكل نظام. وينبغي أن تجمع التدابير بين التحكم التقني والإداري والمادي.

5-47- وينبغي أن يوفِّر تحليل الأصول الرقمية قيمة نوعية أو كمية لعتبة المخاطر المقبولة.

التحقق من تقييم مخاطر الأمن الحاسوبي للنظام

5-48- ينبغي أن يقوم المشغِّل بالتحقق والتثبت من تقييم مخاطر الأمن الحاسوبي لكل نظام على النحو المحدد في نطاق التقييم. ويمكن أن تستخدم عملية التحقق من مخرجات إدارة مخاطر الأمن الحاسوبي للنظم أساليب التقييم الموضحة في الفقرة 4-98 فيما يتعلق بإدارة مخاطر الأمن الحاسوبي للمرفق.

5-49- يُشكل بيان التهديد الوطني أو التهديد المحتاط له في التصميم الأساس لدوافع الخصوم المحتملين وقدراتهم ونواياهم وفرصهم (بما في ذلك الخصوم الذين يستخدمون تقنيات الفضاء الإلكتروني).

5-50- وينبغي أن يضع المشغِّل سيناريوهات ذات مصداقية لكل نظام على أساس خصائص التهديد باعتبار ذلك هو الأساس للتثبت من تدابير الأمن الحاسوبي التي توفر الحماية للنظام. وينبغي أن تشمل السيناريوهات ذات المصداقية العواقب المحتملة لإجراءات الخصوم التي قد تسفر عن إخلال بالأصول الرقمية الحساسة.

5-51- وينبغي أن تشمل السيناريوهات طرق الهجوم وتقنياته الشائعة. ويمكن أن تشمل ما يلي:

(أ) الهندسة الاجتماعية، بما فيها هجمات الانتحال الإلكتروني؛
(ب) رسائل البريد الإلكتروني الضارة؛
(ج) المواقع الشبكية الضارة؛
(د) أجهزة الوسائط المحمولة الملوثة؛
(هـ) معدات الصيانة والتفتيش المخترقة؛
(و) الوصول عن بُعد؛
(ز) الأطراف الداخلية (عن قصد وعن غير قصد)؛
(ح) الإخلال بسلسلة الإمداد.

5-52- وينبغي أن توضع السيناريوهات بما يتسق مع بيان التهديد الوطني أو التهديد المحتاط له في التصميم الذي ينطبق على المرفق لتحديد الأُصول الرقمية الحساسة التي قد تكون معرضة لتلك الهجمات. وقد يكون من المفيد أن يبدأ وضع السيناريوهات بدراسة الحالات الأكثر احتمالية أو الأعلى من حيث العواقب.

5-53- وينبغي أن يكون لوضع السيناريوهات الأهداف التالية (مرتبة حسب الأهمية):

(أ) تحديد سيناريوهات العواقب الأعلى التي تنطوي على أصول رقمية حساسة؛

(ب) تحديد السيناريوهات الأكثر احتمالاً التي تنطوي على أصول رقمية، بما فيها أصول رقمية حساسة.

5-54- وينبغي أن تشمل أساليب التقييم (الفقرة 4-98) سيناريوهات ذات مصداقية (الفقرات من 4-116 إلى 4-125) للتحقق من فعالية تدابير الأمن الحاسوبي المنفذة.

5-55- وينبغي أن يتحقق المشغِّل من الأصول الرقمية، بما فيها الأصول الرقمية الحساسة، للتأكد من حصولها على المستوى المناسب من الحماية ضد الخصوم المحددين في بيان التهديد الوطني أو التهديد المحتاط له في التصميم الذي ينطبق على المرفق.

تقرير إدارة مخاطر الأمن الحاسوبي للنظم

5-56- وينبغي توثيق مخرجات عملية إدارة مخاطر الأمن الحاسوبي للنظم في تقرير يشمل ما يلي:

(أ) تحديد جميع الأصول الرقمية الحساسة، بما يشمل (قدر المستطاع) جميع الأجهزة والبرامج الحاسوبية لكل أصل من الأصول الرقمية الحساسة.
(ب) تحديد الأصول الرقمية التي تُشكل مكونات في الأصول الرقمية الحساسة أو ترتبط معها بعلاقة بينية أو تدعمها أو لديها القدرة على الوصول إلى مسارات الاتصال المتصلة بها. وقد تشمل مكونات النُظم المخصصة لمستوى من مستويات الأمن الحاسوبي.
(ج) تحديد الثغرات أو أوجه القصور أو الثغرات المعروفة في النُظم أو المكونات، ومنها على سبيل المثال مسائل الشراء المحتملة (مثل توريد قطع غيار مزيَّفة أو دون المستوى المطلوب)، أو الإجراءات أو جوانب القصور البشرية التي قد تؤثر على الأمن.
(د) تحديد تدابير التحكم التقني والإداري والمادي.
(هـ) توصيات لتنفيذ التدابير المضادة.
(و) التوصيات بشأن التحسينات في التدابير المضادة (أي التدابير الإضافية للتحكم التقني أو الإداري أو المادي).
(ز) تحديد أوجه القصور في وثائق المرفق أو سجلاته.
(ح) تصنيف المعلومات الحساسة.
(ط) قوائم التحكم في دخول الأفراد والخدمات.

(ي) الإجراءات التصحيحية عند حدوث ظروف معاكسة.
(ك) تقييم المخاطر المتبقية على مستوى النظام.
(ل) تحديد ووصف المؤشرات الأخرى التي ستساعد في تقييم الأمن الحاسوبي (مثل متوسط المدة الزمنية بين الأعطال، ومتوسط المدة الزمنية اللازمة للإصلاح، ومتوسط المدة الزمنية اللازمة للكشف، ومتوسط المدة الزمنية اللازمة للتعافي، ومقاييس جودة الأمن).

5-57- وينبغي تصنيف تقرير إدارة مخاطر الأمن الحاسوبي للنظم باعتباره معلومات حساسة وينبغي حمايته وفقاً لذلك.

6- اعتبارات إدارة مخاطر الأمن الحاسوبي للمرفق أثناء مراحل محددة من عمر المرفق

6-1- يُقدم هذا القسم إرشادات محددة بشأن المراحل المختلفة في عمر المرفق.

التخطيط

6-2- ينبغي أن يستعرض المشغِّل خططه المتعلقة بالمرفق في ضوء لوائح السلطة المختصة، وأن يحدد المسائل التي في حاجة إلى معالجة لتلبية المتطلبات الرقابية.

6-3- وينبغي أن يضمن المشغِّل أن لديه منهجية رسمية لأداء عملية مفصلة لإدارة مخاطر الأمن الحاسوبي للمرفق.

6-4- ينبغي أن يضع المشغِّل عملية إدارة مخاطر الأمن الحاسوبي للمرفق على النحو الموضح في القسم 4.

6-5- وينبغي أن يتحقق المشغِّل من أن المخاطر المتبقية لن تتجاوز المستويات المقبولة، شريطة استيفاء مواصفات بنية الأمن الحاسوبي الدفاعية.

6-6- وينبغي أن يخطط المشغِّل لتطوير الكفاءات اللازمة لدعم الأمن الحاسوبي خلال جميع المراحل في عمر المرفق.

6-7- ويمكن أن تشمل مرحلة التخطيط أنشطة في أماكن بعيدة عن موقع المرفق المقصود. وينبغي أن يُطبق المشغِّل تدابير الأمن الحاسوبي على المعلومات المستخدمة في هذه الأنشطة، وعلى المدخلات والمخرجات الأخرى المرتبطة بدورة حياة التخطيط التي تُشكل معلومات حساسة أو تستخدم أصول المعلومات الحساسة.

تحديد الموقع

6-8- ينبغي أن يُدرج المشغِّل اعتبارات الأمن الحاسوبي في مرحلة تحديد الموقع للمرفق، لأن بعض الأنشطة الداعمة للأمن الحاسوبي لا يمكن إجراؤها إلاّ عندما تكون مرتبطة بموقع محدد وليس عن بُعد أو بشكل عام (مثل إنشاء شبكات معزولة، أو وصول أفرقة التصدي للحادثات الحاسوبية، وتحديد مدى توافر الخبرة في مجال الأمن الحاسوبي في القوة العاملة المحلية).

6-9- وينبغي أن يراعي المشغِّل في خططه لتحديد مواقع المعدات الرئيسية، الحاجة إلى السماح بتشغيل تدابير التحكم المادي التي ستكون ضرورية لتكميل تدابير الأمن الحاسوبي.

6-10- وعند تحديد المواقع، ينبغي أن ينظر المشغِّل في توافر البنية الأساسية المحلية لدعم تدابير الأمن الحاسوبي (مثل شبكات الاتصالات في حالات الطوارئ).

التصميم

6-11- ينبغي أن يستخدم المشغِّل مخرجات أعمال إدارة مخاطر الأمن الحاسوبي للمرفق التي أُجريت أثناء مرحلة التخطيط للتأكد من أن عملية تصميم المرفق توفِّر متطلبات الأمن الحاسوبي لوظائف المرفق (المحددة في بنية الأمن الحاسوبي الدفاعية وبرنامج الأمن الحاسوبي) التي يتعيَّن الوفاء بها كجزء لا يتجزأ من الأنشطة الهندسية للمرفق. وينطبق ذلك على تصميم المرفق الجديد أو على تعديل التصميم لتجديد المرفق أو

تعديلـه أثنـاء مرحلـة تشـغيله.

6-12- وينبغـي أن تراعـي عمليـة التصميـم متطلبـات الأمـن الحاسـوبي التـي تنشـأ بسـبب التبعيـات بيـن وظائـف المرفـق، علـى النحـو المحـدد أثنـاء عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق.

6-13- وينبغـي توفيـر متطلبـات الأمـن الحاسـوبي بتفاصيـل كافيـة للسـماح باتخـاذ القـرارات التصميميـة والتحقـق مـن التصميـم وتقييـم التغييـرات التصميميـة.

6-14- وينبغـي أن يجـري المشـغِّل عمليـة لإدارة مخاطـر الأمـن الحاسـوبي لـكل نظـام، بمـا يشـمل التحقـق فـي كل خطـوة مـن خطـوات تصميـم تدابيـر الأمـن الحاسـوبي.

6-15- وينبغـي النظـر فـي إمكانيـة الوصـول ماديـاً وعـن بُعـد إلـى الأصـول الرقميـة الحساسـة داخـل المناطـق الحيويـة مـن جانـب طـرف داخلـي أثنـاء مرحلـة التصميـم.

6-16- وينبغـي أن يضـع المشـغِّل معاييـر التثبـت مـن الأمـن الحاسـوبي لمرحلـة الإدخـال فـي الخدمـة. وينبغـي التثبـت بشـكل مسـتقل مـن النُظـم التـي تـؤدي وظائـف المرفـق المخصصـة لأعلـى مسـتويات الأمـن الحاسـوبي.

6-17- وينبغـي إشـراك الموظفيـن المطلعيـن علـى الأمـن الحاسـوبي مـن مختلـف قطاعـات المنظمـة المشـغِّلة فـي عمليـة التصميـم لضمـان مـا يلـي:

(أ) إدراج متطلبات الأمن الحاسوبي المناسبة.
(ب) التغيير في التصميم تُحسن الأمن الحاسوبي ولا تؤدي إلى إضعافه.
(ج) التغييرات، على النحو الذي تُنفذ به، تُلبي متطلبات الأمن الحاسوبي المحددة.
(د) استعراض الفعالية يشمل الأمن الحاسوبي.

6-18- وينبغـي أن يشـمل التصميـم التوجيهـات اللازمـة لتنفيـذ متطلبـات الأمـن الحاسـوبي. وينبغـي الاحتفـاظ بالمعلومـات التصميميـة، مثـل تقاريـر التحليـل، لكـي تكـون متاحـة فـي المسـتقبل لمسـتخدمي التصميـم المـأذون لهـم.

6-19- وبالنظـر إلـى أن وثائـق التصميـم قـد تحتـوي علـى معلومـات حساسـة مرتبطـة بالأمـن

الحاسوبي، ينبغي تصنيف جميع وثائق التصميم باعتبارها وثائق سرية وفقاً لنظام تصنيف المعلومات، وينبغي حمايتها بناءً على ذلك.

6-20- وينبغي أن يضمن المشغِّل أن متطلبات الأمن الحاسوبي التي يتعيّن على البائعين والمتعهدين والموردين اتباعها محددة في عقودهم[39].[19] وينبغي مطالبة البائعين والمتعهدين والموردين بأن تكون لديهم نُظم لإدارة الأمن الحاسوبي وبيئات هندسية آمنة وتطبيق الأمن من خلال التصميم على الأصول الرقمية الحساسة التي يُنتجونها أو يوردونها.

البناء

6-21- ينبغي أن يضمن المشغِّل اتخاذ تدابير للتحكم المادي والإداري والتقني أثناء عملية البناء للحفاظ على تدابير الوقاية والحماية المطلوبة بموجب برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية. وعلى سبيل المثال، إذا كان من المقرر تركيب أبواب قابلة للقفل على مساحة مطوقة، ينبغي تثبيت الأقفال ووضعها تحت المراقبة قبل تركيب الأصول الرقمية الحساسة داخل تلك المساحة المطوقة، أو ينبغي وضع تدابير تعويضية مناسبة.

6-22- وينبغي أن يضمن المشغِّل تنفيذ إجراءات الأمن الحاسوبي التالية على النحو المطلوب في برنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية أثناء مرحلة البناء.

(أ) أنشطة الضمان (أي الاختبار والتقييمات وعمليات المراجعة)؛
(ب) استخدام مناطق تخزين وسيطة مزوّدة بضوابط للعمليات والأمن للتحقق من عدم التلاعب بالأصول الرقمية الحساسة؛
(ج) إدارة الموظفين والتحقق من منتجات البائعين والمتعهدين والموردين (سواءً من يعملون في الموقع أو من يعملون عن بُعد)، من التصنيع إلى التركيب؛
(د) تقييم سلسلة الإمداد وإدارتها، بما يضمن اتباع عملية الشراء التي يتم التحقق منها باستمرار وعدم التلاعب بها.

[39] يمثل المعيار ISO/IEC 15408 [18] 'المعايير المشتركة' للمنظمة الدولية للتوحيد القياسي واللجنة الدولية للتقنيات الكهربائية أحد الأدوات التي يمكن الاسترشاد بها في متطلبات الأمن المحتملة.

الإدخال في الخدمة

6-23- ينبغي أن يُدرج المشغِّل اختبار تدابير الأمن الحاسوبي في اختباره الخاص بقبول تسليم النُظم إلى المرفق من مقدِّم النظام.

6-24- وينبغي أن يُجري المشغِّل أنشطة تشكيل الأنساق والاختبار أثناء إدماج النظام وبنية الأمن الحاسوبي الدفاعية (الشكل 7) لتلبية متطلبات الأمن الحاسوبي. ومن ذلك على سبيل المثال، ينبغي إجراء الأنشطة التالية:

(أ) ينبغي تغيير كلمات المرور وأساليب المصادقة الثانوية الخاصة بالأصول الرقمية وفقاً للإجراءات المعتمدة.
(ب) ينبغي إزالة حسابات التطوير والبناء الخاصة بالأصول الرقمية، وينبغي تمكين تدابير التحكم التقني.
(ج) ينبغي تقديم أدوات دعم النظام (البرامج والأجهزة الحاسوبية) للاختبار والتقييم باستخدام تدابير الأمن الحاسوبي المناسبة.

6-25- وينبغي أن يجري المشغِّل اختباراً للتثبت من تدابير الأمن الحاسوبي. وينبغي التثبت من تدابير الأمن الحاسوبي وتدابير الحماية المادية معاً لضمان تحقيق مستوى مناسب من التكامل.

6-26- وفي حال حدوث تضارب بين تدابير الأمان وتدابير الأمن، ينبغي الحفاظ على تدابير ضمان الأمان، وينبغي أن يجد المشغِّل حلاً يُلبي أيضاً متطلبات الأمن الحاسوبي. وإلى أن يتم التوصل إلى هذا الحل، ينبغي تنفيذ تدابير أمن حاسوبي لخفض مستوى المخاطر إلى مستوى مقبول، وينبغي أن تكون مدعومة بتبرير شامل وتحليل لمخاطر الأمن. وينبغي ألّا تعتمد التدابير التعويضية على تدابير التحكم الإداري فقط لمدة طويلة. وينبغي ألّا يُقبل بأي حال من الأحوال عدم وجود حل أمني.

6-27- وينبغي الانتهاء من استعراض وثائق برنامج الأمن الحاسوبي القابلة للتطبيق والمواد الداعمة (المطلوبة لتشغيل النظام) والموافقة عليها قبل التشغيل.

6-28- ينبغي أن يُسند المشغِّل المسؤولية المستمرة عن تغيير التصميم والإدارة والصيانة والعمليات الخاصة ببرنامج الأمن الحاسوبي بأكمله إلى فرد (يدعمه، حسب الضرورة، أشخاص آخرون من ذوي المهارات والمعرفة المناسبة).

6-29- وينبغي أن يحتفظ المشغِّل بالوثائق التي تصف كيفية تنفيذ تدابير الأمن الحاسوبي وفقاً لبرنامج الأمن الحاسوبي وبنية الأمن الحاسوبي الدفاعية وأي متطلبات مفروضة من الخارج.

6-30- وينبغي أن يضمن المشغِّل أن المتطلبات التشغيلية متسقة مع مستوى الأمن الحاسوبي للنُظم والأصول الرقمية. ومن ذلك على سبيل المثال، قد يلزم النظر في الآتي:

(أ) إمكانية اختلاف قيود الوصول، والتحكم في الدخول والرصد بالنسبة للمعدات المخصصة لمستويات أمن حاسوبي مختلفة.
(ب) إمكانية اختلاف مستويات التحقق من الجدارة بالثقة للأفراد الذين يرتبط عملهم بنُظم مختلفة، تبعاً لمستوى الأمن الحاسوبي المخصصة لتلك النُظم.
(ج) يمكن الفصل بين الواجبات.

6-31- ويمكن أن تؤدي الإجراءات المطبقة على النُظم كجزء من تقييم الثغرات إلى عدم استقرار المحطة أو العملية، ولذلك ينبغي النظر فيها فقط باستخدام أحواض الاختبار أو النُظم الاحتياطية، أو أثناء اختبارات قبول المحطات أو أثناء فترات الانقطاع المقررة منذ فترة طويلة.

الصيانة

6-32- ينطبق هذا القسم على أنشطة الصيانة الروتينية التي تستغرق مدة قصيرة أثناء مرحلة العمليات. ويتم تناول الصيانة التي تستغرق مدة طويلة (مثل التجديد واستبدال النُظم والإصلاحات) في مراحل التصميم والبناء ووقف العمليات.

6-33- وينبغي أن يتأكد المشغِّل من تنفيذ أنشطة الصيانة وفقاً لمستويات الأمن

الحاسوبي للنُظم أو الأصول الرقمية المراد صيانتها. ومن ذلك على سبيل المثال، بالإضافة إلى الاعتبارات العامة أثناء التشغيل الواردة في الفقرة 6-30، ينبغي اتخاذ الخطوات التالية:

(أ) ينبغي تحديد أنشطة الصيانة المسموح بها.
(ب) ينبغي تحديد الوصول اللازم للصيانة والتحكم فيه.
(ج) يمكن تقييد معدات الصيانة لتقتصر على الاستخدام داخل نطاق أمن حاسوبي محدد (أو نظام محدد أو أصل رقمي محدد) أو لنُظم ذات مستوى أمن حاسوبي معيّن.
(د) قد تكون بيئات الصيانة الآمنة مطلوبة لبعض النُظم أو الأصول الرقمية.

6-34- وقد تكون النُظم أكثر عرضة للخطر أثناء الصيانة عندما تُلغى أو تُعطل تدابير الأمن الحاسوبي. وعلاوة على ذلك، يمكن أن تكون هناك طرق وصول إضافية أثناء الصيانة تنشأ على سبيل المثال عن الحاجة إلى تمكين برامج الصيانة عن بُعد أو استخدام وسائط التخزين القابلة للنقل لتهيئة نسق البرنامج الحاسوبي أو تطويره.

6-35- وينبغي أن يضع المشغّل تدابير تعويضية كافية عند إزالة تدابير الأمن الحاسوبي العادية أو تعطيلها. وتشمل أمثلة ذلك ما يلي:

(أ) ينبغي أن توفِّر التدابير التعويضية حماية مادية عند فتح المعدات.
(ب) ينبغي تحديد الحاجة إلى برامج للصيانة عن بُعد (وتبريرها) مسبقاً، وينبغي تطبيق تدابير أمن حاسوبي مناسبة على هذه البرامج وفقاً لبرنامج الأمن الحاسوبي.
(ج) ينبغي التحكم في استخدام الأدوات القائمة على الحاسوب (مثل معدات القياس والاختبار والمعايرة) ورصدها لضمان عدم الإخلال بالأدوات بسبب الهجوم على الفضاء الإلكتروني، أو توفير طريق للإخلال بالنُظم التي تُستخدم فيها تلك الأدوات. وينبغي حماية المعدات الحاسوبية التي قد تكون متصلة مؤقتاً بالنظام - مثل معدات الاختبار أو تشكيل الأنساق - من البرامج الضارة ونقل البيانات غير المأذون به. وينبغي التقليل إلى أدنى حد من استخدام المعدات الخارجية لهذه الأغراض. وينبغي فحص أيٍ من هذه المعدات قبل إدخالها إلى المرفق.
(د) ينبغي التحقق من البرامج الحاسوبية للتأكد من خلوها من أي برامج حاسوبية ضارة قبل تحميلها في النظام. ويمكن أن يشمل ذلك عملية تحقق من أن البرنامج

الحاسوبي لم يحدث تلاعب به وأنه أصلي، وذلك على سبيل المثال من خلال توقيع البرنامج الحاسوبي باستخدام اختصارات تشفيرية.

(هـ) يمكن أيضاً استخدام تدابير الأمان (مثل التحقق المتزامن من جانب طرف ثانٍ) لأغراض الأمن.

توقف العمليات

6-36- أثناء مرحلة توقف العمليات، يمكن إجراء تعديلات واسعة النطاق في آن واحد، مما يؤثر على نُظم متعددة.

6-37- وينبغي أن ينظر المشغِّل في تطبيق تدابير تعويضية لمعالجة أي مخاطر تنشأ عن التعديلات في نُظم الأمن أو تدهورها بسبب التغيُّرات البيئية أو الهيكلية. ويمكن أن يشمل ذلك زيادة الاعتماد على تدابير التحكم الإداري وعلى البائعين والمتعهدين والموردين لتنفيذ هذه التدابير.

6-38- ومن أمثلة التغييرات التي يمكن تطبيق تدابير تعويضية بشأنها ما يلي:

(أ) تعديل بنية الأمن الحاسوبي وتدابيره أو تعطيلها للسماح بإجراء أعمال التعديل.

(ب) التقلبات في مستويات التوظيف، مما يمكن أن يشمل إحضار موظفين جُدد إلى الموقع للاضطلاع بالأنشطة التي تنطوي على أصول رقمية، بما فيها الأصول الرقمية الحساسة. ويمكن أن يتطلب ذلك فحوصاً إضافية للتحقق من الجدارة بالثقة أو اتخاذ تدابير أخرى للتصدي للتهديد الداخلي.

(ج) استبدال كبير للمكونات، مما يتطلب إنشاء بيئة تركيب آمنة، والتخزين الآمن، وتدابير إضافية للتعامل مع الأصول الرقمية الحساسة المستبدلة وتطهيرها على نحو آمن.

الإخراج من الخدمة

6-39- عند إخراج الأصول الرقمية من الخدمة، ينبغي تقييم وتوثيق تأثير هذا الإخراج من الخدمة (بما في ذلك أي فقدان للتكامل مع الأصول الرقمية الأخرى خارج المرفق)

على الأمن الحاسوبي. وإذا كان إخراج نظام أو أصل رقمي من الخدمة يُقلل من فعالية تدابير الأمن الحاسوبي، ينبغي أن يتخذ المشغِّل تدابير تعويضية.

6-40- ومع تغيُّر مجموعة وظائف المرفق، يمكن إعادة تخصيص الأصول الرقمية التي تدعم هذه الوظائف لمستوى أمن حاسوبي مختلف أو إلغاء تخصيصها. ويمكن أن يُفضي ذلك إلى ضرورة تعديل تدابير الأمن الحاسوبي لهذه الأصول الرقمية.

6-41- وينبغي أن يضمن المشغِّل إجراء إتلاف آمن لأي أصول رقمية محتوية على معلومات حساسة لا يمكن رفع السرية عنها على نحو آمن عند إخراجها من الخدمة.

7- عناصر برنامج الأمن الحاسوبي

متطلبات الأمن الحاسوبي

7-1- ينبغي أن تُشكل سياسة الأمن الحاسوبي وبرنامجه الأساس لمتطلبات الأمن الحاسوبي التي تحددها نتائج إدارة مخاطر الأمن الحاسوبي للمرفق والنظام (القسمان 4 و5 على التوالي) مع مراعاة المراحل المحددة في عمر المرفق (القسم 6).

7-2- وينبغي أن تُدرك الإدارة العليا وكبار المديرين أن الأمن الحاسوبي في المرافق النووية تخصص شامل يحتاج إلى معارف وخبرات ومهارات متخصصة.

7-3- وتقع على الإدارة العليا المسؤولية العامة عن الأمن الحاسوبي في المرفق النووي، ويتعيّن أن تكون على وعي وفهم بتهديد الفضاء الإلكتروني والتأثير الضار المحتمل على الأمن النووي.

7-4- وينبغي أن تضمن الإدارة العليا أن جميع تفاعلات المشغِّل مع الآخرين وجميع العمليات الداخلية متوافقة مع المتطلبات القانونية والرقابية المتصلة بأمن المعلومات والأمن الحاسوبي.

7-5- وينبغي أن ينشر المديرون معتقدات ثقافة الأمن النووي وقيمها فيما يتعلق بالأمن الحاسوبي. ويشمل ذلك تعزيز الاعتراف بوجود تهديد ذي مصداقية من خصوم لديهم مهارات في مجال الفضاء الإلكتروني، وأن هؤلاء الخصوم (بما يشمل التهديدات الداخلية) قد يستهدفون المرافق النووية عن طريق هجوم على الفضاء الإلكتروني أو من خلال هجوم مختلط.

سياسة الأمن الحاسوبي

7-6- تُحدِّد سياسة الأمن الحاسوبي أهداف الأمن الحاسوبي العالية المستوى في المنظمة. وينبغي أن تبدأ سياسة الأمن الحاسوبي ببيان واضح يُحدد أسباب وضع السياسة، وينبغي أن يُحدد المسألة المراد معالجتها، وكذلك الأهداف والعواقب في حال عدم اتباع السياسة. وينبغي أن تكون السياسة متوافقة مع سياسة الأمن الحاسوبي للدولة والمتطلبات الرقابية المناسبة. وينبغي أن تكون السياسة قابلة للإنفاذ ويمكن تحقيقها، وينبغي أن تشمل مؤشرات يمكن قياسها ومراجعتها.

7-7- وينبغي أن تأخذ سياسة الأمن الحاسوبي الخاصة بالمشغِّل في الاعتبار نتائج إدارة مخاطر الأمن الحاسوبي للمرفق (انظر القسم 4). وينبغي أن تشترط سياسة الأمن الحاسوبي حماية الأصول الرقمية، بما في ذلك الأصول الرقمية الحساسة ضد أي إخلال من هجمات على الفضاء الإلكتروني. وينبغي أن تكون بنود السياسة واضحة وموجزة في تحديد هذه المتطلبات. ويعالج برنامج الأمن الحاسوبي بالتفصيل تنفيذ هذه المتطلبات.

7-8- وينبغي اعتماد سياسة الأمن الحاسوبي وإنفاذها من جانب الإدارة العليا. وينبغي أن تُحدد المنظمة المسؤولة أو الفرد المسؤول عن السياسة وبرنامج الأمن الحاسوبي.

7-9- وينبغي أن تُشكل سياسة الأمن الحاسوبي جزءاً من سياسة الأمن الحاسوبي العامة للمرفق، وينبغي تنسيقها مع سائر مسؤوليات الأمن ذات الصلة. وعند وضع سياسة أمن حاسوبي، ينبغي أيضاً مراعاة تأثيرها على الجوانب القانونية والموارد البشرية.

7-10- ويمكن أن تُحدد سياسة الأمن الحاسوبي الجزاءات المحتملة والإجراءات التأديبية ضد الأفراد الذين لا يمتثلون لمتطلبات السياسة.

7-11- وينبغي أن يُعبِّر برنامج الأمن الحاسوبي عن سياسة الأمن الحاسوبي وينبغي

تجسيدها من خلال عناصر برنامج الأمن الحاسوبي التي تدعم تنفيذ الأمن الحاسوبي.

7-12- ويتعيَّن أن تُحدد السياسة مؤشرات واضحة تُستخدم لإثبات الوفاء بالسياسات من جميع الجوانب وأن كل جانب يُنفذ بصورة مُرضية.

برنامج الأمن الحاسوبي

7-13- يشمل برنامج الأمن الحاسوبي تفاصيل عن كيفية تحقيق الأهداف المحددة في سياسة الأمن الحاسوبي. ويُحدد برنامج الأمن الحاسوبي الأدوار والمسؤوليات والعمليات والإجراءات التنظيمية اللازمة لتنفيذ سياسة الأمن الحاسوبي. ويمكن أن يكون برنامج الأمن الحاسوبي خاص بمرفق بعينه (بما في ذلك المباني والمعدات المرتبطة به) أو بمنظمة (بما في ذلك جميع المواقع والوحدات التنظيمية).

7-14- وينبغي وضع برنامج الأمن الحاسوبي والتمرن والحفاظ عليه ضمن إطار خطة الأمن الحاسوبي الشاملة للمرفق.

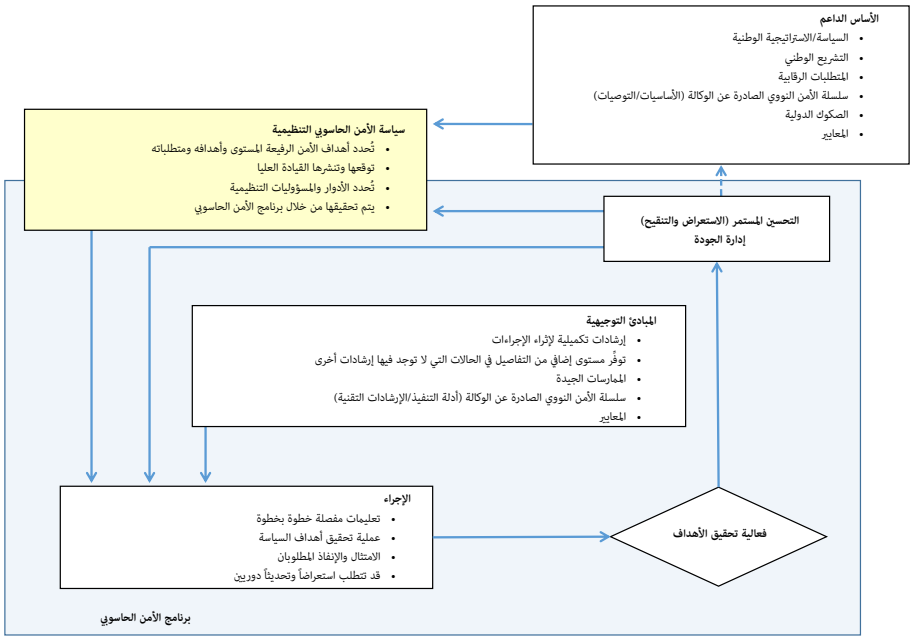
7-15- وينبغي أن يأخذ برنامج الأمن الحاسوبي في الاعتبار نتائج إدارة مخاطر الأمن الحاسوبي للمرفق (القسم 4). ويمكن أن يشمل وضع برنامج الأمن الحاسوبي الأفراد المعنيين بالأمن الحاسوبي، والحماية المادية، والأمان، والعمليات، وتكنولوجيا المعلومات. ويعرض الشكل 8 مخططاً يوضح برنامج الأمن الحاسوبي.

7-16- وينبغي استعراض برنامج الأمن الحاسوبي وتحديثه (أ) دورياً كي يُعبِّر عما يستجد من تطورات في التكنولوجيا والتهديدات، و(ب) في حالة وقوع حادثات أمن حاسوبي أو غيرها من أحداث الأمن الحاسوبي.

عناصر برنامج الأمن الحاسوبي

7-17- يتناول المرجع [7] بالوصف عناصر برنامج الأمن الحاسوبي المنطبقة بصفة عامة على المنظمات داخل منظومة الأمن النووي. وتتضمن الفقرات من 7-18 إلى 7-20 مزيداً من التفاصيل المحددة بشأن عناصر برنامج الأمن الحاسوبي للمرافق النووية.

7-18- وينبغي أن تشمل عناصر برنامج الأمن الحاسوبي معالجة ثغرات النُظم، وتطبيق



الشكل -8- لمحة عامة عن برنامج نمطي للأمن الحاسوبي

تدابير الأمن الحاسوبي، وإجراء تحليل للمخاطر، والاضطلاع بأنشطة الضمان للوصول بمخاطر الأمن الحاسوبي إلى مستوى مقبول.

7-19- وينبغي تكييف عناصر برنامج الأمن الحاسوبي مع مختلف مراحل عمر المرفق ومع مختلف أطوار دورات حياة النُظم الفردية وتطبيقه عليها. وينبغي أن يشمل برنامج الأمن الحاسوبي تفاصيل محددة عن التنفيذ في هذه الحالات.

7-20- وينبغي أن يُصمم المشغِّل برنامج الأمن الحاسوبي بما يناسب مرفقه، ولكن يُقترح كحد أدنى أن يشمل المجالات التالية:

(أ) التنظيم والمسؤوليات:

'1' الخرائط التنظيمية؛

'2' الأشخاص المسؤولون ومسؤوليات الإبلاغ (انظر الفقرات من 3 إلى 13 في التذييل)؛

'3' الاستعراض الدوري وعمليات الموافقة؛

'4' الترابط مع البرامج الأخرى، مثل الموارد البشرية، والأمن المرتبط بالأفراد، والحماية المادية والتدريب (انظر الفقرات من 15 إلى 38 في التذييل.

(ب) إدارة المخاطر والثغرات والامتثال:

'1' عملية إدارة مخاطر الأمن الحاسوبي للمرفق ومخرجاتها (انظر القسم 4)؛

'2' عملية إدارة مخاطر الأمن الحاسوبي للنظم ومخرجاتها (انظر القسم 5)، بما في ذلك عملية تصنيف الأصول الرقمية،[40] بما فيها الأصول الرقمية الحساسة، وتحديدها؛

'3' تواتر استعراض خطة الأمن وتقييمها؛

'4' ممارسات التقييم الذاتي؛

'5' إجراءات المراجعة وتتبع أوجه القصور وتصحيحها؛

'6' أسلوب البدء في إجراء تقييم المخاطر والثغرات وتكراره والمناسبات التي يتم فيها ذلك؛

'7' الامتثال الرقابي والتشريعي.

(ج) تصميم الأمن وإدارته:

'1' البنية الأساسية للأمن (أي بنية الأمن الحاسوبي الدفاعية)؛

'2' النُهج الأساسية لتصميم الأمن (أي مستويات الأمن الحاسوبي ونطاقاته)؛

'3' تخصيص تدابير الأمن الحاسوبي الأساسية لكل مستوى من مستويات الأمن الحاسوبي؛

'4' إضفاء الطابع الرسمي على متطلبات الأمن الحاسوبي للمتعهدين والبائعين والموردين، بما يشمل عقود الصيانة؛

'5' الاعتبارات الأمنية للمراحل المطبقة في عمر المرفق (انظر القسم 6).

(د) إدارة الأصول الرقمية:

'1' سمات الأصول الرقمية (التحديد، ومستوى الأمن الحاسوبي، والنطاق، والمكان، والعواقب ذات الصلة)؛

'2' تنظيم نسق المكونات (الأجهزة، ونُظم التشغيل، والبرامج الثابتة، وتطبيقات البرامجيات الحاسوبية، وحالة المعدات، والأنساق ذات الصلة)؛

'3' تدفق البيانات ومخططات الشبكة التي تُحدِّد جميع الوصلات الخارجية إلى النُظم الأخرى؛

'4' معلومات الموردين فيما يتصل بالأصول.

[40] تشمل الأصول الرقمية تدابير المراقبة التقنية التي تستخدم التكنولوجيات الرقمية.

(هـ) إجراءات الأمن:

'1' التعامل مع حادثات الأمن؛

'2' استمرارية العمل؛

'3' النسخ الاحتياطي للنُظم واستعادتها واسترجاعها؛

'4' سلسلة الإمداد؛

'5' التحكم في الدخول؛

'6' إدارة المعلومات والاتصالات؛

'7' أمن المنصات والتطبيقات (مثل تحصين النُظم)؛

'8' رصد النُظم، بما في ذلك تسجيل الدخول.

(و) إدارة الأفراد:

'1' فحوص التحقق من الجدارة بالثقة؛

'2' التوعية والتدريب؛

'3' تأهيل الأفراد؛

'4' الإبلاغ عن مسائل الأمن، بما فيها حماية الموظفين الذين يقومون بالإبلاغ عن هذه المسائل؛

'5' الإنهاء أو النقل.

7-21- ويمكن الرجوع إلى مزيد من المعلومات عن عناصر برنامج الأمن الحاسوبي في المعايير الدولية [19–21].

الأدوار والمسؤوليات التنظيمية

7-22- ينبغي أن يحدد المشغِّل الأدوار والمسؤوليات المتصلة بالأمن الحاسوبي داخل المنظمة.

7-23- وينبغي أن يضمن المديرون أن جميع الموظفين على علم بالجهة المسؤولة داخل المنظمة عن قيادة برنامج الأمن الحاسوبي في المجالات الوظيفية ذات الصلة بعملهم. ويتعيّن تدريب الموظفين الذين يضطلعون بمسؤوليات في مجال الأمن الحاسوبي على العناصر والمتطلبات المحددة في برنامج الأمن الحاسوبي.

7-24- وينبغي أن تُشكل إدارة الأمن الحاسوبي جزءاً لا يتجزأ من نظام الإدارة القائم في المنشأة (انظر الفقرات من 7-30 إلى 7-34) قدر المستطاع وبالقدر الممكن عملياً.

وسيشـمل نظـام الإدارة بالفعـل أدواراً ومسـؤوليات محـددة جيـداً، وينبغـي تعديلهـا لتشـمل الأمـن الحاسـوبي.

7-25- ينبغـي ألاّ يكـون لـدى الموظفيـن الذيـن يضطلعـون بمسـؤوليات مهمـة فـي مجـال الأمن الحاسـوبي تضـارب فـي المصالـح مـع وظائـف أخـرى فـي المنظمـة أو مـع واجبـات أخـرى. وينبغـي أن يضـع المديـرون سياسـات وعمليـات لتجنـب أي تضـارب محتمـل أو التخفيـف منـه.

7-26- وينبغـي أن يضمـن المشـغِّل أن مـن يقومـون بأنشـطة التقييـم والتحقـق الرئيسـية مـن أفـراد أو منظمـات يتمتعـون بمؤهـلات مناسـبة ومسـتقلون.

7-27- يتطلـب الأمـن الحاسـوبي تعاونـاً بيـن الموظفيـن فـي مختلـف الأدوار والوحـدات التنظيميـة. وينبغـي أن يضـع المشـغِّل إطـاراً رسـمياً بهـدف ضمـان التعـاون بيـن التخصصـات.

7-28- وينبغـي أن يحـدد المشـغِّل التفاعـلات الخارجيـة والداخليـة التـي ينطـوي عليهـا برنامـج الأمـن الحاسـوبي. ويشـمل ذلـك مـا يلـي:

(أ) التفاعـلات الروتينيـة بيـن مشـغِّل المرفـق والسـلطات المختصـة ذات الصلـة (علـى سـبيل المثـال، الهيئـات الرقابيـة، وأجهـزة إنفـاذ القانـون، والـوكالات الاسـتخباراتية، والدوائـر الأمنيـة)؛

(ب) إبـلاغ السـلطات المختصـة والتفاعـل مـع قـوات التصـدي الخارجيـة فـي حـال وقـوع حادثـة متصلـة بالأمـن؛

(ج) التفاعل الداخلي مع فريق التصدي داخل الموقع؛

(د) العلاقات العامة؛

(هـ) العلاقات مع البائعين والمتعهدين والموردين، بما في ذلك سلسلة الإمداد.

7-29- وينبغـي أن يقـوم المشـغِّل بـإدارة المخاطـر مـن خـلال عمليـة رسـمية (أي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق والنظـام) لتقييـم المخاطـر والثغـرات فـي المرفـق وإدارتهـا. وينبغـي أن يسـتخدم نتائـج هـذه العمليـات داخـل نظامـه الخـاص بـالإدارة.

نظام الإدارة

7-30- ينبغي أن يكون نظام الإدارة متكاملاً ليشمل الأمن الحاسوبي، والحماية المادية، وعناصر الأمان، والصحة، والبيئة، والجودة، والعناصر المالية.

7-31- وينبغي أن يكون لنظام الإدارة تفاعلات رسمية وراسخة مع عمليات إدارة مخاطر الأمن الحاسوبي للمرفق والنظام.

7-32- وينبغي تحديد أهداف الأمن الحاسوبي وأمن المعلومات وإدارتها داخل نظام الإدارة على نحو مماثل لسائر أهداف العمل.

7-33- وينبغي استعراض نظام الإدارة لضمان اكتماله وامتثاله لسياسات أمن المرفق. وينبغي استعراضه وتكييفه مع الظروف المتغيرة في المرفق وفي البيئة. ويوضح الشكل 3 من المرجع [22] عملية التحسين المستمر لنُظم الإدارة.

7-34- وينبغي استعراض عناصر برنامج الأمن الحاسوبي (بما فيها عملية إدارة مخاطر الأمن الحاسوبي للمرفق والنظام) وينبغي أن تُشكل الترتيبات الضرورية للأمن الحاسوبي جزءاً لا يتجزأ من نظام الإدارة.

مؤشرات الأمن الحاسوبي

7-35- يمكن أن تُشكل مؤشرات الأمن الحاسوبي أداة فعالة لمدير الأمن لقياس مدى نُضج نظام الإدارة؛ والمخاطر المرتبطة بالهجمات المحتملة على الفضاء الإلكتروني التي تؤثر على الأصول الرقمية الحساسة؛ وفعالية مختلف مكونات برامج الأمن الخاصة بهم؛ وأمن نظام أو منتج معيّن أو عملية معيّنة؛ وقدرة الموظفين داخل المنظمة على معالجة المسائل الأمنية التي يتحملون المسؤولية عنها.

7-36- وينبغي أن تدعم المؤشرات القرارات المتعلقة بالمستوى المقبول للمخاطر وينبغي أن توفِّر مدخلات في سجل المخاطر.

7-37- وينبغي إجراء تحليل لتحديد البارامترات ووضع المؤشرات التي تدعم الإدارة الفعالة لبرنامج الأمن الحاسوبي وتشمل المؤشرات التي يمكن أن تكون مفيدة متوسط

زمـن التعافـي (مـن هجـوم علـى الفضـاء الإلكترونـي)، وعـدد حادثـات الأمـن الحاسـوبي، وعـدد عمليـات اسـتعادة الأصـول الرقميـة الحساسـة (الوقائـع المحتملـة)، وقوائـم المسـائل الأمنيـة المتأخـرة ومعلومـات تتبـع الثغـرات (علـى سـبيل المثـال، نظـام التقديـر المشـترك، وفعاليـة التخفيـف، وزمـن نشـر المراقبـة، ونشـر التصحيحـات).

7-38- وينبغي أن يُشكل استخدام المؤشرات جزءاً لا يتجزأ من نظام الإدارة في المنظمة.

تصميم الأمن وإدارته

7-39- يُحـدَّد تصميـم أمـن المرفـق والنظـام فـي عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق والنظـام (انظـر القسـمين 4 و5، علـى التوالـي). ويصـف القسـم 8 أحـد الطـرق العمليـة لتنفيـذ هـذه المخرجـات، وتحديـداً بنيـة الأمـن الحاسـوبي الدفاعيـة والتدابيـر المخصصـة لمسـتويات الأمـن الحاسـوبي.

متطلبات الأمن الحاسوبي

7-40- وينبغـي تحليـل التعديـلات التـي يتـم إدخالهـا علـى المرفـق أو النظـام لتحديـد التأثيرات المحتملـة علـى الأمـن قبـل إجـراء التغييـرات للسـماح بـإدارة المخاطر.

7-41- وينبغـي اعتبـار الأمـن الحاسـوبي عامـلاً عنـد تحديـد مدخـلات التصميـم التـي تشـمل مـا يلـي:

(أ) المتطلبات الوظيفية؛
(ب) متطلبات التفاعلات؛
(ج) المتطلبات التشغيلية؛
(د) مكان المعدات؛
(هـ) الاعتبارات البيئية؛
(و) المدونات والمعايير الواجب استخدامها؛
(ز) الاعتبارات التعاقدية؛
(ح) اعتبارات سلسلة الإمداد؛

(ط) اللوجستيات (على سبيل المثال، تنسيق العمليات المعقدة المنطوية على كثير من الأفراد أو المرافق أو الإمدادات)؛
(ي) الخبرة التشغيلية السابقة؛
(ك) إدخال تقنيات حديثة؛
(ل) اعتبارات العامل البشري؛
(م) متطلبات التصميم لكل تخصص هندسي (بما في ذلك الأمن الحاسوبي)؛
(ن) اعتبارات التصنيع؛
(س) التركيب؛
(ع) الإدخال في الخدمة؛
(ف) الإخراج من الخدمة؛
(ص) الاعتبارات المالية.

إدارة الأصول الرقمية

7-42- ينبغي أن يوثِّق المشغِّل لكل أصل من الأصول الرقمية سماته المهمة للأمن الحاسوبي. ويمكن أن تشمل هذه السمات ما يلي:

(أ) الرقم التعريفي للأصول وأماكنها؛
(ب) نسق مكونات الأصول
(ج) الوظائف وطرق التشغيل؛
(د) وصلات الربط البيني، بما فيها إمدادات القوى؛
(هـ) تدفق البيانات، بما في ذلك الوصلات الداخلية والخارجية؛
(و) إجراءات إطلاق الاتصال، وتواتر الاتصال، والبروتوكولات الخاصة بهذا الاتصال؛
(ز) تحليل مجموعات المستخدمين؛
(ح) الملكية (فيما يتصل بالبيانات والنُظم المحوسبة)؛
(ط) مستوى الأمن الحاسوبي ونطاقه، وتقييم عواقب الإخفاق.

7-43- وينبغي أن تأخذ إدارة الأصول الرقمية في الحسبان حالة المعدات فيما يتصل بتدابير التحكم التقني التي تستخدم التكنولوجيا الرقمية. ويمكن أن يكون لعمليات الأمن الحاسوبي وعمليات الحماية المادية مسؤولية مشتركة عن التدابير والنُظم والإجراءات الأمنية المتكاملة. ويمكن أن تشمل المراقبة التشغيلية المشتركة التحكم في الأجهزة

المادية المستخدمة لحماية المعدات الحاسوبية (على سبيل المثال، الغرف والأبواب والمفاتيح والأقفال والكاميرات وأجهزة استشعار الحركة ومؤشرات التلاعب).

تنظيم نسق المكونات

7-44- يهدف تنظيم نسق المكونات إلى الحصول على سجلات مفصلة ومواكبة لآخر التطورات بشأن البرامج المثبتة ومكونات الأجهزة ونسق مكوناتها. وينبغي أن يشمل تنظيم نسق المكونات المعلومات المطلوبة لما يلي:

(أ) تحديد الحاجة إلى تدابير أمن حاسوبي؛
(ب) التحقق من تنفيذ تدابير الأمن الحاسوبي ووضع نسق مكوناتها بصورة صحيحة؛
(ج) إدارة التغييرات طوال دورة حياة النُظم؛
(د) دعم تقييمات الأمن الحاسوبي؛
(هـ) فهم أسباب التغييرات التي تطرأ على تدابير الأمن الحاسوبي.

7-45- ويشمل تنظيم نسق المكونات عملية إدارة التغيير. وينبغي إدراج الأمن الحاسوبي في هذه العملية بحيث تُقيَّم جميع التغييرات من منظور الأمن الحاسوبي قبل التنفيذ. وعلى سبيل المثال، يتم إجراء استعراضات مناسبة وتوثيقها قبل تنفيذ الإجراءات التي يمكن أن تتجاوز فعالية تدابير الأمن الحاسوبي المعمول بها أو تغيرها أو تقلل منها. ويمكن أن تتطلب التغييرات في الأفراد أيضاً تغييرات متصلة بالأمن الحاسوبي (على سبيل المثال، إلغاء بيانات الاعتماد وإدارتها).

إجراءات الأمن

7-46- ينبغي أن يضع المشغِّل إجراءات أمنية لدعم تصميم وإدارة الأمن الحاسوبي للمرافق والنُظم. وأثناء وضع هذه الإجراءات، ينبغي أن يراعي المشغِّل قاعدة الشخصين أو الفصل بين واجبات العمل، مع مراعاة نموذج الثقة المناسب ومستوى الأمن المخصص للنطاق (النطاقات) المنطبقة على الإجراء.

7-47- وينبغي أن تشمل الإجراءات التي توفر تعليمات مفصلة بشأن كيفية تعطيل تدابير الأمن الحاسوبي أو تجاوزها تسجيل هذه الأنشطة والاحتفاظ ببياناتها في السجلات.

ويمكـن أن يوفـر الإجـراء أيضـاً تعليمـات بشـأن تطبيـق تدابيـر الأمـن الحاسـوبي البديلـة أو التعويضيـة فـي حـال تعطيـل تدابيـر الأمـن الحاسـوبي الأساسـية.

7-48- وهـذه الإجـراءات يمكـن أن تكـون إجـراءات جديـدة قائمـة بذاتهـا، أو يمكـن أن تُشـكل جـزءاً مـن إجـراءات قائمـة تفـي بواحـد أو أكثـر مـن أهـداف الأمـان أو الأمـن أو الأهـداف التنظيميـة.

إدارة الأفراد

7-49- تشـمل إدارة الأفـراد الترتيبـات الضروريـة لوضـع مسـتوى مناسـب مـن الجـدارة بالثقـة، وإنفـاذ الالتزامـات المتعلقـة بالسـرية، وتحديـد الكفـاءات المطلوبـة وكذلـك، عنـد الضـرورة، فـرض جـزاءات أو إنهـاء الخدمـة.

7-50- وينبغـي تنسـيق أنشـطة الأمـن الحاسـوبي والأمـن المتصـل بالأفـراد لتوفيـر حمايـة ضـد التهديـدات الداخليـة. ويمكـن أن يتطلـب الموظفـون الذيـن يضطلعـون بمسـؤوليات رئيسـية فـي مجـال الأمـن (علـى سـبيل المثـال، المسـؤولون عـن إدارة النظـام، وفريـق الأمـن) بصفـة خاصـة مسـتوى أعلـى مـن الجـدارة بالثقـة. ويـرد مزيـد مـن الإرشـادات بشـأن الحمايـة مـن التهديـدات الداخليـة فـي المرجـع [6].

7-51- وينبغـي أن يشـمل برنامـج الأمـن الحاسـوبي ترتيبـات للتدريـب والتوعيـة لتطويـر الكفـاءات والمؤهـلات الشـخصية والتنظيميـة الضروريـة للأمـن الحاسـوبي والمحافظـة عليهـا.

8- مثال على بنية الأمن الحاسوبي الدفاعية وتدابير الأمن الحاسوبي

8-1- فيمـا يلـي مثـال علـى تنفيـذ بنيـة الأمـن الحاسـوبي الدفاعيـة علـى خمسـة مسـتويات مختلفـة للأمـن الحاسـوبي فـي محطـة للقـوى النوويـة. ويمثـل ذلـك أحـد الطـرق الممكنـة لتنفيـذ نهـج متـدرج؛ وينبغـي أن يكـون الاختيـار الدقيـق للمسـتويات، وبنيـة الأمـن الحاسـوبي الدفاعيـة، وتدابيـر الأمـن الحاسـوبي، متوافقـاً مـع المرفـق وبيئتـه مـن خـلال تحليـل محـدد.

مثال على تنفيذ بنية الأمن الحاسوبي الدفاعية

8-2- عند تنفيذ بنية الأمن الحاسوبي الدفاعية، ينبغي أن يفكر المشغِّل في تقليل العناصر الدينامية في الشبكات والنُظم الفردية لزيادة إمكانية التنبؤ بسلوكها. ويمكن لزيادة إمكانية التنبؤ أن تساعد في تنفيذ تدابير أمن حاسوبي فعالة.

8-3- وينبغي أن تكون النطاقات المخصصة لمستوى الأمن الحاسوبي الأكثر صرامة متصلة فقط بالنطاقات التي يخصص لها أدنى مستويات الأمن من خلال مسارات اتصال بيانات محصنة من الأعطال وقطعية وأحادية الاتجاه. وينبغي أن يكون اتجاه مسارات البيانات من النطاق الذي يخصص له مستوى الأمن الحاسوبي الأكثر صرامة إلى النطاق الذي يخصص له مستوى الأمن الحاسوبي الأقل صرامة.[41] ولا يُنصح بشدة بمنح أي استثناءات، ولا يجوز النظر في منحها إلّا في أضيق الحدود تبعاً لكل حالة على حدة وإذا كانت مدعومة بتبرير كامل وتحليل للمخاطر الأمنية.[42]

8-4- وينبغي ألّا تتجاوز الأجهزة أو الاتصالات الرقمية المستخدمة في الرصد والصيانة والتعافي تدابير الأمن الحاسوبي المستخدمة لحماية مسارات الاتصال بين الأجهزة المتباينة من حيث مستويات الأمن الحاسوبي.

8-5- وينبغي وضع النُظم المخصصة لمستوى الأمن الحاسوبي الأكثر صرامة ضمن حدود النطاق الأكثر أمناً.[43]

8-6- وينبغي حماية اتصالات البيانات بين النُظم داخل المرفق ومركز الطوارئ (سواءً في الموقع أو خارجه) من خلال تدابير الأمن الحاسوبي.

---

[41] تستثنى من ذلك النطاقات التي تقتصر على وظائف إدارة المعلومات الحساسة، والتي يُعكس اتجاهها. ويمكن نقل المعلومات الحساسة إلى شبكات البيانات المقيدة، ولكن ليس العكس.

[42] لا تسمح بعض الدول الأعضاء بمنح استثناءات للمرافق التي تنطوي على عواقب وخيمة أو وخيمة جداً. وفي أنواع أخرى من المرافق، قد تسمح السلطة المختصة للمشغِّل بحرية التصرف في تطبيق المسارات الثنائية الاتجاه.

[43] تنطوي وظائف الاتصالات اللاسلكية على إشكالية عند تنفيذها في نُظم مخصصة لمستوى الأمن الأكثر صرامة نظراً لصعوبة توفير حدود آمنة لهذه الاتصالات.

الفصل بين نطاقات الأمن الحاسوبي

8-7- تعتمد تدابير الأمن الحاسوبي التي تضمن الفصل المنطقي والمادي بين النطاقات على متطلبات مستويات الأمن الحاسوبي للمناطق. وللحفاظ على الدفاع في العمق، ينبغي عدم السماح بمسار مباشر يربط بين عدة نطاقات.

8-8- وينبغي تصميم تدابير التحكم التقني التي توفّر الأمن عند حدود النطاقات بحيث تكون قادرة على الصمود أمام الهجمات على الفضاء الإلكتروني وتوفير تنبيهات في حال حدوث إخلال محتمل أو نشاط ضار.

الاتصال الإلكتروني الخارجي

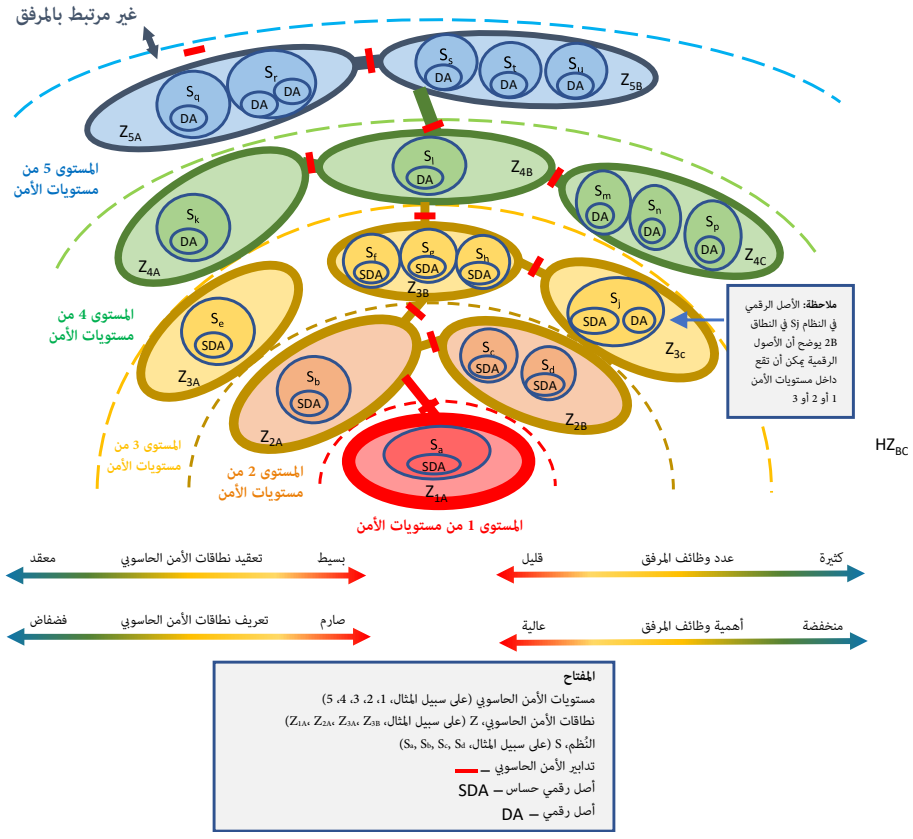
8-9- عند توفير اتصال إلكتروني خارجي، ينبغي تطبيق الأمن باستخدام نهج متدرج. وينبغي أن يفي الاتصال الإلكتروني الخارجي بمتطلبات حماية السرية والسلامة وتوافر المعلومات الحساسة بما يتسق مع مستوى الأمن الحاسوبي المخصص للنطاق.

8-10- وينبغي تطبيق قيود الوصول المناسبة (بما في ذلك التحكم في الدخول) لتوفير الحماية على أساس النهج المتدرج لأن هذه الوصلات الخارجية يمكن أن تُشكل مساراً للإخلال بالنُظم في المرفق.

8-11- وفيما يلي أمثلة على النُظم التي يمكن الوصول إليها من الخارج:

(أ) نُظم الرصد البيئي؛
(ب) نُظم التشغيل الآلي للمباني؛
(ج) نُظم الحماية من الحرائق؛
(د) الاتصالات مع مراكز الطوارئ؛
(هـ) وصول البائعين عن بُعد (حيثما يُسمح بذلك)؛
(و) الأجهزة الميدانية الواقعة خارج محيط الأمن المادي؛
(ز) التحكم في دخول الزائرين.

8-12- ويُعطي الشكل 9 مثالاً على أحد طرق تنفيذ بنية الأمن الحاسوبي الدفاعية، ويُظهر



الشكل -9- مثال على تنفيذ بنية أمن حاسوبي دفاعية

الشكل المستويات والنطاقات والنُظم والأصول الرقمية. ويستند ذلك إلى الإرشادات الواردة في القسم 3.

أمثلة من المتطلبات

8-13- ترد في الفقرات من 8-16 إلى 8-21 أمثلة على متطلبات الأمن المطبقة داخل كل مستوى من مستويات الأمن الحاسوبي. وينبغي أن يكون الاختيار الدقيق للمستويات ومتطلباتها الأمنية مناسباً للمرفق وبيئته من خلال تحليل محدد.

الأصول الرقمية غير المخصصة

8-14- يمكن مصادفة نوعين من الأصول الرقمية غير المخصصة:

(أ) المعدات المقيَّدة أو المحظورة، حيث تعني القيود المفروضة على المشغِّل عدم إمكانية تقييم أمن الأصول الرقمية. ويمكن أن يكون ذلك راجعاً إلى شروط الترخيص، أو المتطلبات التعاقدية أو الرقابية أو القانونية التي تحظر على المشغِّل فحص المعدات وتعديلها (مثل المعدات المرتبطة بالضمانات).

(ب) المعدات غير المعلن عليها التي قد يتم إحضارها إلى المرفق من دون أن يطلبها المشغِّل أو من دون موافقته المسبقة. وتعتبر هذه المعدات "ممنوعات" لحين الانتهاء من إجراء تقييم لمخاطر الأمن الحاسوبي.

8-15- ويمكن للمشغِّل فرض قيود على الأصول غير المخصصة لحين تقييمها وتخصيصها لمستوى الأمن الحاسوبي المناسب، ووضع تدابير الأمن الحاسوبي المطلوبة. وينبغي عدم إحضار الأجهزة غير المخصصة، على سبيل المثال، على مقربة من النُظم التي تُسند إلى مستويات أمن حاسوبي متوسطة إلى عالية.

المتطلبات العامة

8-16- فيما يتعلق بالنُظم والمستويات المطبقة، تُطبق المتطلبات العامة التالية:

(أ) تُصمم جميع التدابير الأمنية التقنية والمادية والشخصية والتنظيمية للنُظم والشبكات وتُنفذ بطريقة منهجية ووفقاً للعمليات والإجراءات المعتمدة.

(ب) تُحدد سياسات وممارسات لكل مستوى من مستويات الأمن الحاسوبي.

(ج) يلتزم المستخدمون بالامتثال لسياسات الأمن وإجراءات التشغيل الأمنية.

(د) يكون الموظفون المسموح لهم بالوصول إلى النظام مؤهلين تأهيلاً مناسباً ويتمتعون بالخبرة ويحددون بأنهم جديرون بالثقة عند الضرورة.

(هـ) لا يُتاح للمستخدمين والمسؤولين عن الإدارة الوصول إلى ما يوجد في هذه النُظم من وظائف يحتاجون إليها من أجل أداء وظائفهم. ويُمنع مراكمة حقوق الوصول من جانب الفرد.

(و) تكـون وظائـف النظـام وتفاعلاتـه محـدودة إلـى أقصـى حـد ممكـن بهـدف تقليـل الضعـف العـام للنظـام.
(ز) تُطبق التدابير المناسبة للتحكم في الدخول والمصادقة على المستخدمين.
(ح) تُطبق الحماية ضد العدوى وانتشار البرامجيات الضارة.
(ط) يُستخدم التسجيل الأمني والمراقبة، بما في ذلك إجراءات التصدي المناسبة.
(ي) تُرصد ثغرات التطبيقات والنُظم وتُتخذ التدابير المناسبة حيال ذلك.
(ك) تخضع كفاية التدابير وفعاليتها للاستعراض دورياً.
(ل) يتم إجراء تقييمات للثغرات في النُظم بصورة دورية.
(م) تُراقـب وسـائط التخزيـن القابلـة للنقـل وفقـاً لإجـراءات التشـغيل الأمنيـة، ولا يُسـمح بتوصيـل الأجهـزة المملوكـة ملكيـة خاصـة بالنُظـم والشـبكات.
(ن) يتـم الحفـاظ بصـورة صارمـة علـى الأصـول الرقميـة وتدابيـر الأمـن الحاسـوبي المرتبطـة بهـا باسـتخدام إجـراءات إدارة التغييـر المعمـول بهـا.
(س) تُطبق إجراءات النسخ الاحتياطي والتعافي المناسبة.
(ع) يُخصص جهاز خدمة لواحد بالضبط من مستويات الأمن الحاسوبي.
(ف) يُقيَّد الوصول المادي إلى المكونات والنُظم، بما فيها أجهزة الخدمة، تبعاً لوظائفها.
(ص) تُتخذ تدابير لمنع إدخال نُظم من دون إذن إلى نطاقات الأمن الحاسوبي.
(ق) لا يُسمح إلّا للمستخدمين المعتمدين والمؤهلين بإدخال تعديلات على النُظم.

متطلبات المستوى 1 من مستويات الأمن

17-8- بالإضافـة إلـى المتطلبـات العامـة، تُسـتخدم متطلبـات تدابيـر الوقايـة والحمايـة للنُظـم الحيويـة للمرفـق التـي تتطلـب أعلـى مسـتوى مـن الأمـن (مثـل نُظـم حمايـة المفاعـلات). ويمكـن أن تشـمل هـذه المتطلبـات مـا يلـي:

(أ) تُصمـم النُظـم وتُنفـذ لتكـون قابلـة للتحقـق منهـا وقابلـة للاختبـار ضـد أي هجـوم محتمـل مـن الخصـم.
(ب) لا يمكـن لأي تدفـق مـن تدفقـات البيانـات الشـبكية مـن أي نـوع مـن النُظـم المخصصـة لمسـتويات أمـن حاسـوبي أقـل صرامـة أن يدخـل نُظـم المسـتوى 1 عندمـا تكـون السـلامة والتوافـر مـن الأولويـات. ولا يمكـن إجـراء اتصـالات إلّا مـن الداخـل إلـى الخارج.

ويُنصح بشدة بعدم منح أي استثناء، ولا يمكن النظر فيها إلّا في أضيق الحدود لكل حالة على حدة وإذا كانت مؤيدة بتبرير كامل وتحليل للمخاطر الأمنية.[44]

(أ) لا يُسمح بإجراء أي صيانة عن بُعد.

(ب) يخضع الوصول المادي والمنطقي إلى النُظم لمراقبة صارمة ويُرصد ويُسجل.

(ج) يقتصر عدد الموظفين المسموح لهم بالوصول إلى النُظم على الحد الأدنى المطلق.

(د) تُطبق قاعدة الشخصين لمنع الأعمال غير المأذون بها من جانب أي تهديد داخلي.

(ه) تُسجل وتُرصد جميع الأنشطة وأحداث الأمن المحتملة.

(و) تصدر الموافقة على توصيل أجهزة التخزين الخارجية ويتم التحقق منها على أساس كل حالة على حدة.

(ز) تُطبق بصورة صارمة الإجراءات التنظيمية والإدارية على أي تعديلات، بما يشمل صيانة الأجهزة وتحديثات البرامجيات وتعديلاتها.

متطلبات المستوى 2 من مستويات الأمن

8-18- بالإضافة إلى المتطلبات العامة، ينبغي استخدام تدابير لوقاية النُظم وحمايتها، مثل نُظم المراقبة التشغيلية، التي تتطلب مستوى عالياً من الأمن. ويمكن أن تشمل هذه المتطلبات ما يلي:

(أ) لا يُسمح إلّا بتدفق البيانات عبر الشبكة من الداخل إلى الخارج في اتجاه أحادي من نُظم المستوى الثاني إلى نُظم المستوى 3. ولا يمكن قبول سوى رسائل الإقرار الضرورية أو رسائل الإشارات الخاضعة للمراقبة في الاتجاه المعاكس (إلى الداخل) (على سبيل المثال TCP/IP (بروتوكول التحكم في الإرسال/بروتوكول الإنترنت)).

(ب) لا يُسمح بالصيانة عن بُعد.

(ج) يقتصر عدد الموظفين الذين يُمنحون حق الوصول إلى النُظم على الحد الأدنى، مع تمييز واضح بين المستخدمين والموظفين الإداريين.

(د) يخضع الوصول المادي والمنطقي إلى النُظم لمراقبة صارمة ويتم توثيقه.

[44] لا تسمح بعض الدول الأعضاء بمنح استثناءات.

(هـ) يُمنع الوصول الإداري من مستويات الأمن الحاسوبي الأخرى. وإذا لم يكن ذلك ممكناً، تُفرض مراقبة صارمة على هذا الوصول (على سبيل المثال من خلال تطبيق قاعدة الشخصين والمصادقة الثنائية).

(و) تُتخذ جميع التدابير المعقولة لضمان سلامة النُظم وتوافرها.

متطلبات المستوى 3 من مستويات الأمن

8-19- بالإضافة إلى المتطلبات العامة، ينبغي استخدام متطلبات تدابير الوقاية والحماية للنُظم الآنية غير المطلوبة للعمليات (مثل نُظم الإشراف على العمليات في غرفة التحكم)، إذا كانت جميع هذه النُظم تنطوي على مستوى متوسط الشدة بالنسبة لمختلف تهديدات الفضاء الإلكتروني. ويمكن أن تشمل هذه المتطلبات ما يلي:

(أ) لا يُسمح بالوصول إلى الإنترنت من نُظم المستوى 3.

(ب) تُرصد مسارات تسجيل دخول الموارد الرئيسية وتُراجع سجلاتها.

(ج) تُستخدم بوابات الأمن لحماية هذا المستوى من وصلات البيانات غير الخاضعة للمراقبة من نُظم المستوى 4 والسماح فقط بنشاط محدد ومحدود.

(د) تُراقب الوصلات المادية المرتبطة بالنُظم.

(هـ) يُراقب الوصول المادي والمنطقي إلى النُظم ويتم توثيقه.

(و) يُسمح بالوصول لأغراض الصيانة عن بُعد لكل حالة على حدة، بشرط أن يخضع ذلك لمراقبة صارمة؛ وتُطبق على الحاسوب المتصل عن بُعد والمستخدم سياسة أمن محددة منصوص عليها في العقد.

(ز) تُراقب وظائف النظام المتاحة للمستخدمين من خلال آليات التحكم في الدخول وتبعاً لقاعدة 'الحاجة إلى المعرفة'. ويُنظر بعناية في أي استثناء لهذه القاعدة وتُستخدم وسائل أخرى لضمان الحماية (على سبيل المثال، الوصول المادي).

(ح) يُمنع الوصول الإداري من مستويات الأمن الحاسوبي الأخرى، حيثما أمكن ذلك. وإذا لم يكن ذلك ممكناً يخضع هذا الوصول لمراقبة صارمة (على سبيل المثال من خلال التحقق من الهوية باستخدام عاملين).

متطلبات المستوى 4 من مستويات الأمن

8-20- بالإضافة إلى المتطلبات العامة، ينبغي تطبيق متطلبات تدابير الأمن الحاسوبي على نُظم إدارة البيانات التقنية المستخدمة للصيانة أو إدارة أنشطة التشغيل المتصلة بالمكونات أو النُظم التي تقتضيها المواصفات التقنية للتشغيل (مثل تصريح العمل، وأمر العمل، وبطاقة تعليق الخدمة، وإدارة الوثائق)، إذا كانت هذه النُظم تحتاج إلى مستويات متوسطة من الأمن الحاسوبي. ويمكن أن تشمل هذه المتطلبات ما يلي:

(أ) لا يُسمح بالوصول إلى الإنترنت من نُظم المستوى 4.

(ب) تُستخدم بوابات الأمن لحماية هذا المستوى من اتصالات البيانات غير المأذون بها من خلال شركة خارجية موثوقة ومعتمدة أو شبكات المرفق، وللسماح بأنشطة محددة مأذون بها.

(ج) تُراقب الوصلات المادية المرتبطة بالنُظم.

(د) يُسمح بالصيانة عن بُعد ولكن بشرط خضوعها للمراقبة؛ وتُطبق على الحواسيب والمستخدمين الذين يعملون عن بُعد سياسة أمنية محددة منصوص عليها في العقد.

(هـ) تُراقب وظائف النظام المتاحة للمستخدمين من خلال آليات التحكم في الدخول. ويتم النظر بعناية في أي استثناء لهذه القاعدة، وتُستخدم وسائل أخرى لضمان الحماية.

(و) يُسمح بالوصول الخارجي عن بُعد إلى خدمات مختارة وللمستخدمين المعتمدين، بشرط وجود آليات مناسبة للتحكم في الدخول.

متطلبات المستوى 5 من مستويات الأمن

8-21- ينبغي استخدام المتطلبات التي تُحدد تدابير الأمن الحاسوبي للنُظم غير المهمة بشكل مباشر للمراقبة التقنية أو الأغراض التشغيلية (مثل نُظم التشغيل الآلي للمكاتب)، إذا كانت هذه النُظم تحتاج إلى مستويات منخفضة من الأمن الحاسوبي. ويمكن أن تشمل هذه المتطلبات ما يلي:

(أ) لا يقل مستوى الأمن الحاسوبي عن مستوى الحماية الأساسي المحدد وفقاً لأحدث ما توصلت إليه التكنولوجيا.

(ب) لا يُسمح إلّا للمستخدمين المؤهلين والمعتمدين بإدخال تعديلات على النُظم.

(ج) يُسمح بالوصول إلى الإنترنت من نُظم المستوى 5، بشرط تطبيق تدابير الوقاية والحماية المناسبة.

(د) يُسمح بالوصول الخارجي عن بُعد للمستخدمين المأذون لهم، بشرط تطبيق التدابير المناسبة.

(ه) تُراقب التوصيل المادي لأجهزة الأطراف الثالثة بالنُظم والشبكات وتُحدد خصائص هذه التفاعلات مع نُظم المستويات الأعلى وتُقيَّم بصورة مستقلة لضمان الامتثال لبنية الأمن الحاسوبي.

التذييل

عناصر مختارة من برنامج الأمن الحاسوبي

ألف-1- يُقدم هذا التذييل أمثلة لمجموعة مختارة من عناصر برنامج الأمن الحاسوبي للاستخدام مع النهج القائم على الأداء في الأمن الحاسوبي. ويمكن أن يحتاج المشغِّل إلى تعديل هذه العناصر لكي تُعبِّر عن ظروف تنظيمية معيّنة أو الظروف الخاصة بالمرفق، ولكن الأمثلة تغطي جميع أنواع المعلومات التي يحتاج إليها المشغِّل بوضع برنامج أمن حاسوبي فعال وتنفيذه.

ألف-2- ينبغي أن يطلب المشغِّل هذه العناصر أو ما يشابهها لتيسير التفاهم بين الوحدات التنظيمية والبائعين والمتعهدين والموردين والسلطات المختصة. وقد يتعيّن تكييف العناصر مع الخصائص المحددة للمنظمة المشغِّلة والمرفق لتحسين التفاهم.

التنظيم والمسؤوليات في المرفق

الإدارة

ألف-3- تضع الإدارة العليا في المرفق سياسة للأمن الحاسوبي وكذلك عمليات وآليات داعمة لضمان تنفيذ السياسية. وتحقيقاً لهذه الغاية، ينبغي أن تتخذ الإدارة العليا الخطوات التالية:

(أ) تحمل المسؤولية العامة عن جميع جوانب الأمن الحاسوبي.
(ب) تحديد الأهداف الأمنية للمرفق.
(ج) ضمان الامتثال للقوانين واللوائح ذات الصلة.
(د) الحفاظ على الوعي بالتهديد الحالي للأمن والاتجاهات المرتبطة به.
(هـ) تحديد مستوى تقبل المخاطر في المرفق.
(و) تخصيص المسؤوليات التنظيمية فيما يتصل بالأمن الحاسوبي.
(ز) ضمان التواصل الكافي بين الأفراد المسؤولين عن مختلف جوانب الأمن النووي.
(ح) ضمان الامتثال لسياسة الأمن الحاسوبي.

(ط) توفير ما يكفي من الموارد لتنفيذ برنامج أمن حاسوبي مستدام.
(ي) ضمان إجراء استعراضات وتحديثات دورية لسياسة الأمن الحاسوبي وإجراءاته.
(ك) ضمان دعم برامج التدريب والتوعية.

أخصائي الأمن الحاسوبي

ألف-4- ينبغي أن يسند المشغِّل المسؤولية العامة عن الأمن الحاسوبي في المرفق إلى فرد واحد أو إلى مجموعة واحدة. وفي هذا المنشور، يُستخدم لقب 'أخصائي الأمن الحاسوبي' لتحديد هذا الدور.[1]

ألف-5- وينبغي أن ينسق أخصائي الأمن الحاسوبي عن كثب مع الأنشطة في المرفق برمته، وعلى نحو مستقل. وينبغي أن يكون لأخصائي الأمن الحاسوبي تسلسل إداري واضح ويمكنه من الوصول مباشرة إلى الإدارة العليا نظراً لأن الأمن الحاسوبي يمكن أن يؤثر على جميع أنشطة المرفق تقريباً.

ألف-6- وينبغي أن تُحدد بوضوح مسؤوليات الأمن الحاسوبي داخل الإدارات التنظيمية المختلفة وينبغي التنسيق بينها لتجنب الثغرات أو أوجه التضارب، ولضمان تنفيذ الأمن الحاسوبي بصورة متسقة. ومن الضروري بصفة خاصة تحقيق ذلك إذا كان دور أخصائي الأمن الحاسوبي مستنداً إلى مجموعة وليس إلى فرد واحد. وينبغي أن يُشكل أخصائي الأمن الحاسوبي سلطة واحدة داخل المنظمة المشغِّلة وأن يكون مسؤولاً عن معالجة المسائل على نطاق المنظمة وحل أي تضارب قد ينشأ.

ألف-7- وينبغي أن يكون لدى أخصائي الأمن الحاسوبي معرفة متعمقة بالأمن الحاسوبي ودراية جيدة بسائر جوانب الأمن في المرافق النووية، وينبغي أيضاً أن تكون لديه معرفة بالأمان النووي وإدارة المشروعات وينبغي أن تكون لديه القدرة على إدماج الأشخاص من مختلف التخصصات في فريق فعال.

ألف-8- وينبغي أن تكون لأخصائي الأمن الحاسوبي السلطة والمسؤولية عن إدارة برنامج الأمن الحاسوبي.

---

[1] يمكن في حالات أخرى الإشارة إلى هذه الوظيفة باسم 'موظف الأمن الحاسوبي' أو 'رئيس موظفي أمن المعلومات'، أو 'موظف أمن تكنولوجيا المعلومات'، أو 'موظف أمن المعلومات'، أو يمكن أن تُسند إليها أدوار متعددة.

ألف-9- وتشمل المسؤوليات النمطية المحددة لأخصائي الأمن الحاسوبي ما يلي:

(أ) إسداء المشورة إلى الإدارة العليا بشأن الأمن الحاسوبي.
(ب) قيادة فريق الأمن الحاسوبي.
(ج) تعزيز الأمن الحاسوبي داخل المنظمة، بما في ذلك التحسينات عند الضرورة.
(د) تنسيق ومراقبة تطوير أنشطة الأمن الحاسوبي (على سبيل المثال، تنفيذ سياسة الأمن الحاسوبي، والتوجيهات والمبادئ التوجيهية المحددة، والإجراءات، وفي نهاية المطاف، تدابير الأمن الحاسوبي).
(هـ) التنسيق مع موظفي الحماية المادية وسائر أفراد الأمن والأمان لتخطيط تدابير الأمن الحاسوبي وتحديدها، بما يشمل التدابير التي تتصدى لحادثات الأمن الحاسوبي.
(و) تحديد النُظم الحاسمة الأهمية للأمن الحاسوبي داخل المرفق (أي النُظم التي توفِّر تدابير الأمن الحاسوبي الأساسي). وينبغي أن تكون الجهات المسؤولة عن الأصول على علم بدور معداتها في الأمن الحاسوبي.
(ز) إجراء تقييمات دورية لمخاطر الأمن الحاسوبي بصورة مستقلة عن الموظفين التشغيليين.
(ح) إجراء عمليات تفتيش ومراجعات واستعراضات دورية لتدابير الأمن الحاسوبي الأساسي وتقديم تقارير عن الحالة إلى الإدارة العليا.
(ط) إعداد وترتيب التدريب على الأمن الحاسوبي وتأهيل الأفراد المعنيين.
(ي) التحضير لعمليات التصدي لحادثات الأمن الحاسوبي وقيادتها، بما يشمل التنسيق مع الموظفين الداخليين والخارجيين المعنيين بالتصدي.
(ك) التحقيق في حادثات الأمن الحاسوبي ووضع إجراءات تصحيحية في أعقاب الحادثات.
(ل) المشاركة في تقييم الأمن العام للمرفق.
(م) المشاركة في تحليل متطلبات النُظم الجديدة القائمة على الحاسوب.

فريق الأمن الحاسوبي

ألف-10- ينبغي أن يحدد المشغِّل موظفي فريق الأمن الحاسوبي وأن يعينهم. ويمكن أن يكون هذا الفريق مؤلفاً من مجموعة ثابتة من الأفراد أو يمكن أن يشمل أفراداً لديهم خبرة محددة بحسب ما تقتضيه الحاجة. ويدعم الفريق أخصائي الأمن الحاسوبي في أداء مسؤولياته: يحتاج أخصائي الأمن الحاسوبي إلى الحصول على الخبرة في جميع

التخصصات المرتبطة بالأمن الحاسوبي، بما فيها أمان المرفق وعمليات المنشأة والحماية المادية والأمن المتصل بالأفراد.

ألف-11- وينبغي أن يكون أعضاء فريق الأمن الحاسوبي مسؤولين عن تعزيز الأمن الحاسوبي، كل في وحدته داخل المنظمة.

ألف-12- وتشمل أنشطة فريق الأمن الحاسوبي الاضطلاع بدور فاعل في رصد الأصول الرقمية، بما في ذلك الأصول الرقمية الحساسة، للتعرف على أي مؤشرات تدل على هجوم محتمل على الفضاء الإلكتروني، وتنسيق التصدي لحادثات الأمن الحاسوبي. وقد يشمل ذلك تعيين موظفين في مركز لعمليات الأمن لرصد حادثات الأمن الحاسوبي المحتملة وتقييمها، وللشروع في أنشطة التصدي ودعمها، وهو ما قد يحتاج أيضاً إلى دعم من منظمات أخرى.

مسؤوليات الإدارة الأخرى

ألف-13- ينبغي أن يضمن المديرون على مختلف المستويات داخل المنظمة إيلاء العناية المناسبة للأمن الحاسوبي داخل نطاق مسؤولياتهم. وتشمل المسؤوليات النمطية للمديرين، كل في مجال تخصصه، ما يلي:

(أ) فهم أهمية الأمن الحاسوبي ودوره في الأمن النووي؛
(ب) العمل وفقاً للمتطلبات والعمليات المحددة في برنامج الأمن الحاسوبي؛
(ج) توفير المتطلبات التشغيلية والتعقيبات إلى الإدارة العليا فيما يتصل بالأمن الحاسوبي، وحل أي أوجه تضارب بين المتطلبات التشغيلية والمتطلبات المتعلقة بالأمن والأمان؛
(د) تنبيه الإدارة العليا إلى أي ظروف يمكن أن تفضي إلى تغييرات في مستوى الأمن الحاسوبي، مثل التغييرات في الأفراد أو المعدات أو العمليات؛
(ه) ضمان توفير التدريب الكافي للموظفين وإحاطتهم بمسائل الأمن الحاسوبي ذات الصلة بأدوارهم؛
(و) التأكد من أن البائعين والمتعهدين والموردين الذين يعملون لديهم يلتزمون بالمتطلبات والعمليات المحددة في برنامج الأمن الحاسوبي؛
(ز) تتبع حادثات الأمن الحاسوبي ورصدها والتصدي لها والإبلاغ عنها؛
(ح) إنفاذ تدابير الأمن الحاسوبي.

المسؤوليات الفردية

ألف-14- ينبغي أن يكون كل فرد داخل المنظمة مسؤولاً عن أداء مهامه الخاصة بما يتفق مع برنامج الأمن الحاسوبي. وتشمل المسؤوليات المحددة ما يلي:

(أ) فهم أهمية الأمن الحاسوبي ودوره في الأمن النووي؛
(ب) فهم سياسة المنظمة بشأن الأمن الحاسوبي؛
(ج) معرفة إجراءات الأمن الحاسوبي ذات الصلة بعمله؛
(د) العمل في حدود القيود التي تنطوي عليها سياسة الأمن الحاسوبي؛
(هـ) إخطار المديرين بأي تغييرات قد تؤثر تأثيراً ضاراً على الأمن الحاسوبي؛
(و) إخطار جهات الاتصال ذات الصلة والمديرين بأي حادثات فعلية أو بأي حادثات محتملة تنطوي على إخلال بالأمن الحاسوبي؛
(ز) حضور التدريب الأوّلي على الأمن الحاسوبي والتدريب التنشيطي بانتظام.

المسؤوليات المشتركة بين الإدارات

ألف-15- يُمثل الأمن الحاسوبي مجالاً متعدد التخصصات يؤثر على كثير من الوحدات والأنشطة التنظيمية المختلفة ويتأثر بها. ويحتاج الأمن الحاسوبي إلى تنسيق وتعاون وثيقين بين الوحدات التنظيمية المختلفة لكي يكون فعالاً. وتصف الفقرات من 16 إلى 38 بعض مسؤوليات الإدارات والمسائل الشاملة.

الحماية المادية

ألف-16- تُعد خطة أمن الموقع وبرنامج الأمن الحاسوبي كلاهما ضروريان لوضع خطة أمن شاملة للمرفق، ويتعيّن بالتالي أن يُكمِّل منهما الآخر. وتحمي متطلبات التحكم في الدخول المادي الأصول الرقمية الحساسة، ويمكن أن يفضي الإخلال بالنُظم القائمة على الحاسوب إلى تدهور وظائف الحماية المادية أو فقدانها. وعلاوة على ذلك، قد يسعى الخصوم إلى مهاجمة مرفق ما من خلال هجوم على الفضاء الإلكتروني وهجوم مادي منسقين (أي هجوم مختلط).

ألف-17- وإذا كانت الوحدات التنظيمية المسؤولة عن خطة أمن الموقع وبرنامج الأمن الحاسوبي مختلفة، ينبغي أن يحدث تواصل بينها وأن تُنسق جهودها لضمان الاتساق بين الخطط أثناء وضعها واستعراضها.

ألف-18- وينبغي أن يُسند المشغِّل إلى موظفي الحماية المادية الأدوار والمسؤوليات ذات الصلة في وضع برنامج الأمن الحاسوبي وتنفيذه وتعهده. ويشمل ذلك ما يلي:

(أ) ضمان الوصول إلى الأصول الرقمية الحساسة إلّا للأشخاص المأذون لهم؛
(ب) تحديد وسائط التخزين القابلة للنقل والأجهزة المحمولة غير المأذون بها التي تدخل المرفق؛
(ج) تحديد نقل المعلومات أو أصول المعلومات من دون إذن من المرفق؛
(د) ضمان تطبيق السياسات المطبقة على أي وسائط تخزين قابلة للنقل وأي أجهزة محمولة مسموح بها في المرفق (على سبيل المثال، إجراء مسح لاكتشاف أي برامجيات خبيثة قبل الدخول إلى المرفق)؛
(ه) الإبلاغ عن حادثات الأمن الحاسوبي (على سبيل المثال، كشف برامجيات خبيثة، أو نقل أصول معلومات من دون إذن) وفقاً لإجراء التصدي للحادثات؛
(و) تقييم ممارسات أمن المعلومات (على سبيل المثال، تفتيش المكاتب، وتفتيش الغرف والمقصورات المغلقة، وتوفير معايير للأجهزة تنص على الحماية المادية لأصول المعلومات، والتحكم في الدخول ورصده)؛
(ز) دعم التصدي لحادثات الأمن الحاسوبي المتصلة بنظام الحماية المادية.

تكنولوجيا المعلومات

ألف-19- يتولى موظفو تكنولوجيا المعلومات أداء مهام الدعم والإدارة والمهام الإدارية داخل المرفق النووي. ويمكن أن تشمل هذه المهام أنشطة تنطوي على أصول رقمية مستخدمة في إعداد وتخزين إجراءات التشغيل والصيانة، وتعليمات العمل، ونُظم تنظيم نسق المكونات، ووثائق التصميم، وأدلة التشغيل.

ألف-20- وينبغي أن يُحدد برنامج الأمن الحاسوبي بوضوح الأصول الرقمية والشبكات المرتبطة بها التي تقع المسؤولية عنها على عاتق موظفي تكنولوجيا المعلومات. وينبغي أن يقوم موظفو تكنولوجيا المعلومات برصد الأصول الرقمية المحددة والشبكات المرتبطة

بهـا والإبـلاغ عـن أي حادثـات متصلـة بالأمـن الحاسـوبي إلـى الإدارة العليـا وأخصائـي الأمـن الحاسـوبي وفقـاً لخطـة التصـدي للحادثـات.

ألف-21- وينبغـي أن يتخـذ موظفـو تكنولوجيـا المعلومـات إجـراءات لضمـان عـدم انتشـار حادثـات الأمـن الحاسـوبي المنطويـة علـى أصـول رقميـة (ولكنهـا لا تنطـوي علـى أصـول رقميـة حساسـة) وشـبكاتها لضمـان عـدم تأثيرهـا علـى الأصـول الرقميـة الحساسـة.

الهندسة

ألف-22- ينبغـي أن تكـون لـدى الموظفيـن الهندسـيين عمليـات رسـمية لضمـان التنسـيق مـع الوحـدات التنظيميـة الأخـرى ذات الصلـة مـن أجـل ضمـان تصميـم تدابيـر الأمـن النـووي والأمـان النـووي وتنفيذهـا علـى نحـو متكامـل وفقـاً للمتطلبـات المحـددة فـي برنامـج الأمـن الحاسـوبي. وينبغـي أن يُـدرك الموظفـون فـي مجـال الهندسـة أن الأمـان والحمايـة الماديـة والأمـن الحاسـوبي مبـادئ كل منهـا مختلـف عـن الآخـر وتحتـاج إلـى دعـم مـن خبـراء مؤهليـن تأهيـلاً مناسـباً فـي هـذه التخصصـات المختلفـة.

ألف-23-وينبغـي أن يُقـدم الموظفـون فـي مجـال الهندسـة أدلـة علـى فعاليـة بنيـة الأمـن الحاسـوبي (أي بنيـة الأمـن الحاسـوبي الدفاعيـة) التـي يمكـن مقارنتهـا مـع النتائـج المتوقعـة علـى أسـاس عمليـة إدارة مخاطـر الأمـن الحاسـوبي للمرفـق والنظـام.

ألف-24- وينبغـي أن يتولـى الموظفـون فـي مجـال الهندسـة قيـادة عمليـة إدارة مخاطـر الأمـن الحاسـوبي للنظـم أو دعمهـا لنُظـم المرفـق التـي يكونـون مسـؤولين عنهـا.

ألف-25- وينبغـي أن يُقـدم الموظفـون فـي مجـال الهندسـة التوجيـه للبائعيـن والمتعهديـن والموردييـن فيمـا يتعلـق بمتطلبـات الأمـن الحاسـوبي داخـل نُظـم المرفـق. وتقـع علـى الموظفيـن الهندسـيين مسـؤولية اسـتعراض تصاميـم البائعيـن للتأكـد مـن تلبيتهـا متطلبـات الأمـن الحاسـوبي. وينبغـي أن يحصـل الموظفـون فـي مجـال الهندسـة علـى تأكيـد مـن البائـع بـأن المنتجـات المـوردَة للمرفـق قـد طـوِّرت فـي بيئـة آمنـة. وينبغـي أن يضـع الموظفـون فـي مجـال الهندسـة إجـراءات واتباعهـا لاسـتعراض الوثائـق التقنيـة للمنتـج، وقبـول شـحنات المنتـج فـي الموقـع، واختبـار المنتجـات لضمـان تلبيـة متطلبـات الأمـن الحاسـوبي.

ألف-26- وينبغي أن يضمن الموظفون في مجال الهندسة وجود أنشطة لرصد الأداء وتطبيقها لتأكيد استمرار فعالية تدابير الأمن الحاسوبي.

العمليات

ألف-27- ينبغي أن يحدد برنامج الأمن الحاسوبي نُظم المرفق وشبكاته التي تقع المسؤولية عنها على عاتق موظفي العمليات. وتقع على موظفي العمليات المسؤولية عن الامتثال للمتطلبات المحددة لهذه النُظم في برنامج الأمن الحاسوبي.

ألف-28- وينبغي أن يضمن موظفو العمليات الحفاظ على بنية الأمن الحاسوبي الدفاعية وتدابير الأمن الحاسوبي الواقعة تحت مسؤولياتهم وبقاءها فعالة.

ألف-29- وينبغي أن يضمن موظفو العمليات وجود إجراءات وتنفيذها لتحديد حادثات الأمن الحاسوبي والشروع في تقديم استجابة للنُظم والشبكات الواقعة تحت مسؤوليتهم.

ألف-30- وينبغي أن يعزز موظفو العمليات الإلمام بالحالة لضمان عدم استخدام سوى وسائط التخزين القابلة للنقل والأجهزة المحمولة المأذون بها داخل المرفق.

تنظيم الشراء وسلسلة الإمداد

ألف-31- ينبغي شراء المنتجات لتلبية المواصفات الخاصة بالمعدات أو الأجهزة أو المكونات. وينبغي أن تشمل المواصفات متطلبات أمن حاسوبي مناسبة.

ألف-32- وينبغي أن تشمل عمليات الشراء فحوص للتأكد من أن الأصول الرقمية الحساسة التي يطورها أو يوردها البائعون والموردون تشمل تدابير أمن حاسوبي متسقة مع كل مستوى من مستويات الأمن الحاسوبي المخصصة لكل أصل من الأصول الرقمية الحساسة.

ألف-33- وينبغي أن يفهم موظفو المشتريات أهمية وجود متطلبات أمن حاسوبية محددة في عمليات الشراء. وينبغي إنفاذ هذه المتطلبات من خلال اتفاقات قانونية مع البائعين والمتعهدين والموردين، مثل التراخيص أو العقود.

ألف-34- وقد لا يكون موظفو المشتريات والموظفون في مجال الهندسة على علم بأن جهازاً من الأجهزة المستخدمة في الأغراض العامة سيُصنف كأصل من الأصول الرقمية الحساسة إذا كان المشغِّل يستخدمه في تطبيق معيّن. وفي هذه الحالات، ينبغي عند شراء هذه الأجهزة مراعاة إمكانية استخدامها كأصول رقمية حساسة، وينبغي تطبيق متطلبات الأمن الحاسوبي المناسبة.

ألف-35- وينبغي أن يعمل موظفو المشتريات مع الموظفين في مجال الهندسة لضمان تحديد متطلبات الأمن الحاسوبي كمتطلبات تعاقدية للبائعين أو المتعهدين أو الموردين، ولضمان تلبية التصاميم المقدمة من البائعين أو المتعهدين أو الموردين متطلبات الأمن الحاسوبي. وينبغي أن يقوم أيضاً بإبلاغ الموظفين في مجال الهندسة بما إذا كان الدعم المقدم من البائع أو المتعهد أو المورِّد لأصل رقمي حساس لم يعد متاحاً أو يبدو من المرجح أنه لم يعد متاحاً.

ألف-36- وينبغي أن ينظر موظفو المشتريات في إجراء استعراضات للبائعين والمتعهدين والموردين قبل الدخول في اتفاقات تعاقدية. ويمكن أن تشمل هذه الاستعراضات تحليل العمليات التي يستخدمها البائع أو المتعهد أو المورِّد لتصميم الأصول الرقمية الحساسة أو تطويرها أو اختبارها أو تنفيذها أو دعمها، أو تقييم مستوى التدريب والخبرة لدى البائع أو المتعهد أو المورِّد في تطوير الأصول الرقمية الحساسة بحيث تُلبي مستويات الأمن الحاسوبي المطلوبة. ويمكن أن تساعد الاستعراضات في (أ) تحديد ما إذا كان البائعون أو المتعهدون أو الموردون الرئيسيون لديهم تدابير أمنية لتقييم الجدارة بالثقة للبائعين والمتعهدين والموردين التابعين لهم بشكل صحيح، و(ب) ضمان التحقق من منشأ الأصول الرقمية الحساسة، ومكونات الأصول الرقمية الحساسة، والبرامجيات الحاسوبية، والتحديثات المقدمة إلى المشغِّل.

ألف-37- وينبغي أن يضمن موظفو المشتريات أن جميع بائعي ومتعهدي وموردي الأصول الرقمية الحساسة لديهم إجراءات معمول بها لإخطار المشغِّل في حال وقوع أي حادثات في سلسلة الإمداد يمكن أن تؤثر على الأصول الرقمية الحساسة (على سبيل المثال، الإخلال بمكونات الأصول الرقمية الحساسة، أو تكنولوجيا الأصول الرقمية الحساسة، أو عمليات التطوير أو المعلومات الحساسة).

ألف-38- وينبغي أن يأخذ موظفو المشتريات في الاعتبار التأكد من أن بائعي ومتعهدي وموردي الأصول الرقمية الحساسة لديهم طريق توزيع موثوق لتسليم الأصول الرقمية

الحساسة ومكونات الأصول الرقمية الحساسة والبرامجيات الحاسوبية والتحديثات إلى المشغِّل.

إدارة المخاطر والثغرات والامتثال

العلاقات والتفاعلات الخارجية اللازمة لإدارة المخاطر

ألف-39- ينبغي أن تشمل عمليات إدارة المخاطر تحليلاً للعلاقات الخارجية (أي مع البائعين والمتعهدين والموردين). وينبغي أن تُحدد في الترتيبات التعاقدية المسؤوليات والمساءلات عن تلبية المتطلبات المستمدة من عملية إدارة مخاطر الأمن الحاسوبي للنظم.

ألف-40- وينبغي أن يجري المشغِّل مراجعة وفحصاً للأنشطة ذات الصلة للبائعين والمتعهدين والموردين للتأكد من تلبية متطلبات الأمن الحاسوبي المنصوص عليها في برنامج الأمن الحاسوبي. وينبغي أن تشترط العقود المبرمة مع البائعين والمتعهدين والموردين السماح للمشغِّل بإداء هذه الأنشطة.

ألف-41- وينبغي أن تأخذ عمليات إدارة المخاطر التي يُجريها المشغِّل في الاعتبار المتطلبات الرقابية والمتطلبات الخارجية الأخرى التي تؤثر على الأمن الحاسوبي. وينبغي أن يتيح المشغِّل للسلطات المختصة ذات الصلة الإشراف وإجراء عمليات تفتيش فيما يتعلق بالتدابير اللازمة لتلبية هذه المتطلبات.

ضمان الأمن الحاسوبي

ألف-42- ينبغي إجراء أنشطة ضمان الأمن الحاسوبي طوال عمر المرفق على النحو الموضح في القسمين 4 و5. وستختلف أنشطة الضمان المحددة وفقاً للمرحلة في العمر. ويتضمن المرجع [8] تفاصيل أنشطة الضمان المنطبقة على نُظم الأجهزة والتحكم.

ألف-43- وقد تشمل هذه الأنشطة التي يُجريها المشغِّل تقييمات (بما فيها عمليات مراجعة) واستعراضات وتمارين واختبارات.[2]

ألف-44- وينبغي أن يتحقق المشغِّل من أن برنامج الأمن الحاسوبي متسق مع سياسة المشغِّل للأمن الحاسوبي (على سبيل المثال، يمكن استخدام تقييم الأمن الحاسوبي للتحقق من تلبية متطلبات الأمن الحاسوبي التي تُعبِّر عن سياسة المشغِّل). ويمكن أن يشمل ذلك عدداً من التقييمات التكميلية لتقييم مختلف عناصر برنامج الأمن الحاسوبي وتنفيذها. وستشمل مخرجات التقييم تحديد أوجه القصور والممارسات الجيدة واقتراحات التحسين.

ألف-45- وينبغي أن تُشكل هذه الأنشطة الأساس للتحسين المستمر لبرنامج الأمن الحاسوبي. ويتطلب دعم ذلك أن تكون أنشطة الضمان قابلة للتكرار وموثوقة، وينبغي إجراؤها بصورة دورية، وكذلك عند وقوع حادثة متصلة بالأمن الحاسوبي أو عند حدوث تغييرات في التهديد.

ألف-46- وينبغي أن تشمل أنشطة الضمان تقييم الفعالية التنظيمية والتدابير الموضوعة لضمان التنفيذ السليم للأمن الحاسوبي وفعاليته.

ألف-47- ويمكن أن تتولى مجموعات داخلية أو خارجية إجراء أنشطة الضمان: على سبيل المثال، يمكن أن يتولى إجراء تقييم الأمن الحاسوبي فريق داخلي كنشاط من أنشطة التقييم الذاتي. وفي حال إجراء التقييم من جانب مجموعات خارجية، يتعيّن التحقق من النتائج داخلياً.

ألف-48- وينبغي استكمال أنشطة الضمان الداخلية والخارجية بتقييمات مستقلة تُجريها أطراف خارجية. وسيحتاج المقيمون المستقلون إلى الوصول إلى الموظفين المعنيين والوثائق والمعدات ذات الصلة. ويمكن أن يكون المقيّمون المستقلون أعضاء في المنظمة المشغِّلة أو من خارجها، ولكن يتعيّن أن يكونوا مستقلين عن الأشخاص الذين تولوا إجراء العمل الذي يتم تقييمه والذين قاموا بالتحقق منه والإشراف عليه.

---

[2] يمكن أيضاً استخدام التمارين والاختبارات مع سائر عناصر برنامج الأمن الحاسوبي، مثل إجراءات الأمن وإدارة شؤون الموظفين.

ألف-49- وينبغي تحديد الجدارة بالثقة للمقيمين المستقلين أو الخارجيين قبل السماح لهم بالاطلاع على المعلومات أو الوصول إلى المرفق، إذ من المرجح أن تشمل أنشطة الضمان معلومات حساسة عن الأمن الحاسوبي. ويرد مزيد من المعلومات عن تقييمات الجدارة بالثقة في المرجع [6].

ألف-50- وينبغي أن تشمل إجراءات التقييم المستقل قيوداً مناسبة على نقل المعلومات الحساسة واستخدامها وخزنها وتوزيعها، وينبغي أن تنص على تدمير هذه المعلومات عندما لا تكون هناك حاجة إليها.

ألف-51- وينبغي تطوير القدرات في مجال إجراء أنشطة الضمان والحفاظ عليها لمواكبة التغيُّرات في التكنولوجيا وتهديد الفضاء الإلكتروني. وهذه القدرات مطلوبة للموظفين الذين يقومون بإجراء أنشطة الضمان والسلطة المختصة التي قد تحتاج إلى استعراض نتائج هذه الأنشطة.

نطاق التقييم

ألف-52- ينبغي أن يحدد المشغِّل نطاق التقييم من حيث المجالات الوظيفية والأمنية.

ألف-53- وينبغي أن يكون نطاق التقييم ملائماً لمرحلة عمر المرفق. ومن ذلك على سبيل المثال أن التقييم الكامل للأمن الحاسوبي قد يكون مطلوباً أثناء بعض المراحل، في حين أنه قد يكون من الأنسب إجراء تقييم لمجالات وظيفية أو أمنية محددة في مراحل أخرى. (يُحدد المرجع [8] أنشطة التقييم في مختلف النقاط في دورة عمر نظام الأجهزة والتحكم).

تقنيات التقييم

ألف-54- ينبغي أن يستخدم فريق التقييم التقنيات التالية، بحسب الاقتضاء، للحصول على المعلومات التي يحتاج إليها الفريق للتوصل إلى استنتاجاته وتوصياته:

(أ) استعراض الوثائق والسجلات (مثل التشريعات واللوائح وسجلات المرفق)؛
(ب) المقابلات مع الموظفين من المنظمات ذات الصلة، مثل موظفي السلطة المختصة، وموظفي التشغيل في المرفق وممثلي المنظمات الأخرى؛

(ج) الملاحظة المباشرة للمنظمة وممارساتها ونُظمها، ولتنفيذ تدابير الأمن الحاسوبي.

إعداد تقرير التقييم

ألف-55- يتألف مكون جمع البيانات اللازمة للتقييم من تسجيل الملاحظات والبيانات ذات الأهمية المستمدة من استعراض الوثائق والسجلات، والمقابلات مع الموظفين، والملاحظات المباشرة. وقد تكون ملاحظات بعينها مهمة، ولكنها قد تُشكل أيضاً مؤشراً جماعياً على اتجاهات سائدة في المرفق أو المنظمة قد تحتاج إلى معالجة. ولذلك، ينبغي أن يحدد المشغِّل الملاحظات التي تؤيد النتائج التي تُشير إلى اتجاهات أو مسائل متكررة.

ألف-56- وينبغي تحليل الملاحظات عن طريق مقارنتها مع المتطلبات، مثل اللوائح الوطنية، والإجراءات التنظيمية، ومعايير الصناعة، بحسب الاقتضاء. وتُحدد النتيجة إذا كان هناك عدم امتثال لمتطلبات رقابية أو إجراء داخلي. وينبغي وضع أساس واضح والاتفاق عليه لتحديد النتائج أثناء مرحلة التخطيط والتقييم.

ألف-57- ولا تُسفر الملاحظات دائماً عن نتائج، ولا تكون جميع النتائج سلبية. ويمكن أن تشمل تحديد ممارسات جيدة أو ممارسات أو إجراءات تنظيمية توفِّر طريقة فعالة وجديدة عموماً لتحقيق أهداف الأمن. ويمكن تحديد الممارسات الجيدة التي يمكن أن تأخذ بها المنظمات الأخرى لتحسين أمنها الحاسوبي، والإبلاغ عن هذه الممارسات.

ألف-58- وبالإضافة إلى النتائج والممارسات الجيدة، يمكن أيضاً لفريق التقييم تقديم توصيات واقتراحات متصلة بالنتائج الواردة في تقرير التقييم.

ألف-59- وتوفِّر التوصيات مبادئ توجيهية لتلبية المتطلبات القانونية والرقابية أو المعايير الدولية (على سبيل المثال، الالتزامات بموجب الاتفاقيات) عند الاقتضاء. ولا تشمل التوصيات في العادة طريقة تصحيح مشكلة ما، بل تُشير فقط إلى الحاجة إلى تصحيح المشكلة.

ألف-60- وتوفِّر الاقتراحات مستوى إضافياً من المعلومات المتعلقة بالنتائج، بما في ذلك التدابير التصحيحية أو التخفيفية المقترحة. ولا تُستمد هذه المعلومات بالضرورة

مـن التوجيهـات الرقابيـة، ولكنهـا تُسـتمد فـي الأغلـب مـن المعاييـر التقنيـة للصناعـة ومـن الممارسـات الجيـدة.

مثال لأسلوب من أساليب التقييم

ألف-61- يصـف المرجـع [23] مثـالاً لأحـد أسـاليب التقييـم. ويوفِّـر هـذا المثـال تقييمـاً شـاملاً لعـدة ميادين للعمليـات الوظيفيـة للمرفـق وأمنـه الحاسـوبي. ويسـاعد ذلـك فـي ضمان تغطيـة العمليـات والنُظـم التـي تـؤدي وظائـف فـي المرفـق، بمـا فـي ذلـك العمليـات، والأمـان، والأمـن، والاسـتعداد للطـوارئ والتصـدي لهـا.

إدارة الأصول الرقمية

خطة تنظيم نسق المكونات

ألف-62- ينبغـي أن تُـدار تدابيـر الأمـن الحاسـوبي التـي تحمـي الأصـول الرقميـة الحساسـة وفقـاً لخطـة لتنظيـم نسـق المكونـات. وينبغـي وضـع هـذه الخطـة وتنفيذهـا مـن جانـب المشـغِّل، وينبغـي أن تشـمل التدابيـر التاليـة:

(أ) تخصيـص الأدوار والمسـؤوليات ذات الصلـة، وتحديـد العمليـات والإجـراءات الخاصـة بتنظيـم نسـق المكونـات.
(ب) تحديد تفاصيل نسق مكونات الأصول الرقمية الحساسة وتفاعلاتها.
(ج) تحديد الوقت في دورة حياة تطوير النظام الذي يتم فيه تنظيم نسق المكونات.
(د) وضـع الوسـائل اللازمـة لتحديـد الأصـول الرقميـة الحساسـة وتحديـد عمليـة لإدارة تدابيـر الأمـن الحاسـوبية اللازمـة لحمايتهـا.

النسق الأساسي للمكونات

ألف-63- ينبغـي الحفـاظ علـى مراقبـة النسـق الأساسـي القائـم الخـاص بالأصـول الرقميـة الحساسـة. وينبغـي تحديـث نسـق المكونـات الأساسـي بحسـب الضـرورة علـى أسـاس مراقبـة أداء النظـام، وبحيـث يُعبِّـر، علـى سـبيل المثـال، عـن تحصيـن النظـام أو تأثيـر التعديـلات علـى الأمـن الحاسـوبي.

تحصين النظام

ألف-64- ينبغي أن ينظر المشغِّل في وضع عملية منهجية لتحصين نظام الأصول الرقمية الحساسة. ويعني تحصين النظام تطبيق مجموعة من تدابير التحكم الإداري والتقني المصممة لجعل مكونات النظام الحاسوبي أقل عرضة للهجمات على الفضاء الإلكتروني عن طريق الإلغاء أو التعطيل لمكونات الأجهزة والبرامجيات الحاسوبية غير الضرورية لتشغيل النظام أو صيانته. وتشمل الأجهزة والبرامجيات الحاسوبية تلغى أو تعطل في العادة ما يلي:

(أ) واجهات الشبكة أو بروتوكولاتها غير المستخدمة (بما في ذلك برمجية التشغيل)؛
(ب) المكونات الطرفية غير المستخدمة (بما في ذلك تعطيل برامجيات التشغيل)؛
(ج) دعم وسائط التخزين القابلة للنقل؛
(د) الاتصالات السلكية واللاسلكية غير المأذون بها؛
(هـ) خدمات المراسلة غير المتصلة بوظائف المرفق التي يؤديها النظام؛
(و) خدمات وسائل التواصل الاجتماعي وتطبيقاتها؛
(ز) وحدات الخدمة أو برامجيات الخدمات غير المستخدمة؛
(ح) برامج معالجة البرامجيات الحاسوبية في محطات المستخدمين ووحدات الخدمة، باستثناء البرامج المستخدمة لتطوير النظام؛
(ط) برامج معالجة البرامجيات الحاسوبية باللغات غير المستخدمة في نظام التحكم؛
(ي) بروتوكولات الشبكة والاتصالات غير المستخدمة؛
(ك) أدوات المساعدة الإدارية وأدوات التشخيص ووظائف إدارة الشبكة ووظائف إدارة النظام غير المستخدمة؛
(ل) عمليات النسخ الاحتياطي للملفات وقواعد البيانات والبرامج المستخدمة أثناء تطوير النظام؛
(م) البيانات وملفات نسق المكونات غير المستخدمة؛
(ن) عينات البرامج والنصوص البرامجية؛
(س) أدوات المساعدة في معالجة الوثائق غير المستخدمة؛
(ع) الوظائف الإضافية غير الضرورية للتطبيقات (مثل برامج التصفح)؛
(ف) الألعاب.

ألف-65- وينبغي أن يكون تحصين النظام إلزامياً بالنسبة للأصول الرقمية الحساسة التي تستخدم مكونات تجارية 'جاهزة للاستخدام'، والتي ينبغي تقليل وظائفها إلى الحد

المطلـوب لأداء وظائـف المرفـق الـذي توجـد فيـه الأصـول الرقميـة الحساسـة (أو وظائـف النظـام الخـاص بالأصـول الرقميـة الحساسـة).

ألف-66- وينبغـي أن يكـون الهـدف مـن تحصيـن النظـام هـو تقليـل مقـدار البيانـات التـي تحتـاج إلـى رصـد وتحليـل لتحديـد أمـن الأصـل الرقمـي أو النظـام الرقمـي المحمـي. ويمكـن أن يسـاعد تحصيـن النظـام أيضـاً المشـغِّل فـي بلـورة فهـم أفضـل لأنمـاط السـلوك والوظائـف الطبيعيـة للنظـام.

ألف-67- ويمكـن أن يشـمل تحصيـن النظـام اسـتخدام التكنولوجيـا لضمـان عـدم السـماح بـأن تُشـغَّل علـى الأصـول الرقميـة الحساسـة سـوى الإصـدارات المعتمـدة مـن البرامجيـات الحاسـوبية المـأذون بهـا. وينبغـي أن تشـمل سـجلات تحصيـن النظـام توثيـق المكتبـات التـي اسـتخدمتها التكنولوجيـا.

ألف-68- وينبغـي ألّا يُسـتخدم فـي تحصيـن النظـام سـوى آليـات تحديـث آمنـة وموثوقـة. وينبغـي تقييـم آليـات التحديـث للتأكـد مـن أنهـا تُزيـل أو تقلـل احتمـالات اسـتخدام التحديـث كطريـق لمهاجمـة النظـام الـذي يتـم تحديثـه، وذلـك علـى سـبيل المثـال مـن خـلال ضمـان تحديـد تحديثـات النظـام مـن خـلال التوقيعـات المشـفرة للبائعيـن المـأذون لهـم.

الاعتبارات الخاصة بتحديث البرامجيات

ألف-69- يُصـدر البائعـون تحديثـات للأمـن الحاسـوبي تتخـذ فـي العـادة شـكل 'تصحيحـات' لمعالجـة الثغـرات المحـددة فـي نُظمهـا. وبالنظـر إلـى أن التعديـلات التـي يتـم إدخالهـا علـى نُظـم الأمـان تحتـاج إلـى اتبـاع إجـراءات كثيفـة المـوارد، قـد لا يكـون التثبيـت الفـوري للتصحيـح ممكنـاً، ممـا يجعـل النظـام معرضـاً للخطـر لبعـض الوقـت.

ألف-70- وينبغـي أن يحصـل المشـغّل مـن البائـع علـى قائمـة بمكونـات البرامـج المسـتخدمة فـي النُظـم وتحديثـات البرامجيـات المنطبقـة (بمـا فـي ذلـك التصحيحـات الخاصـة بالأمـن).

ألف-71- وينبغـي أن يسـتخدم المشـغِّل عمليـة رسـمية لضمـان تقييـم تحديثـات الأمـن الحاسـوبي للمعـدات والمكونـات مـن أجـل تحديـد مـدى قابليتهـا للتطبيـق وتأثيرهـا، وعلـى وجـه التحديـد، مـا إذا كان تثبيـت التحديثـات ضروريـاً للحـد مـن الثغـرات المرتبطـة بهـا.

وينبغي أن يقوم المشغِّل بتثبيت التحديث أو أن يوفِّر تدابير تعويضية فعالة مناسبة للحماية من استغلال هذه الثغرات.

ألف-72- وينبغي أن يحدد المشغِّل تدابير الأمن الحاسوبي التي توفِّر مستوى قوي من الأمان وتنفيذها للسماح بتقييم التحديثات والثغرات المرتبطة بها من دون استغلال الثغرات أثناء فترة التقييم والتثبيت. وعلى سبيل المثال، يمكن أن يؤدي تحصين النظام إلى تقليل عدد التحديثات الأمنية التي يتعيّن تقييمها وتثبيتها، حيث لا يلزم تثبيت التحديثات التي يقتصر تأثيرها على الوظائف التي أُلغيت أو عُطلت.

إجراءات الأمن

رصد النُظم

ألف-73- ينبغي تعيين مشرف (على سبيل المثال، مهندس نُظم) لجميع النُظم التي يغطيها برنامج الأمن الحاسوبي، بحيث يتولى المسؤولية عن رصد النظام.

ألف-74- وينبغي أن يشمل رصد النظام رصد حالة فعالية تدابير الأمن الحاسوبي وفعاليتها.

ألف-75- وينبغي أن يكون المشرف على النظام مسؤولاً عن التأكد من تحديث وسائط الاسترداد ومعلومات نسق المكونات، وأنه يتم الاحتفاظ بخطط لاسترداد النظام وأن هذه الخطط يمكن تنفيذها عند الضرورة (على سبيل المثال من خلال التمرن بانتظام على خطة الاسترداد).

مراقبة التغييرات في نسق المكونات

ألف-76- ينبغي مراقبة التغييرات التي تطرأ على نسق تكوين الأصول الرقمية الحساسة، مع إيلاء المراعاة الصريحة لتحليلات العواقب الأمنية. وينبغي أن يوفِّر المدير أو المشرف على الأصول على أي تغييرات في أنساق مكونات الأصول الرقمية الحساسة قبل تنفيذ هذه التغييرات. وينبغي أن تكون هذه الموافقة موثقة رسمياً.

ألف-77- وينبغي استعراض الأنشطة المرتبطة بالتغييرات في نسق مكونات الأصول الرقمية الحساسة على يد أخصائي الأمن الحاسوبي. وينبغي إعداد سجلات بالتغييرات التي تطرأ على نسق مكونات الأصول الرقمية الحساسة والاحتفاظ بها واستعراضها.

ألف-78- وينبغي أن يكون أخصائي الأمن الحاسوبي مسؤولاً بشكل عام على الإشراف على أنشطة مراقبة التغييرات في أنساق المكونات التي تنطوي على أصول رقمية حساسة، ولكن يجوز له تفويض هذه المسؤولية إلى المشرفين على الأصول. وينبغي أن يضع أخصائي الأمن الحاسوبي متطلبات لضمان إجراء عمليات الإشراف وتنسيقها بفعالية.

تمارين الأمن الحاسوبي (بما في ذلك التدريبات)

ألف-79- ينبغي أن يشمل الرصد المستمر لفعالية برنامج الأمن الحاسوبي في الممارسة العملية تقييم مكونات برنامج الأمن الحاسوبي من خلال التمارين.

ألف-80- ويمكن أن تجمع التمارين الخاصة بأمن المعلومات والأمن الحاسوبي بين التقييم والتدريب. وينبغي أن تتضمن التمارين أيضاً سيناريوهات تشمل هجمات مختلطة، بما في ذلك هجوماً منسقاً على الفضاء الإلكتروني وهجوماً مادياً.

ألف-81- ويمكن التمرن على نظام إدارة أمن المعلومات والأمن الحاسوبي بطريقة متدرجة بالنسبة للموظفين المكلفين بأدوار مختلفة وعلى مستويات مختلفة داخل المنظمة. وتختبر التمارين مدى فعالية أساليب تسيير العمل ووظيفة الاتصالات في التصدي لحادثات الأمن الحاسوبي؛ وتوفِّر أيضاً التدريب لجميع مستويات الموظفين المشاركين في الإدارة والتصدي.

ألف-82- وينبغي أن يأخذ المشغِّل في الاعتبار الاستفادة مما يلي:

(أ) التمارين المتعلقة بإجراءات الأمن لاختبار فعالية الإجراءات في تلبية أهداف برنامج الأمن الحاسوبي؛
(ب) التدريبات لتدريب الموظفين على تنفيذ الإجراءات وبالتالي زيادة الوعي بالإجراءات، والأساس المنطقي الذي تستند إليه المهام التي يشملها الإجراء، والتصدي لحادثات الأمن الحاسوبي.

الاختبار الاقتحامي

ألف-83- ينبغي أن يأخذ المشغِّل في الاعتبار ما إذا كان سيُجري اختباراً اقتحامياً (محاكاة هجوم حقيقي على الفضاء الإلكتروني في نُظم حقيقية) كجزء من تقييم الأمن الحاسوبي لنظام أو أصل رقمي، مع مراعاة الاعتبارات القانونية واعتبارات الأمان والأمن، وقدرة المشغِّل على تجنب أو معالجة أي تأثيرات ضارة تحدث للأصل الرقمي والنظام. ويُحدد المرجع [8] القيود المحددة المفروضة على الاختبار الاقتحامي لنُظم الأجهزة والتحكم.

ألف-84- وبالنظر إلى أن الأسلوب المفصل للهجوم على الفضاء الإلكتروني سيعتمد بشدة على النسق الدقيق لمكونات النُظم التي تتعرض للهجوم، ينبغي أن يكون النظام الذي يخضع للاختبار مشابهاً للنظام الحقيقي قدر المستطاع. وينبغي وجود إجراءات كاملة للنسخ الاحتياطي والاستعادة لإعادة النظام إلى حالة مستقرة معروفة إذا أدى الاختبار التقييمي إلى ظروف غير طبيعية.

ألف-85- وينبغي أن تُحدد خطة الاختبار الجدول الزمني للاختبار وميزانيته، وتحديد أهداف الاختبار، ومخرجاته المتوقعة، والأجهزة والبرامج التي سيجري استخدامها، والموارد اللازمة، وقواعد الاشتباك، وإجراءات الاسترداد.

ألف-86- ويمكن أن تشمل تقنيات الاختبار ما يلي:

(أ) 'جمع البصمات'، ويشمل ذلك تحديد جميع الاتصالات داخل المكونات وبينها في النظام وقياسها، وتحليل آثار هذه الاتصالات على الأصول الرقمية الحساسة التي يتعلق بها الاختبار. ويوفِّر جمع بصمات الشبكة ما يلي:
'1' خط أساس للشبكة؛
'2' مخطط بياني دقيق للشبكة؛
'3' تحديد أي أجهزة مارقة أو اتصالات بيانات ضارة؛
'4' التحقق من أن أجهزة حماية الحدود تعمل بحسب التصميم؛
'5' تحديد فرص تحسين تقسيم المناطق وحماية المحيط.

(ب) 'التشويش' الذي يهدف إلى اكتشاف الأخطاء أو الثغرات في مكون أو نظام عن طريق ضخ مجموعة متنوعة من البيانات بطريقة آلية لتحديد أنواع البيانات

ونقاط الضخ التي يمكن استخدامها لأغراض ضارة. ويمكن من خلال ذلك تحديد نقاط الضعف في الترميز البرمجي وتوفير مؤشر على مدى صلابة النظام.

ألف-87- ويمكن أن توفِّر مؤشرات الأمن الحاسوبي أساساً مشتركاً لتقييم الثغرات. وتوفِّر المؤشرات المختارة جيداً والمتفق عليها عموماً (مثل نظام التقدير المشترك للثغرات) أساساً مشتركاً لمقارنة الثغرات بين النُظم المختلفة. وينبغي أن يقيّم المشغِّل الطرق الممكنة التي يمكن من خلالها استغلال الثغرات واتخاذ ترتيبات لمنع ذلك الاستغلال. وينبغي أن ينظر المشغِّل في الإبلاغ عن جميع الثغرات لإدراجها في قاعدة بيانات وطنية بشأن الثغرات.

التصدي لحادثات الأمن الحاسوبي

ألف-88- ينبغي أن يكون موظفو الأمن الحاسوبي مسؤولين عن الإبلاغ عن أي حادثات أمن حاسوبي مشتبه بها وفقاً لخطة التصدي للحادثات. وينبغي أن ينظر المشغِّل في تقديم توعية متخصصة للموظفين الذين يؤدون أدوار رئيسية غير مرتبطة بصورة مباشرة بالأمن الحاسوبي ولكن يمكن أن تتأثر بحالات فشل الأمن الحاسوبي.

ألف-89- وينبغي أن يكون لدى المشغِّل خطة طوارئ لكشف حادثات الأمن الحاسوبي التي يمكن أن تؤثر على الأصول الرقمية الحساسة (وأي أحداث أخرى متصلة بالأمن النووي يمكن أن تنطوي على حادثات أمن حاسوبي) والتصدي لها. وينبغي أن تشمل الخطة إجراءات لتحديد مكان التهديد وطبيعته، ومنع عواقب أي فعل ضار أو التخفيف من هذه العواقب، وإخطار السلطات المختصة ذات الصلة، والتعافي من الحدث.

ألف-90- ويتألف التصدي للحادثات من مجموعة من الأنشطة (انظر الشكل 10) التي ينبغي النظر في كل منها.

ألف-91- ويمكن أن تشمل حادثات الأمن الحاسوبي الإخلال بالسرية و/أو السلامة و/أو التوافر فيما يتصل بالبيانات المعالجة أو المخزنة أو المنقولة بواسطة نظام قائم على الحاسوب. وقد تشمل حادثة الأمن الحاسوبي أيضاً انتهاك سياسة أمن حاسوبي صريحة أو ضمنية، أو سياسة الاستخدام المقبول، أو ممارسة الأمن الحاسوبي القياسية. ويمكن أن تتسبب بعض الأحداث المعاكسة (مثل الفيضانات والحرائق وانقطاع التيار الكهربائي

الشكل -10 التصدي لحادثات الأمن الحاسوبي (مستنسخ من المرجع [24] بتصريح من المعهد الوطني للمعايير والتكنولوجيا)

والحرارة الزائدة) في تعطل النظام، ولكنها ليست ناتجة عن أفعال ضارة، وبالتالي لا تعتبر حادثات أمن حاسوبي.

ألف-92- وقد تصبح حادثة الأمن الحاسوبي حادثة أمن معلومات أو خرق لها إذا كانت تنطوي على الإخلال الفعلي بمعلومات حساسة أو الاشتباه في الإخلال بها. ويُقدم المرجع [5] أمثلة على المعلومات التي يمكن أن تكون حساسة المرتبطة بالمرافق النووية.

ألف-93- وينبغي أن ينشئ المشغِّل فريقاً محلياً للتصدي لحادثات الأمن الحاسوبي يكون مسؤولاً عن التصدي لحادثات الأمن الحاسوبي التي تقع داخل المنظمة. وسيعتمد حجم فريق التصدي لحادثات الأمن الحاسوبي وتكوينه وقدراته على طبيعة المنظمة والبنية الأساسية الحاسوبية الخاصة بها، ولكن ينبغي أن يشمل أفراداً من ذوي الخبرة في مجال الأمن النووي والأمان النووي والتأهب والتصدي للطوارئ وكذلك الأمن الحاسوبي. ويمكن أن يتكون فريق التصدي لحادثات الأمن الحاسوبي من الأعضاء أنفسهم الذين يتكون منهم فريق الأمن الحاسوبي أو من بعض الأعضاء المشتركين معه.

ألف-94- ويمثل فريق التصدي للطوارئ الحاسوبية سلطة تقنية توفِّر المساعدة وقدرات التصدي عند وقوع حادثة متصلة بالأمن الحاسوبي. ويمكن أن يكون فريق التصدي للطوارئ الحاسوبية موجوداً على مستويات مختلفة (على سبيل المثال، المستوى الوطني أو المحلي أو على مستوى القطاع الصناعي). ويمكن أن يكون فريق التصدي للطوارئ الحاسوبية متاحاً لتكميل القدرات الداخلية للتصدي للأمن الحاسوبي في المنظمة

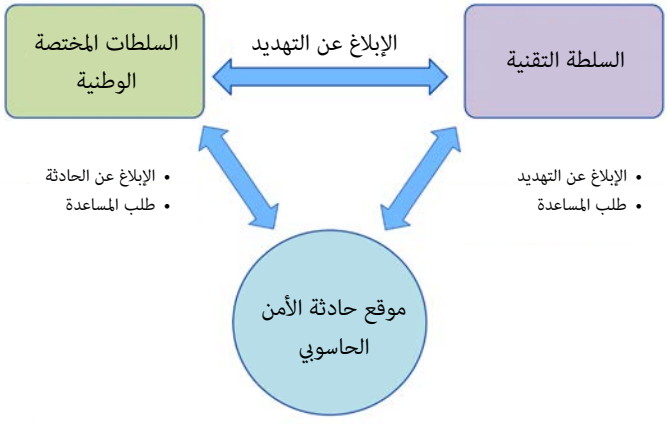
المشغِّلة عند التصدي لأي حادثة أمن حاسوبي. وينبغي مراعاة أن يكون هذا الفريق متاحاً للتصدي في أوقات الأزمات عند التخطيط لأنشطة التصدي في المنظمة المشغِّلة.

ألف-95- وينبغي أن يضمن المشغِّل أن يُشارك في التمارين أي أعضاء من فريق التصدي للطوارئ الحاسوبية الذين سيشاركون في التصدي، بالإضافة إلى أعضاء فريق التصدي لحادثات الأمن الحاسوبي. وينبغي مراعاة التفاعلات بين فريق التصدي للطوارئ الحاسوبية وفريق التصدي لحادثات الأمن الحاسوبي، بما في ذلك الأنشطة التحضيرية (على سبيل المثال الحصول على إذن مسبق بوصول أعضاء فريق التصدي للطوارئ الحاسوبية إلى المناطق المحددة في المرفق). وينبغي تصميم التمارين لاختبار عناصر الاتصال الرئيسية بين السلطات المختصة وفريق التصدي للطوارئ الحاسوبية وفريق التصدي لحادثات الأمن الحاسوبي وعمليات الموقع، كما هو موضح في الشكل 11.

مراحل التصدي لحادثة أمن حاسوبي

الإعداد

ألف-96- تشمل إجراءات التخطيط في مرحلة الإعداد وضع سياسة لتوجيه العمليات التشغيلية من أجل التصدي لحادثات الأمن الحاسوبي، وتحديد أدوار جميع الأطراف المعنية بالتصدي للحادثة ومسؤولياتها، وصياغة الإجراءات المتوافقة مع السياسة، وتحديد الأصول المتاحة للتصدي. وينبغي أن تُحدد بوضوح المتطلبات والمعايير الخاصة



الشكل -11- تفاعلات التصدي لحادثات الأمن الحاسوبي

بالاستخدام في التصدي لحادثات الأمن الحاسوبي. وينبغي موافقة الإدارة العليا على خطة إجراءات التصدي.

الكشف والتحليل

ألف-97- أثناء مرحلة الكشف والتحليل، ينبغي أن يكون فريق التصدي لحادثات الأمن الحاسوبي مسؤولاً عن تحديد الخصائص التقنية للحادثة. وتشمل أنشطة الكشف ضمان الرصد الكافي للبيانات لدعم الكشف من خلال جمع المعلومات المتصلة بالحادثات الممكنة وحفظها. ويمكن لفريق التصدي لحادثات الأمن الحاسوبي استخدام بيئة اختبار وتقييم مخصصة لهذا الغرض من أجل تحليل الحادثات من دون التأثير على النُظم التشغيلية أو الإخلال بأدلة التحليل الجنائي المحتملة.

ألف-98- ويمكن أن تمتد أنشطة التحليل إلى ما يتجاوز فريق التصدي لحادثات الأمن الحاسوبي والتحديد الأوّلي للخصائص التقنية للحادث، ويمكن أن تتطلب بعض جوانب التحليل موارد كبيرة. وتشمل الأولويات النموذجية للتحليل ما يلي:

(أ) تحديد التأثيرات المحتملة لحادثة الأمن الحاسوبي على الأمن النووي والأمان والتأهب للطوارئ والتصدي لها، وتحديد الإجراءات المطلوبة لوضع المرفق في حالة مأمونة؛
(ب) تقييم مدى الحادث لتحديد الاستجابة المناسبة؛
(ج) تحديد الضرر المحتمل من حادثة الأمن الحاسوبي من حيث فقدان المعلومات والأضرار المادية للمرفق والصورة العامة؛
(د) تحديد طبيعة حادثة الأمن الحاسوبي فيما يتعلق بالنوايا المباشرة للخصم والتهديدات المستقبلية المحتملة، بما في ذلك إمكانية وقوع هجوم في المستقبل يستغل التأثيرات الناتجة عن هذه الحادثة؛
(ه) تحديد السبب الجذري لحادثة الأمن الحاسوبي والتدابير المطلوبة لمنع تأثيرات الحوادث المستقبلية ذات الطابع المماثل أو التخفيف منها؛
(و) تحديد الخصم وإعداد توصيف له، بما في ذلك التقنيات والأدوات المستخدمة والثغرات التي استغلها الخصم.

التخفيف (الاحتواء، والاستئصال، والاسترداد)

ألف-90- تهدف إجراءات التخفيف إلى احتواء حادثة أمن حاسوبي؛ واستئصال أي برامجيات خبيثة أو تصحيح أي اختلال في التشغيل أو تغيير في نسق المكونات في النُظم المتأثرة؛ واسترداد وظيفة النظام وسلامة البيانات، باستخدام تدابير تعويضية عند الضرورة. وحتى إذا كانت المكونات أو النُظم التي يحدث إخلال بها لا تؤدي وظيفة أمان أو أمن حاسمة الأهمية، يتعيَّن فحصها وتطهيرها لمنع انتشار الهجوم إلى مكون أو نظام لا يؤدي هذه الوظيفة. وتستمر أنشطة التخفيف وتُعدَّل بحسب ما يُجمع من معلومات، وتُحلل أثناء مرحلة الكشف والتحليل.

ألف-100- عند التخطيط لطريقة احتواء حوادث الأمن الحاسوبي، ينبغي أن يدرك المشغِّل أن عدداً من المكونات أو النُظم يمكن أن يُحدد أثناء التحقيق في الحادثة على أنه قد جرى الإخلال به. وإذا كان إخلال قد حدث لأيٍ من المكونات أو النُظم التي تؤدي وظيفة أمان أو أمن حاسمة الأهمية - مثل المساهمة في حماية الأصول الرقمية الحساسة، أو أمان تشغيل المرفق أو حماية المواد النووية أو المواد المشعة الأخرى - سيكون من الضروري تنفيذ تدابير تعويضية لأداء هذه الوظيفة لحين إعادة تشغيل المكوِّن أو النظام.

ألف-101- ويمكن أن تشمل تدابير الاسترداد استبدال المثل بالمثل (على سبيل المثال، جدار حماية احتياطي)؛ وعزل هياكل الأمان ونُظمه ومكوناته عن المكوِّن أو النظام الذي حدث إخلال به؛ أو تدابير مؤقتة، مثل آلية حراسة للتحكم في الدخول إلى الجزء ذي الصلة من المرفق لاستبدال نظام رقمي للتحكم في الدخول. وينبغي أن تستبدل تدابير الاسترداد الوظيفة، وليس بالضرورة المكوِّن أو النظام الذي حدث إخلال به.

أنشطة ما بعد الحادثة

ألف-102- تتمثل المرحلة الأخيرة من التصدي في أنشطة ما بعد الحادثة لتنفيذ التدابير التي من شأنها منع تكرار وقوع أنواع مماثلة من حادثات الأمن الحاسوبي في المستقبل، والتمكين من كشفها بسرعة و/أو تقليل عواقبها. ويمكن أن تشمل هذه المرحلة تعلم الدروس المستفادة داخل المنظمة وتبادل المعلومات الاستخباراتية بشأن التهديدات والدروس المستفادة، بحسب الاقتضاء، مع الأوساط المعنية بحادثات الأمن الحاسوبي على النطاق الأوسع للمساعدة في منع هجوم مماثل من النجاح في مكان

آخـر. ويمكـن أن تتيـح نتائـج مـا بعـد الحادثـة وضـع تدابيـر أمنيـة جديـدة لمنـع تكـرار العـدوى وتوفيـر معلومـات لتحديـث توصيفـات التهديـد والثغـرة. ويمكـن أن تشـمل الأنشـطة الأخـرى فـي مرحلـة مـا بعـد الحادثـة تقييـم فعاليـة برنامـج الأمـن الحاسـوبي وتحديـد التدريب المطلـوب لمعالجـة أي فجـوات فـي موظفـي التصـدي، وكذلـك تقييـم المـوارد التـي كانـت مطلوبـة لمعالجـة حادثـة الأمـن الحاسـوبي كدليـل للاسترشـاد بـه فـي التخطيـط للحادثـات المسـتقبلية.

الإبلاغ

ألف-103- أثنـاء التصـدي لحادثـة أمـن حاسـوبي، يمكـن أن تكـون هنـاك حـالات يمكـن أن يكـون فيهـا إبـلاغ السـلطات المختصـة (أو المنظمـات الأخـرى) مطلوبـاً أو مسـتصوباً. ويتيـح الإبـلاغ لـكل مـن يتعيّـن أن يكـون علـى درايـة بحادثـة الأمـن الحاسـوبي إبلاغـه فـي الوقـت المناسـب. وبالنظـر إلـى أن مـن المحتمـل أن يكـون القائمـون بالتصـدي مشـغولين، يتعيّـن علـى المشـغِّل أن يفكـر بعنايـة فـي تواتـر الإبـلاغ ومسـتوى التفاصيـل المقدمـة. ويمكـن أن ينظـر المشـغِّل فـي تعييـن فـرد معيّـن كجهـة اتصـال للإبـلاغ عـن حادثـات الأمـن الحاسـوبي ولطلبـات المعلومـات مـن المنظمـات الخارجيـة.

تخطيط الأنشطة

ألف-104- ينبغـي أن يضمـن تخطيـط الأنشـطة تحديـد متطلبـات الأمـن الحاسـوبي لـلأداء والتحقـق مـن الأنشـطة والتخطيـط لهـذه المتطلبـات.

ألف-105- وينبغـي تحديـد مؤهـلات الموظفيـن والمتعهديـن المطلوبـة فيمـا يتعلـق بالأمـن الحاسـوبي للأنشـطة المنفـذة، وينبغـي أن يؤخـذ ذلـك فـي الاعتبـار عنـد التخطيـط. وتقـع علـى عاتـق كل منظمـة مسـؤولة المسـؤولية عـن الإبـلاغ عـن حادثـات الأمـن الحاسـوبي المشـتبه بهـا وفقـاً لخطـة التصـدي للحادثـات.

ألف-106- وعنـد وضـع تعليمـات للعمـل، ينبغـي مراعـاة متطلبـات الأمـن الحاسـوبي. ويمكـن أن تشـمل هـذه التعليمـات مـا يلـي:

(أ) إزالة تدابير الأمن الحاسوبي (للسماح بإجراء الصيانة)؛
(ب) توفير تدابير بديلة أو تعويضية (عندما تكون التدابير العادية غير متاحة)؛

(ج) إعادة تطبيق تدابير الأمن الحاسوبي (بعد الصيانة)؛
(د) تأكيد إعادة وضع تدابير الأمن الحاسوبي بشكل صحيح.

ألف-107- ينبغي أن تشمل تعليمات الصيانة تعليمات لتهيئة نسق إعدادات الأمن في الأجهزة.

ألف-108- وإذا كانت الصيانة تتطلب التصرف في المعدات التي لم تعد مطلوبة، ينبغي تطهير هذه المعدات أو تدميرها بشكل آمن.

ألف-109- ينبغي تحديد متطلبات الشراء المتصلة بالأمن الحاسوبي وتنفيذها في خطة العمل.

الوعي والتدريب

ألف-110- على الرغم من استخدام الحواسيب في كثير من جوانب العمل والحياة الشخصية، هناك نقص عام في الوعي والمعرفة بشأن التكنولوجيا وتهديدات الفضاء الإلكتروني وتدابير الأمن الحاسوبي والتأثيرات المحتملة للإخلال. وهناك حاجة إلى زيادة الوعي والتدريب في مجال الأمن الحاسوبي لجميع الموظفين والمتعهدين في المنظمات التي لديها مسؤوليات متعلقة بالأمن النووي.

ألف-111- ويتسبب الخطأ البشري أو يُساهم بدور معاكس في حوادث الأمن الحاسوبي. ويحتاج الموظفون على جميع المستويات إلى الوعي وإعادة تأكيد الأمن الحاسوبي.

ألف-112- ويمكن أن يؤدي الوعي بأهميتها إلى دعم الأمن الحاسوبي على النحو التالي:

(أ) من خلال تعزيز الفهم بأن الأمن الحاسوبي لا يقتصر على دعم الأمن النووي للمرفق، بل وكذلك أمانه؛
(ب) من خلال ضمان بلورة فهم مشترك للجوانب الرئيسية للأمن الحاسوبي داخل المنظمة؛
(ج) من خلال تشجيع الملاحظة وتدريب الزملاء والإبلاغ عن حادثات الأمن الحاسوبي وأمن المعلومات المحتملة، والوعي بالحالة؛

(د) من خلال تعزيز فهم إمكانية تأثير الهجمات ضد الفضاء الإلكتروني على العديد من تدابير الأمن و/أو الأمان في آن واحد، مما يُقلل من الدفاع في العمق؛
(هـ) من خلال توفير وسيلة يمكن من خلالها حل التضارب بين أهداف الأمان والأمن؛
(و) من خلال التعرف على الممارسات الجيدة في مجال الأمن الحاسوبي وتعزيزها؛
(ز) من خلال زيادة الوعي بالطريقة التي يُساهم بها البشر عن غير قصد في حادثات الأمن الحاسوبي.

ألف-113- ويمكن استخدام المؤشرات التالية لتقييم الوعي بالأمن الحاسوبي في المنظمة:

(أ) متطلبات الأمن الحاسوبي موثقة بشكل واضح ومفهومة جيداً لدى الموظفين.
(ب) وجود بروتوكولات وإجراءات واضحة وفعالة لتشغيل النُظم الحاسوبية سواءً داخل المنظمة أو خارجها.
(ج) يفهم الموظفون ويدركون أهمية تدابير الأمن الحاسوبي المحددة في برنامج الأمن الحاسوبي.
(د) يُحتفظ بالنُظم الحاسوبية في حالة آمنة وتشغَّل وفقاً لخط أساس الأمن الحاسوبي والإجراءات المعتمدة.
(هـ) ينظر الجميع إلى حالات خرق إجراءات الأمن الحاسوبي باعتبارها خطيرة وغير مرغوب فيها.
(و) نتائج الملاحظات والتقييمات والاختبارات والتمارين إيجابية (على سبيل المثال، تُشير الاختبارات إلى أن الموظفين لا يستجيبون لرسائل البريد الإلكتروني الانتحالية).
(ز) يلتزم المديرون التزاماً كاملاً بالمبادرات الأمنية ويدعمونها، سواءً كانت متعلقة بنُظم الفضاء الإلكتروني أو بالنُظم المادية.

ألف-114- والهدف من برنامج التدريب على الأمن الحاسوبي هو ضمان حصول جميع الموظفين والمتعهدين على المعرفة والقدرة التي تمكنهم من أداء عملهم وفقاً لمتطلبات الأمن الحاسوبي وإجراءاته في المرفق. وينبغي أن يكون التدريب على الأمن الحاسوبي جزءاً لا يتجزأ من النظام القائم لإدارة التدريب.

ألف-115- وينبغي أن يكون لدى المشغِّل برنامج تدريبي يشمل العناصر التالية:

(أ) برنامج للتدريب على الأمن الحاسوبي، ويُعتبر إتمامه بنجاح شرطاً مسبقاً للوصول إلى النُظم الحاسوبية. وينبغي أن يتناسب تدريب الأفراد مع مستويات الأمن الحاسوبي للنُظم التي يُسمح لهم بالوصول إليها.

(ب) التدريب والتأهيل المتخصصان للأفراد الذين تقع عليهم مسؤوليات رئيسية في مجال الأمن (مثل أخصائي الأمن الحاسوبي وفريق الأمن الحاسوبي وأفراد الأمن الآخرين ومديري المشاريع ومسؤولي تكنولوجيا المعلومات ومهندسي النُظم والمصممين والتقنيين وموظفي إدارة الوثائق وموظفي المشاريع وموظفي الشراء والمتعهدين والإدارة العليا).

(ج) مواد تدريبية يتم تحديثها بانتظام لتشمل الإجراءات والتدابير الجديدة لمعالجة التهديدات الناشئة.

(د) التدريب الذي يتكرر بانتظام للتأكد من أن الموظفين على دراية بأحدث الإجراءات والتهديدات.

(هـ) اشتراط إقرار الموظفين بفهمهم مسؤوليات الأمن الحاسوبي الخاصة بهم.

(و) تقييمات عملية لفهم الموظفين لمسؤولياتهم في مجال الأمن الحاسوبي.

ألف-116- ينبغي استخدام مجموعة متنوعة من نُهج التدريب، مثل التدريب الإلكتروني، والتدريب داخل قاعات الدراسة، والتمارين العملية ومحافل المناقشة.[3] ويمكن للمنظمات الخارجية، بما فيها الوكالة الدولية للطاقة الذرية، توفير مواد لدعم هذه الأنشطة.

ألف-117- وينبغي أن يشمل برنامج التدريب (أ) مؤشرات لتقييم الوعي بالأمن الحاسوبي وفعالية التدريب، و(ب) عمليات للتحسين المستمر والتدريب الدوري لتنشيط معلومات الموظفين وتحديثها، بحسب ما تقتضيه الحاجة.

مثال لعملية تخطيط الاستجابة لحادثات الأمن الحاسوبي

ألف-118- يمكن الرجوع إلى مثال لعملية تخطيط التصدي لحادثات الأمن الحاسوبي في المرجع [25].

[3] قد تؤدي محافل المناقشة إلى تسرب المعلومات، وهو ما يمكن أن يساعد الخصم؛ ولذلك، لا يُنصح بنشر المعلومات في محافل المناقشة المفتوحة والمتاحة للجمهور.

المراجع

[1] الوكالة الدولية للطاقة الذرية، الهدف والعناصر الأساسية لمنظومة الأمن النووي الخاصة بالدولة، العدد 20 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2013).

[2] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية (INFCIRC/225/Revision 5)، العدد 13 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2011).

[3] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن المواد المشعة والمرافق ذات الصلة، العدد 14 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2011).

[4] مكتب الشرطة الأوروبي (اليوروبول)، والوكالة الدولية للطاقة الذرية، ومنظمة الطيران المدني الدولي (إكاو)، والمنظمة الدولية للشرطة الجنائية (الإنتربول)، ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الجمارك العالمية، توصيات الأمن النووي بشأن المواد النووية والمواد المشعة الأخرى الخارجة عن التحكم الرقابي، العدد 15 من سلسلة الوكالة للأمن النووي، الوكالة، فيينا (2011).

[5] الوكالة الدولية للطاقة الذرية، أمن المعلومات النووية، العدد G-23 من سلسلة منشورات الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2015).

[6] تدابير الوقاية والحماية من تهديدات المطلعين على بواطن الأمور، سلسلة الأمن النووي رقم G (Rev. 1-8) الصادرة عن الوكالة الدولية للطاقة الذرية، الوكالة، فيينا (2020).

[7] الوكالة الدولية للطاقة الذرية، الأمن الحاسوبي لأغراض الأمن النووي، العدد G-42 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2021).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[9] التقييم الوطني لتهديدات الأمن النووي ووصف التهديدات المحتاط لها في التصميم وبيانات نماذج التهديدات، العدد G-10 (الصيغة المنقحة Rev. 1) من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة، فيينا (2021).

[10] الوكالة الدولية للطاقة الذرية، الأمن أثناء عمر المرفق النووي، سلسلة الأمن النووي رقم G-35 الصادرة عن الوكالة الدولية للطاقة الذرية، الوكالة، فيينا (2019).

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018).

[12] الوكالة الدولية للطاقة الذرية، مسرد مصطلحات الأمان الصادر عن الوكالة الدولية للطاقة الذرية، المصطلحات المستخدمة في مجالي الأمان النووي والوقاية من الأشعاعات، طبعة 2018، الوكالة، فيينا (2019).

[13] الوكالة الدولية للطاقة الذرية، أمان محطات القوى النووية: التصميم، سلسلة معايير الأمان الصادرة عن الوكالة الدولية للطاقة الذرية، العدد SSR-2/1 (الصيغة المنقحة Rev. 1)، الوكالة، فيينا (2016).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2018, ISO, Geneva (2018).

[15] الحمايـة الماديـة للمـواد النوويـة والمرافـق النوويـة (تنفيـذ الوثيقـة INFCIRC/225/Revision 5)، العـدد G-27 مـن سلسـلة منشـورات الأمـن النـووي الصـادرة عـن الوكالـة، الوكالـة، فيينـا (2018).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2009, ISO, Geneva (2009).

[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Requirements, ISO/IEC 27001:2013, ISO, Geneva (2013).

[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva(2014).

[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Conducting Computer Security Assessments at Nuclear Facilities, IAEA, Vienna (2016).

[24] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, NIST SP 800-61, Rev. 2, NIST, Gaithersburg (2012).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna (2016).

المرفق الأول

سيناريوهات الهجمات المحتملة ضد النُظم في المرافق النووية

أولاً-1- يُقدم هذا المرفق بعض الأمثلة على الطرق التي يمكن بها للخصوم استغلال الثغرات الأمنية في النُظم التي تؤدي الوظائف الحاسمة الأهمية في المرفق. ومع ذلك، هذه ليست سوى أمثلة، ويحتاج المشغِّلون إلى التفكير بطريقة خلاقة في الأمن الحاسوبي لتخيُّل الطريقة التي يمكن أن يتصرف بها الخصوم والطريقة التي يمكن أن تتصدى بها تدابير الأمن الحاسوبي لأفعالهم.

أولاً-2- وتُستمد الأمثلة من المناقشات التي دارت مع الخبراء من الدول الأعضاء. ولا يُقصد منها تقديم قائمة شاملة بالاحتمالات، أو وصفة لمهاجمة المرافق النووية، ولكنها تُشكل منطلقاً لمشغِّلي المرافق والدول الأعضاء لوضع خطط لمواجهة بيئة تهديد الفضاء الإلكتروني الدينامية والسريعة التغيُّر.

أولاً-3- وقد يتكون الهجوم على الفضاء الإلكتروني المنسق من عدة مراحل:

(أ) تحديد هدف أو أهداف؛
(ب) إجراء الاستطلاع؛
(ج) الوصول إلى النُظم ذات الصلة أو الإخلال بها؛
(د) تنفيذ الهجوم؛
(هـ) إخفاء الأدلة المتعلقة بالهجوم والخصم.

أولاً-4- سيستخدم الخصوم بعض هذه التكتيكات أو جميعها، وينبغي أن تؤخذ في الاعتبار عند إعداد توصيف لتهديد الفضاء الإلكتروني الذي يستهدف تحديداً نُظم الأجهزة والتحكم في المرفق النووي والأصول الرقمية الحساسة الأخرى. وتشمل أمثلة السيناريوهات الواردة في هذا المرفق استخدام هذه التكتيكات وتوضيح الأنواع الشائعة من الهجمات التي اقترحها خبراء الأمن الحاسوبي من ذوي الخبرة في المجال النووي.

أولاً-5- ويصف المرجع [أولاً-1] أنواع التهديدات.

السيناريو الأول: الإخلال بنظام دعم يؤدي إلى الوصول إلى نُظم التشغيل المهمة

أولاً-6- الهدف من الهجوم: الوصول إلى المعلومات النووية والأصول الرقمية عن طريق استغلال مسارٍ موثوق يستخدمه البائعون لتقديم الدعم.

أولاً-7- الوصف: يوجه الهجوم في البداية إلى بوابة الوصول عن بُعد التي يصل من خلالها البائعون إلى المعلومات الحساسة والأصول الرقمية الحساسة في المرفق لتقديم الدعم. ويخترق الخصم البوابة الإلكترونية، ومن خلال تصعيد امتياز الدخول، يحصل الخصم على تحكم إداري في قاعدة البيانات ويُغيِّر عنوان البريد الإلكتروني المرتبط بمورد محدد. ويمكن لهذا البائع الوصول عن بُعد إلى المعلومات التشغيلية المهمة المتعلقة بالمرفق وبعض الأصول الرقمية الحساسة. ويستخدم الخصم وظيفة 'نسيت كلمة المرور' عند البوابة، ويؤدي ذلك إلى إرسال رابط تحديث كلمة المرور إلى عنوان البريد الإلكتروني الذي قدمه الخصم. ويُستخدم الخصم هذا الارتباط لتغيير كلمة مرور البائع ويُسجِّل الدخول إلى البوابة الإلكترونية بهوية البائع المعتمد. وبمجرد تسجيل الدخول، يمكن للخصم الوصول إلى جميع المعلومات الموجودة في البوابة وجميع الأصول الرقمية الحساسة التي يمكن للبائع الوصول إليها. ويبدأ الخصم بعد ذلك في تعديل الإعدادات والبارامترات التشغيلية للأصول الرقمية الحساسة، مما يؤدي إلى عدم استقرار تشغيلي، ويؤدي ذلك في نهاية المطاف إلى إغلاق المرفق.

السيناريو الثاني: استغلال الثقة المتعدية بين وحدات الخدمة الخاصة بالإبلاغ المتصلة بالشبكة الحدودية والأصول الرقمية الحساسة الداخلية

أولاً-8- الهدف من الهجوم: الوصول إلى الأصول الرقمية الحساسة والنُظم الداخلية.

أولاً-9- الوصف:

(1) يستخدم الخصم أدوات مفتوحة المصدر ومحركات بحث لتحديد موقع وحدة خدمة الشبكة الحدودية[1] المستخدم للإبلاغ عن معلومات الإنتاج المتصلة بالنظائر

[1] تُستخدم هذه الشبكات لتكوين 'حاجز وقاية' بين النُظم الداخلية الموثوقة والنُظم التي يمكن للجمهور الوصول إليها غير الموثوقة، مثل الإنترنت. ويُشار إليها أحياناً باسم 'المناطق المنزوعة السلاح'.

النووية من النُظم الداخلية الموثوقة إلى الإنترنت. وتوجد وحدة الخدمة المذكورة على الشبكة الحدودية ولكنه يحتوي على وحدة خدمة قاعدة البيانات الرئيسية على الشبكة نفسها، مثل نظام التحكم الخاص بالمرفق الذي يُنتج النظائر النووية. وتجمع وحدة خدمة قاعدة البيانات الرئيسية المعلومات من بيئة الإنتاج التصنيعية الداخلية ويُرسل هذه المعلومات إلى قاعدة البيانات الموجودة على الشبكة الحدودية. وتفصل الشبكة الحدودية عن شبكة الإنتاج بواسطة جدار حماية مرتبط بقائمة تحكم في الدخول للتأكد من أن قاعدة البيانات الموجودة في وحدة خدمة الشبكة الحدودية هي التي يمكنها فقط الاتصال بقاعدة البيانات الرئيسية.

(2) يستغل الخصم ثغرة للحصول على وصول إداري إلى وحدة الخدمة الموجودة على الشبكة الحدودية ويتحكم في قناة الاتصال بين وحدة الخدمة هذه ووحدة الخدمة الخاصة بقاعدة البيانات الرئيسية الموجود على شبكة نظام التحكم. ويكون نسق مكونات جدار الحماية مهيأً للسماح بإجراء اتصالات بين الشبكة الحدودية وقاعدة البيانات الرئيسية (أي أنه ينشئ 'ثقة متعدية' بين الشبكات)، بحيث يمكن للخصم الذي يتحكم في وحدة الخدمة الموجودة على الشبكة الحدودية أن يتصل مباشرة بقاعدة البيانات الرئيسية الموجودة على شبكة نظام التحكم.

(3) يستخدم الخصم الوصلة المرتبطة بقاعدة البيانات الرئيسية لإجراء استطلاع وتعداد لأصول نظام التحكم الموجودة على الشبكة نفسها. وبالنظر إلى عدم وجود تدابير للأمن على شبكة نظام التحكم، يتمكن الخصم من التحكم في الأصول الرقمية الحساسة والإخلال بالتكنولوجيا التي تُتحكم في تطوير النظائر وإدارتها ونقلها وخزنها وجردها.

السيناريو الثالث: إصابة نُظم الأجهزة والتحكم في محطة قوى نووية ببرامجية خبيثة

أولاً-10- الهدف من الهجوم: فرض إغلاق محطة قوى نووية.

أولاً-11- الوصف:

(1) مهندس في محطة للقوى النووي يعمل من المنزل على جهاز حاسوب محمول يُستخدم لدعم الأعمال الهندسية في المحطة وتحسينها، وتحديث برامج الأداء، و'ضبط' البرامجيات لرصد الأمان.

(2) أثناء وجوده في المنزل، يستخدم المهندس حاسوبه للوصول إلى الموقع الشبكي الخاص بالبائع والحصول على تحديث لنُظم الأجهزة والتحكم الخاصة بالمحطة التي لها دور محوري في دعم عمليات المحطة. وأثناء تنزيل التحديث، يستخدم المهندس مصرفاً إلكترونياً ويزور الموقع الشبكي للشركة ويستخدم وسائل التواصل الاجتماعي، وأثناء ذلك يحدث تنزيل لبرامجية خبيثة إلى الحاسوب. وهذه البرامجية الخبيثة جديدة ولم تكتشفها برامجية مكافحة الفيروسات الموجودة على الحاسوب.

(3) بالنظر إلى أن سياسة الشركة تحظر إدخال الحاسوب إلى المحطة، يقوم المهندس بنسخ تحديث نظام التحكم الذي قام بتنزيله إلى جهاز متصل بواسطة ناقل تسلسلي عام (USB)، بهدف استخدامها لتطبيق التحديثات البرامجية على أصول الأجهزة والتحكم. ومع ذلك، قامت البرامجية الخبيثة بنسخ نفسها على جهاز التخزين المتحرك، وعندما يستخدمه المهندس لتثبيت التحديث من خلال مركز عمل هندسي في المحطة، تنسخ البرامجية الخبيثة نفسها على نظام المحطة. وافترض مشغِّل المحطة أن تدابير الحماية المادية المعمول بها ستمنع الحاسوب غير المأذون له من الاتصال بشبكة نظام التحكم في المحطة، ولم ينظر في إمكانية الإصابة من خلال وسائط التخزين القابلة للنقل.

(4) بعد أن تصيب البرامجية الخبيثة مركز العمل الهندسي فإنها تتكاثر وتنتقل إلى المكونات الأخرى المرتبطة بالشبكة داخل المحطة. وبالنظر إلى أن المشغِّل لم ينشر تدابير أمن حاسوبي على مستوى المحطة ولا توجد برامجية لمكافحة الفيروسات على النُظم الحاسمة الأهمية في المحطة، فإن البرامجية الخبيثة تُصيب الأصول الرقمية الحاسمة الأهمية على الشبكة، مما يتسبب في حدوث أعطال وإجبار المحطة على الإغلاق.

السيناريو الرابع: الحصول على معلومات حساسة عن عمليات المحطة النووية مباشرة من المعدات التي أُخرجت من الخدمة بطريقة غير مناسبة

أولاً-12- الهدف من الهجوم: الحصول على معلومات كافية لتخطيط هجوم دقيق على عمليات المحطة.

أولاً-13- الوصف:

(1) يجمع خصم ما معلومات من وسائل التواصل الاجتماعي ومن الملاحظات التي تُشير إلى أن مرفقاً نووياً سيشتري نظاماً للتحكم في شكل ترقية للنظام. وبالإضافة إلى ذلك، يعتزم مشغِّل المرفق بيع المعدات التشغيلية القديمة للمساعدة في دفع تكاليف نظام التحكم الجديد.

(2) نظراً لعدم وجود إجراءات رسمية مرتبطة بأمن المعلومات في حالة الإخراج من الخدمة، يُباع النظام الذي جرى استخدامه في تشغيل عمليات الأجهزة والتحكم من دون استعراض المعلومات المخزّنة فيه أو إزالتها. ويشتري الخصوم النظام ويكتشفون ملفات مشاريع محدثة ومخططات الشبكة ومعلومات اسم المستخدم وكلمة المرور وغيرها من البيانات التي توفِّر فهماً شاملاً لعمليات المرفق النووي.

(3) يستخدم الخصم هذه المعلومات لوضع خطة لمهاجمة الأصول الرقمية الحساسة المحددة في المرفق ولإنشاء رسائل بريد إلكتروني مقنعة لاستخدامها في حملة انتحال إلكتروني. وفي نهاية المطاف، يستخدم الخصم المعلومات التي حصل عليها من النظام الذي اشتراه والمعلومات التي حصل عليها عن غير قصد من ضحايا حملة الانتحال الإلكتروني لشن هجوم مختلط على المرفق.

السيناريو الخامس: الهندسة الاجتماعية الاستراتيجية ضد موظف أمن المرفق

أولاً-14- الهدف من الهجوم: الحصول من موظف أمن المرفق، من خلال الهندسة الاجتماعية، على معلومات يمكن استخدامها للمضي قدماً في هجوم.

أولاً-15- الوصف:

(1) يُجري الخصم حملة هندسة اجتماعية مركزة ضد ضابط أمن في مرفق باستخدام الانتحال الإلكتروني والاستطلاع المادي والمعلومات المتاحة للجمهور، بما في ذلك المعلومات المستمدة من تواجد الموظف على وسائل التواصل الاجتماعي.

(2) ويستخدم الخصم الذي يحمل هوية مزوَّرة، هذه المعلومات لبدء الاتصال مباشرة مع موظف الأمن الذي يثق بالخصم تدريجياً، معتقداً أنه شخص آخر. وفي ظل استمرار المراسلات بينهما، يبدأ الخصم في إضافة مرفقات بريد إلكتروني موثوقة، وهي في الواقع برامجية خبيثة تؤدي عند تنشيطها إلى فتح مسار اتصال سراً

يعـود إلـى حاسـوب الخصـم ويرسـل ملفـات محـددة مـن حاسـوب موظـف الأمـن إلـى الخصـم. وباسـتخدام هـذه المعلومـات، يكـون الخصـم قـادراً علـى إنشـاء خطـط دقيقـة ومفصلـة لمهاجمـة نُظـم الحمايـة الماديـة للمحطـة واعتـراض المـواد النوويـة أثنـاء نقلهـا.

مرجع المرفق الأول

[أولاً-1] الوكالـة الدوليـة للطاقـة الذريـة، الأمـن الحاسـوبي لأغـراض الأمـن النـووي، العـدد G-42 مـن سلسـلة الأمـن النـووي الصـادرة عـن الوكالـة، الوكالـة، فيينـا (2021).

المرفق الثاني

مثال لتقييم مستوى الأمن الحاسوبي لمحطة قوى نووية

ثانياً-1- يعتمد تخصيص مستويات الأمن الحاسوبي للنُظم (أو النطاقات المحتوية على نُظم) على العواقب المحتملة للهجوم على كل نظام لأغراض الأمان والأمن والتشغيل في المرفق: كلما كانت العواقب أقل احتمالاً، زادت صرامة مستوى الأمن الحاسوبي.

ثانياً-2- ولتجنب تحليل كل نظام وكل عاقبة محتملة تبعاً لكل حالة على حدة، يمكن وضع معايير لتسهيل تخصيص مستويات الأمن الحاسوبي.

ثانياً-3- وأحد الاعتبارات الأساسية هو تصنيف أمان النظام. ومع ذلك، لا يوجد ارتباط تلقائي بين مستويات الأمن الحاسوبي وفئات الأمان. ويلزم استخدام مستوى أمن حاسوبي صارم للنظام المهم للأمان، ولكن قد تكون هناك حاجة أيضاً إلى مستوى صارم للنُظم التي ليس لها تصنيف من حيث الأمان إذا كان لها دور حاسم الأهمية في منع العواقب المحتملة الخطيرة بالنسبة للأمن.

ثانياً-4- ويستخدم مثال النهج المتدرج حيال مستويات الأمن الحاسوبي المعايير العالية المستوى التالية:

(1) يُخصص المستوى 1 من مستويات الأمن الحاسوبي للنُظم الرقمية الخاصة بالمرفق التي يمكن أن يؤدي الإخلال بسلامتها أو توافرها إلى عواقب إشعاعية على السكان خارج الموقع. ويتوافق هذا مع معيار نُظم تصنيف الأمان 1E/F1A (المقابل للنُظم الداعمة لوظائف الفئة ألف في مخطط الأمان للجنة الدولية للتقنيات الكهربائية [ثانياً-1]).

(2) يخصص المستوى 2 من مستويات الأمن الحاسوبي للنُظم الرقمية للمحطة التي يمكن أن يؤدي الإخلال بسلامتها أو توافرها إلى تدهور واحد أو أكثر مما يلي:
   (1) إدارة حالة الطوارئ؛
   (2) أمان المحطة في التشغيل العادي؛
   (3) تشغيل العمليات النووية الرئيسية؛
   (4) الحماية المادية للمحطة.

(3) يخصص المستوى 3 من مستويات الأمن الحاسوبي للنُظم الرقمية للمحطة التي لا ينطوي الإخلال بسلامتها أو توافرها على أي عواقب إشعاعية أو على أي تأثير معاكس على الأمان أو الحماية المادية، ولكن يمكن أن يكون له تأثيرات كبيرة أخرى. وقد تشمل هذه النُظم، بصفة خاصة، الأصول الرقمية التي تساعد في تشغيل المحطة أو صيانتها، أو النُظم التي يمكن أن يكون لها تأثير على توليد القوى.

(4) يخصص المستوى 4 من مستويات الأمن الحاسوبي للنُظم الرقمية للمحطة التي لا ينطوي الإخلال بسلامتها أو توافرها على أي تأثير قصير الأجل على أداء المحطة، ولكن يمكن أن يكون له مثل هذا التأثير على المدى الطويل.

(5) يخصص المستوى 5 من مستويات الأمن الحاسوبي للنُظم الرقمية للمحطة التي لا ينطوي الإخلال بسلامتها أو توافرها على أي تأثير على الأمان أو على توافر المحطة أو على أداء المرفق.

ثانياً-5- وبالإضافة إلى هذه المعايير العالية المستوى، يمكن أن يشمل تعريف مستويات الأمن الحاسوبي قائمة بوظائف المرفق النموذجية أو أنواع النُظم الخاصة بكل مستوى. ويمكن لهذه القائمة تبسيط تخصيص مستويات الأمن الحاسوبي للنُظم.

ثانياً-6- يُركز تصنيف مستوى الأمن الحاسوبي على العواقب المحتملة المتصلة بالإخلال بالنُظم القائمة على الحاسوب (انظر المرجع [ثانياً-2]). وفي كثير من الحالات، يمكن أيضاً الحصول على المعلومات المكتسبة أو المحسوبة من خلال نظام رقمي باستخدام أدوات تناظرية أو بواسطة شخص، وفي هذه الحالة يمكن أن يكون مستوى الأمن الحاسوبي أقل صرامة (وبالتالي أقل تقييداً للعمليات العادية).

ثانياً-7- وعند استخدام عدة أصول رقمية متنوعة للوظيفة نفسها، ينبغي اختيار النظام الأساسي الذي يدعم الوظيفة وتخصيصه لمستوى أمن حاسوبي وفقاً للعواقب المترتبة على الإخلال به.

مراجع المرفق الثاني

[II–1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, IEC 61513:2011, IEC, Geneva (2011).

[II–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).

المرفق الثالث

مثال على تطبيق مستويات الأمن الحاسوبي ونطاقاته

الخلفية

ثالثاً-1- يُقدم هذا المرفق مثالاً لتطبيق مستويات الأمن الحاسوبي ونطاقاته. ويوفِّر الجدول ثالثاً1- قائمة بالنُظم المستخدمة في هذا المثال ويوضح تخصيص مستويات الأمن الحاسوبي للمناطق المادية والمنطقية المستخدمة في هذا المثال.

ثالثاً-2- وبالنسبة للنُظم البسيطة التي تتألف من عدد صغير من الأصول في أماكن مادية محددة جيداً، من السهل تطبيق مستويات الأمن الحاسوبي والنطاقات المادية والمنطقية. ولكنه يصبح أكثر تعقيداً بالنسبة للنُظم المعقدة التي تمتد في جميع أنحاء المرفق أو للمناطق المادية المحتوية على نُظم تحتاج إلى مستويات أمن متعددة، مثل غرفة التحكم الرئيسية.

غرفة التحكم الرئيسية

ثالثاً-3- تحتوي غرفة التحكم الرئيسية في العادة على عناصر تحكم في كثير من فئات النُظم المختلفة التي لها متطلبات أمنية مختلفة (على سبيل المثال، نُظم الأمان، ونظام توليد البخار (المرجل)، والنُظم الكهربائية، والنُظم المساعدة، ونُظم تكنولوجيا المعلومات). وتوجد واجهات الربط بين الإنسان والآلة لجميع نُظم المرفق كلياً أو جزئياً في غرفة التحكم الرئيسية. وتستخدم هذه النُظم وواجهات الربط بين الإنسان والآلة في العادة الأصول الرقمية لأداء وظائفها.

ثالثاً-4- وفي المرافق القديمة، يؤدي ذلك إلى صعوبات في تطبيق الأمن الحاسوبي لعدة أسباب:

(أ) تشمل وحدات التحكم القديمة في واجهات الربط بين الإنسان والآلة في العادة عناصر تحكم لنُظم متعددة، وخاصة للموازنة بين نُظم المحطة والنُظم المساعدة. ويمكن أن يزيد هذا التجميع من صعوبة عزل هذه النُظم والفصل بينها. وفي بعض الحالات، يمكن إدماج وظائف المرفق التي تؤديها النُظم المخصصة لمستويات أمن حاسوبي مختلفة في وحدة تحكم واحدة لواجهة الربط بين الإنسان والآلة، والتي ينبغي أن يُطبق عليها مستوى الأمن الأكثر صرامة.

(ب) تُسند مستويات أمن حاسوبي مختلفة للأصول الرقمية الموجودة داخل المنطقة المادية لغرفة التحكم الرئيسية وغرف معداتها، باستخدام نهج مستويات الأمن الحاسوبي ونطاقاته. وعلى سبيل المثال، قد يُخصص لنظام حماية المفاعل المستوى الأكثر صرامة (مثل المستوى 1 من مستويات الأمن)، بينما قد يُخصص مستوى أقل صرامة للحاسوب الشخصي الذي يوفِّر للمشغِّل إمكانية الوصول إلى البريد الإلكتروني (على سبيل المثال، المستوى 5 من مستويات الأمن).

(ج) يمكن للموظفين الذين يؤدون الأنشطة المأذون بها على نظام داخل غرفة التحكم الرئيسية الوصول إلى معدات أخرى داخل الغرفة.

ثالثاً-5- وفيما يلي مثال توضيحي لشرح حلول الأمن الحاسوبي المحتملة للمسائل المبيّنة أعلاه، وذلك من حيث المفاهيم الموضحة بالتفصيل في الشكل 1 من النص الرئيسي.

ثالثاً-6- من الصعب تطبيق نطاقات الأمن الحاسوبي على غرفة التحكم الرئيسية (جنباً إلى جنب مع نُظم الحماية المادية ونُظم الحماية من الحرائق) بسبب الحاجة إلى رصد لوظائف المرفق وإدارتها مركزياً. ويسمح مفهوم نطاقات الأمن الحاسوبي بالحدود المادية و/أو المنطقية التي يمكن أن تساعد في معالجة هذه القيود. ويوضح الشكل واحد الوارد في المرفق الثالث هذه العلاقة.

ثالثاً-7- يُفترض أن غرفة التحكم الرئيسية (والغرف الموجودة داخل المنطقة المحمية التي تحتوي على معدات إلكترونية) سرية ومحمية باعتبارها منطقة حيوية. ويعني ذلك أن تخريب المعدات داخل غرفة التحكم الرئيسية يمكن أن يؤدي في نهاية المطاف إلى عواقب إشعاعية غير مقبولة.

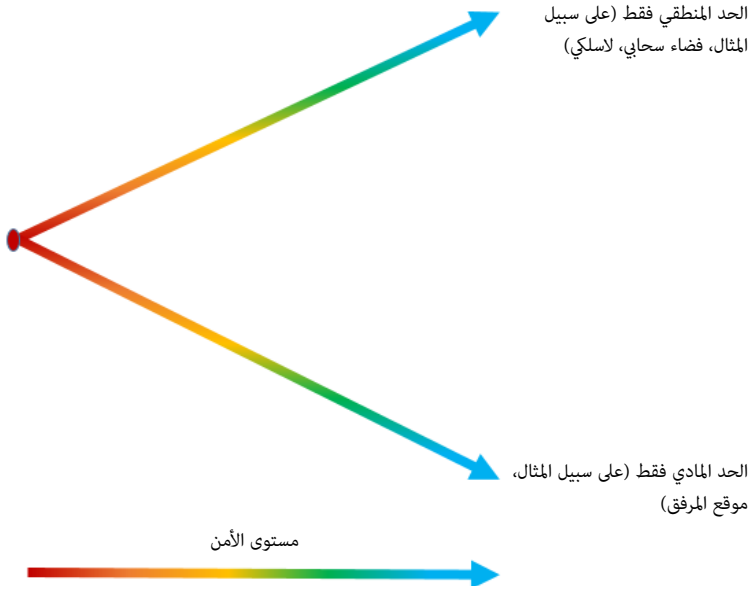
ثالثاً-8- يُقدم الجدول ثالثاً-1 مثالاً على مجموعة فرعية من النُظم التي تحتاج إلى رصد واتصالات أو تشغيل من داخل غرفة التحكم الرئيسية.

النطاقات الواقعة خارج غرفة التحكم الرئيسية المرصودة من داخل غرفة التحكم الرئيسية

نظام حماية المفاعل (المستوى 1 من مستويات الأمن الحاسوبي)

ثالثاً-9- في الجدول ثالثاً-1، يشترط مستوى الأمن الحاسوبي الأكثر صرامة (المستوى 1) تعيين حدود نطاق الأمن الحاسوبي المنطقي والمادي بشكل صارم، وعدم تجاوز هذه الحدود كل منها الآخر. وعلى سبيل المثال، يمكن تقييد الشبكة المخصصة للمواقع داخل المنطقة الحيوية (أو ما يعادلها).

ثالثاً-10- ويحتاج الوصول المادي والمنطقي إلى النطاقات المخصص لها المستوى 1 من مستويات الأمن الحاسوبي إلى تحكم صارم. ويمكن التحكم في الوصول المادي



الشكل ثالثاً -1- متطلبات نطاقات الحدود المادية والمنطقية استناداً إلى مستوى الأمن الحاسوبي

الجدول ثالثاً-1- قائمة النُظم: مثال على تطبيق مستويات الأمن الحاسوبي ونطاقاته

النظام	الوظيفة الأكثر أهمية	مستوى الأمن الحاسوبي	الحد المنطقي	الحد المادي
نظام الأجهزة والتحكم لحماية المفاعل	منع ظروف الحوادث	1	شبكة داخلية مخصصة مفصولة باستخدام صمام بيانات لا يوجد اتصال بشبكة خارجية	المعدات موجودة في منطقة حيوية فقط تدابير الأمن الحاسوبي (صمام البيانات) يقع في منطقة حيوية
نظام الأجهزة والتحكم لتقييد المفاعل	التحكم في التفاعلية	2	شبكات مخصصة، مفصولة باستخدام صمام بيانات أو جدار حماية أو أجهزة أمن أخرى	المعدات تقع في واحدة أو أكثر من المناطق الحيوية تقوية كبلات الشبكة أو المعدات أو التوجيه خارج المناطق الحيوية مادياً (على سبيل المثال، القنوات واللوحات المؤمَّنة)
نظام معلومات العمليات الخاص بالأجهزة والتحكم	توفير الإنذارات والإخطارات للمشغِّل بشأن بيئة المرفق وحالته	3	الشبكات المترابطة التي تشمل واجهات ربط بين الإنسان والآلة ملاحظة: يمكن أن تكون وحدة واجهة ربط بين الإنسان والآلة منفصلة عن غرفة التحكم الرئيسية أو مضافة إليها	المعدات والشبكات الواقعة في المنطقة المحمية و/أو المناطق الحيوية
نظام الأجهزة والتحكم الخاص بنُظم التشغيل الآلي للعمليات	نُظم التحكم في الإنشاءات غير النووية في المحطة	3	الشبكات المترابطة التي تشمل واجهات ربط بين الإنسان والآلة ملاحظة: يمكن أن تكون وحدة واجهة ربط بين الإنسان والآلة منفصلة عن غرفة التحكم الرئيسية أو مضافة إليها أو يمكن أن تكون مقترنة بنظام معلومات خاص بعمليات الأجهزة والتحكم	المعدات والشبكات الواقعة في المنطقة المحمية و/أو المناطق الحيوية

الجدول ثالثاً-1- قائمة النُظم: مثال على تطبيق مستويات الأمن الحاسوبي ونطاقاته (تابع)

النظام	الوظيفة الأكثر أهمية	مستوى الأمن الحاسوبي	الحد المنطقي	الحد المادي
تكنولوجيا المعلومات للمكاتب	إجراء وظائف الموظفين	4	لا يُسمح بأي اتصال منطقي (سلكي أو لا سلكي أو محمول) مع أي نطاق من المستوى 1 أو 2 أو 3 (النظام)	مسموح في منطقة الوصول المحدود، والمنطقة المحمية، والمناطق الحيوية
نُظم الاتصالات	نداء لاستدعاء قوات التصدي أو الوكالات الخارجية الأخرى بحسب الاقتضاء	4	لا يُسمح بأي اتصال منطقي (سلكي أو لا سلكي أو محمول) مع أي نطاق من المستوى 1 أو 2 أو 3	مسموح في جميع الأماكن الضرورية لتحقيق أهداف المشغِّل
أجهزة تكنولوجيا المعلومات المحمولة الشخصية	لا يلزم أي منها - إعفاء فقط	5	غير مسموح بها إلّا في الشبكات من المستوى 5 لا يُسمح باقترابها من أي نطاق مخصص للمستوى 1 أو 2 أو 3	غير مسموح بها في المناطق الحيوية

باستخدام حاجز قوي، مع التحكم في الوصول وكشف الاقتحام لتلبية المتطلبات الموصى بها في المرجع [ثالثاً-1]، ويمكن التحكم في الوصول المادي من خلال مسار اتصالات بيانات محصن من الأعطال وأحادي الاتجاه (على سبيل المثال، صمام بيانات) وفقاً للإرشادات الواردة في هذا المنشور وفي المرجع [ثالثاً-2].

ثالثاً-11- عادة ما تُسند للنُظم التي تؤدي وظيفة منع ظروف الحوادث في المرفق (على سبيل المثال، النُظم المتصلة بنظام حماية المفاعل) مستوى الأمن الحاسوبي الأكثر صرامة. ولكن توضع المعدات التي تؤدي الوظيفة في منطقة حيوية قريبة من المفاعل، ولكن تُرصد المعدات من خلال تفاعل بين الإنسان والآلة في غرفة التحكم الرئيسية. ويؤدي ذلك إلى مشكلة محتملة في تطبيق نطاقات الأمن الحاسوبي، إذ قد يوجه التفاعل بين نظام حماية المفاعل وواجهة الربط بين الإنسان والآلة خارج المناطق الحيوية (على سبيل المثال، في المنطقة المحمية)، مما يؤدي إلى انتهاك لمتطلبات الأمن المادي.

ثالثاً-12- وقد يكون أحد الحلول هو فصل وظيفة الرصد عن وظيفة منع ظروف الحوادث. ومن شأن ذلك أن يسمح بفصل منطقي عن طريق صمام البيانات بين الأصول الرقمية في المنطقة الحيوية التي تمنع حالات الحوادث وتلك الموجودة خارج المنطقة الحيوية المستخدمة للرصد في غرفة التحكم الرئيسية. ولن يكون هذا الحل فعالاً إلا إذا كانت وظيفة منع ظروف الحوادث مستقلة ولا تحتاج إلى أي إجراء أو معلومات من خارج النُظم المكلفة بأداء الوظيفة.

ثالثاً-13- سيُخصص للأصول الرقمية التي تمنع وقوع الحوادث مستوى الأمن الحاسوبي الأكثر صرامة (المستوى 1) على أساس وظيفة المرفق. وستكون هذه الأصول الرقمية موجودة في منطقة حيوية من خارج غرفة التحكم الرئيسية. وسيُخصص للأصول الرقمية المسؤولة عن مراقبة نظام حماية المفاعل (مثل وحدة التحكم في واجهة الربط بين الإنسان والآلة الموجودة داخل غرفة التحكم الرئيسية) المستوى 2 من مستويات الأمن (أو أعلى).

النطاقات الواقعة خارج غرفة التحكم الرئيسية

نظام الأجهزة والتحكم لتقييد المفاعل (المستوى 2 من مستويات الأمن الحاسوبي)

ثالثاً-14- وفقاً للجدول ثالثاً-1، ينبغي أن تكون الأصول الرقمية التي تؤدي وظائف مخصصة للمستوى 2 من مستويات الأمن في منطقة حيوية وأن يكون لها وصول مادي ومنطقي خاضع لمراقبة صارمة. ومع ذلك، ولأسباب تشغيلية، يتطلب التحكم في وظيفة التفاعلية إلى أوامر من غرفة التحكم الرئيسية (على سبيل المثال، تعليمات بزيادة أو خفض القوى).

ثالثاً-15- وتقع المعدات في مناطق حيوية، وتحصّن البنية الأساسية للشبكة (الكبلات والمفاتيح واللوحات) عندما تكون في مناطق أقل أمناً (على سبيل المثال، إذا وجِّهت كبلات الشبكة من خلال المنطقة المحمية). وبالنظر إلى ضرورة إدخال أوامر (أي اتصالات تبدأ من غرفة التحكم الرئيسية إلى المعدات)، فإن تركيب صمام بيانات للتحكم في الوصول المنطقي غير ممكن.

ثالثاً-16- ويكمن الحل في عزل النطاق الذي يحتوي على أصول الشبكة والأصول الرقمية التي تدعم نقل الأوامر من النطاقات الأخرى المخصصة لمستويات أمنية أقل (المستويات من 3 إلى 5). ومن شأن ذلك أن يسمح بالفصل المنطقي بين النُظم الأخرى في المستويات الأدنى. ولن يكون هذا الحل فعالاً ما لم تكن وظيفة منع ظروف الحوادث مستقلة ولا تحتاج إلى أي إجراء أو معلومات من خارج النُظم المخصصة لأداء الوظيفة.

ثالثاً-17- ويمكن أيضاً تطبيق نفس الأساس المنطقي والحل نفسه على نظام معلومات عمليات الأجهزة والتحكم، ونُظم التشغيل الآلي لعمليات الأجهزة والتحكم المخصصة للمستوى 3 من مستويات الأمن الحاسوبي.

النطاقات أو الأجهزة المتصلة بالخارج

نُظم تكنولوجيا المعلومات والاتصالات المكتبية (المستوى 4 أو 5 من مستويات الأمن الحاسوبي)

ثالثاً-18- وفقاً للجدول ثالثاً-1، توفِّر نُظم تكنولوجيا المعلومات والاتصالات المكتبية الوظائف الضرورية التي يحتاج إليها الاتصال بالخارج. ويتيح ذلك للمشغِّل الوصول إلى المعلومات والموارد التي قد تكون مطلوبة أثناء أحداث وظروف معيّنة.

ثالثاً-19- ويمكن للوصلات الخارجية بالإنترنت والخدمات والشبكات والأجهزة الأخرى أن تزيد من المخاطر ما لم تتخذ تدابير لضمان عدم إمكانية تبادل المعلومات بين هذه المصادر والنُظم الخارجية التي تؤدي وظائف المرفق المخصصة لمستويات أمنية أعلى. ويلزم اتخاذ تدابير قوية لمنع أو تقييد الوصول إلى الواجهات البينية المحمولة، والاتصالات السلكية واللاسلكية، وغير ذلك من الوسائل التي يمكن من خلالها تبادل المعلومات مع الأصول الرقمية التي لديها اتصال بالخارج، وكذلك لفرض نطاقات أمن حاسوبي محكمة على هذه الأصول الرقمية باستخدام آليات فصل قوية. ويُناقش فصل النطاقات الأمنية داخل غرفة التحكم الرئيسية بمزيد من الاستفاضة في الفقرات من ثالثاً-21 إلى ثالثاً-27.

أجهزة تكنولوجيا المعلومات النقالة الشخصية (غير المخصصة)

ثالثاً-20- يُفترض أن أجهزة وبرامجيات تكنولوجيا المعلومات النقالة الشخصية غير محصنة لإزالة القدرات الخاصة بتبادل المعلومات من خلال القرب من الأصول الرقمية المعيّنة. ولذلك لا يُسمح بتواجد أجهزة تكنولوجيا المعلومات النقالة الشخصية في غرفة التحكم الرئيسية (أو غرف المعدات المرتبطة بها).

فصل نطاقات الأمن داخل غرفة التحكم الرئيسية

ثالثاً-21- كما لوحظ في الفقرة ثالثاً-13، تؤدي الأصول الرقمية في كثير من الأحيان وظائف متعددة للمرفق بحيث تتطلب مستويات مختلفة من الأمن الحاسوبي، ومن المرجح أن تكون هذه الأصول الرقمية موجودة داخل غرفة التحكم الرئيسية. ويزيد هذا القرب من خطر الإخلال بهذه الأصول من خلال الهجمات على الفضاء الإلكتروني.

ثالثاً-22- وينطبق ذلك بصفة خاصة في الحالات التي لا توجد فيها ضوابط مادية لحماية الوصول إلى الأصول الرقمية والوصلات بينها. وفي مثل هذه الحالة، سيكون لدى الطرف الداخلي الذي يمكنه الوصول منطقياً أو مادياً إلى نطاق غرفة التحكم الرئيسية فرصة غير مقيَّدة للإخلال بالأصول الرقمية في هذا النطاق.

ثالثاً-23- وتؤدي الأصول الرقمية (والنُظم) الموجودة في غرفة التحكم الرئيسية وظائف تحتاج في كثير من الأحيان إلى معلومات من أصول رقمية أخرى، أو تحتاج إلى إجراءات من جانب موظفي التشغيل. وفي حال فصل نظام حماية المفاعل منطقياً ومادياً عن غرفة التحكم الرئيسية كما في المثال أعلاه (على سبيل المثال، من خلال صمام بيانات للرصد)، فإن وظائف الأمان الأساسية الأخرى التي يتعيّن أخذها في الاعتبار هي التحكم في التفاعلية وإزالة الحرارة من قلب المفاعل.

ثالثاً-24- وتُسند النُظم التي تؤدي وظائف الأمان المذكورة في العادة إلى المستوى 2 من مستويات الأمن الحاسوبي. ووفقاً للجدول ثالثاً-1، يتطلب المستوى 2 من مستويات الأمن الحاسوبي حدود نطاق صارمة، ولكن يمكن أن تكون مجموعة من الحدود المادية والمنطقية.

ثالثاً-25- ويـزداد تعقيـد تخصيـص الأصـول الرقميـة فـي غرفـة التحكـم الرئيسـية للنطاقـات بسـبب الحاجـة إلـى وظائـف تكنولوجيـا المعلومـات المؤسسـية (علـى سـبيل المثـال، البريـد الإلكترونـي والإنترنـت وإدارة العمليـات) لمسـاعدة المشـغِّلين فـي غرفـة التحكـم الرئيسـية. ويمكـن أن يـؤدي تثبيـت الأصـول الرقميـة لدعـم هـذه الوظائـف إلـى إيجـاد حالـة تتـاح فيهـا النُظـم المخصصـة للمسـتويين 2 و5 لنفـس الموظفيـن فـي غرفـة التحكـم الرئيسـية، ولكـن يتعيّـن اشـتراط فصـل الأصـول الرقميـة التـي تـؤدي وظائـف المرفـق المخصصـة لمسـتويات أمـن مختلفـة.

ثالثاً-26- وفي هذا المثال، يمكن الأخذ بالحلول التالية:

(أ) لا يتـم توصيـل الشـبكات المنطقيـة بشـكل مباشـر علـى الإطـلاق، وتسـتخدم دائمـاً آليـات فصـل قويـة. ولا تمتـد الشـبكات المخصصـة للمسـتوى 2 مـن مسـتويات الأمـن إلـى خـارج غرفـة التحكـم الرئيسـية (وغـرف المعـدات المرتبطـة بهـا داخـل المنطقـة المحميـة) مـن دون آليـات الفصـل المذكـورة.

(ب) تُفصـل الشـبكات المنطقيـة وتحـدد بوضـوح، ويمكـن إسـناد المسـؤولية عنهـا إلـى وحـدات تنظيميـة مختلفـة (علـى سـبيل المثـال، تكنولوجيـا المعلومـات، أو الهندسـة).

(ج) يمكـن وضـع تدابيـر للتحكـم المـادي مـن أجـل إنشـاء نطاقـات فرعيـة داخـل غرفـة التحكـم الرئيسـية. وقـد تكـون هـذه النطاقـات الفرعيـة لوحـات مقفلـة وأقفـال وصـلات بينيـة محمولـة (علـى سـبيل المثـال، حواجـز المنافـذ) وقنـوات شـبكات آمنـة و/أو مناطـق وصـول محـدودة داخـل غرفـة التحكـم الرئيسـية.

ثالثاً-27- بالنظـر إلـى الحلـول المقترحـة أعـلاه، سـيتيح اسـتخدام عناصـر التحكـم المنطقيـة والماديـة وجـود مسـتويات أمـن حاسـوبي متعـددة داخـل نطـاق مـادي واحـد (مثـل غرفـة التحكـم الرئيسـية). ومـع ذلـك، يمكـن بعـد اتخـاذ إجـراءات أمـن حاسـوبي إضافيـة تقسـيم غرفـة التحكـم الرئيسـية إلـى عـدة نطاقـات فرعيـة يُخصـص كل منهـا لمسـتوى أمنـي خـاص بـه.

مراجع المرفق الثالث

[ثالثاً-1] الوكالـة الدوليـة للطاقـة الذريـة، توصيـات الأمـن النـووي بشـأن الحمايـة الماديـة للمـواد النوويـة والمرافـق النوويـة (INFCIRC/225/Revision 5)، العـدد 13 مـن سلسـلة الأمـن النـووي الصـادرة عـن الوكالـة، الوكالـة، فيينـا (2011).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

مسرد المصطلحات

تدابير التحكم الإداري: السياسات والإجراءات والممارسات التي تُحدد الإجراءات المسموح بها والضرورية والمحظورة لحماية النُظم القائمة على الحاسوب من خلال توفير تعليمات لإجراءات الموظفين والبائعين والمتعهدين والموردين.

هجوم مختلط: عمل ضار ينطوي على استخدام هجوم على الفضاء الإلكتروني بالتنسيق مع هجوم مادي.

النُظم القائمة على الحاسوب: التكنولوجيات التي تُنشئ المعلومات الرقمية أو تتيح الوصول إليها أو تعالجها أو تحوسبها أو تنقلها أو تخزنها، أو التي تؤدي خدمات تنطوي على هذه المعلومات أو تقدم خدمات من هذا القبيل أو تتحكم فيها. ويمكن لهذه النُظم أن تشمل الحواسيب المكتبية والنقالة واللوحية وغيرها من الحواسيب الشخصية؛ والهواتف الذكية، والحواسيب الكبيرة؛ ووحدات الخدمة؛ والحواسيب الافتراضية؛ والتطبيقات البرامجية؛ وقواعد البيانات؛ ووسائط التخزين القابلة للنقل؛ والأجهزة الرقمية وأجهزة التحكم الرقمي؛ وأجهزة التحكم المنطقية القابلة للبرمجة؛ والطابعات، وأجهزة الشبكات، والمكونات والأجهزة المدمجة.

الأمن الحاسوبي: جانب معيّن من جوانب أمن المعلومات يتعلق بحماية النُظم القائمة على الحاسوب.

حادثة أمن حاسوبي: أي واقعة تؤدي بالفعل أو يمكن أن تؤدي إلى الإخلال بسرية النُظم الحاسوبية (بما فيها المعلومات) أو سلامتها أو توافرها، أو تُشكل مخالفة للسياسات الأمنية أو خطراً وشيكاً بمخالفة السياسات الأمنية.

مستوى الأمن الحاسوبي: مدى صرامة الحماية المطلوبة لتحقيق متطلبات الأمن الحاسوبي المتعلقة بوظيفة ذات صلة بالأمن النووي و/أو الأمان النووي و/أو حصر المواد النووية ومراقبتها و/أو إدارة المعلومات الحساسة.

تدابير الأمن الحاسوبي: التدابير المتخذة بقصد منع وقوع أعمال شارة أو أعمال أخرى يمكن أن تخل بالأمن الحاسوبي، أو للكشف عن هذه الأعمال أو تعطيلها أو التصدي لها أو التخفيف من عواقبها في حال وقوعها.

برنامج الأمن الحاسوبي: خطة موضوعة لتنفيذ استراتيجية الأمن الحاسوبي التي تحدد الأدوار والمسؤوليات والإجراءات على مستوى المنظمة الواحدة. ويُحدد البرنامج بالتفصيل سُبل تحقيق أهداف الأمن الحاسوبي ويُشكل جزءاً من الخطة الأمنية العامة (أو يكن مرتبطاً بها).

إدارة مخاطر الأمن الحاسوبي: تقييم المخاطر المرتبطة بالهجمات المحتملة على الفضاء الإلكتروني التي يمكن أن تقوِّض الأمان النووي أو الأمن النووي وإدارة هذه المخاطر. وتُدار مخاطر الأمن الحاسوبي على مستوى المرفق وعلى مستوى النظام.

نطاق الأمن الحاسوبي: مجموعة من النُظم التي لها حدود مادية و/أو منطقية مشتركة - وتخضع لترتيبات قائمة على معايير إضافية، عند الاقتضاء - ويحدد لها مستوى واحد من مستويات الأمن الحاسوبي بهدف تبسيط إدارة تدابير الأمن الحاسوبي والتواصل بشأنها وتطبيقها.

هجوم على الفضاء الإلكتروني: عمل ضار يُنفذ بقصد سرقة بند مستهدف محدد أو تعديله أو منع الوصول إليه أو إتلافه، من خلال الوصول غير المأذون به إلى نظام حساس قائم على الحاسوب (أو تنفيذ إجراءات داخل هذا النظام).

بنية الأمن الحاسوبي الدفاعية: ترتيب النُظم القائمة على الحاسوب وفقاً لمتطلبات التصميم والقيود والتدابير التي تفرض أثناء دورة حياة النظام، مثل النُظم التي تؤدي وظائف المرفق المحددة ذات الأهمية لأمان المرفق وأمنه، والتي تُسند إلى مستويات أمن حاسوبي في المرفق وتحصل على المستوى المطلوب من الحماية.

تهديد محتاط له في التصميم: سمات وخصائص خصوم داخليين و/أو خارجيين محتملين، قد يحاولون سرقة أو تخريب المواد النووية، ويتم تصميم وتقييم نظام حماية مادية للحماية ضد هذه السمات والخصائص.

الكشف: عملية في نظام الحماية المادية تبدأ باستشعار فعل ضار محتمل أو غير مأذون به ويكتمل بتقييم سبب الإنذار.

وظيفة المرفق: مجموعة منسقة من الإجراءات والأعمال والعمليات المرتبطة بمرفق نووي. وقد يكون الغرض منها أداء وظائف مهمة أو متعلقة بالأمان النووي أو الأمن النووي أو حصر المواد النووية ومراقبتها، أو إدارة المعلومات الحساسة. وتشمل وظائف المرفق أيضاً الوظائف التشغيلية والإدارية (أو التنظيمية).

أمن المعلومات: المحافظة على سرية المعلومات وسلامتها وتوافرها.

طرف داخلي: شخص لديه إذن بالوصول إلى المرافق ذات الصلة أو الأنشطة المرتبطة بها أو إلى المعلومات الحساسة أو إلى أصول المعلومات الحساسة ويمكنه ارتكاب أو تسهيل ارتكاب أعمال إجرامية أو متعمدة غير مأذون بها، وتنطوي على مواد نووية أو مواد مشعة أخرى أو المرافق أو الأنشطة المرتبطة بها أو تستهدفها، أو الأعمال الأخرى التي تُقرر الدولة أن لها أثر ضار على الأمن النووي.

حدث متصل بالأمن النووي: حدث ينطوي على تداعيات محتملة أو فعلية على الأمن النووي يجب التصدي له.

تدابير الأمن النووي: تدابير يُقصد منها منع أي تهديد بإكمال عمل ضار أو الكشف عن أحداث الأمن النووي أو التصدي لها.

منظومة الأمن النووي: منظومة تتألف من:

- الإطار التشريعي والرقابي والنُظم والتدابير الإدارية التي تُنظم الأمن النووي للمواد النووية، والمواد المشعة الأخرى، والمرافق ذات الصلة، والأنشطة ذات الصلة؛
- المؤسسات والمنظمات الموجودة داخل الدولة والمسؤولة عن ضمان تنفيذ الإطار التشريعي والرقابي والنُظم الإدارية الخاصة بالأمن النووي؛
- نُظم الأمن النووي وتدابير الأمن النووي اللازمة من أجل منع وقوع أحادث متصلة بالأمن النووي والكشف عنها والتصدي لها.

نظام الأمن النووي: مجموعة متكاملة من تدابير الأمن النووي.

تدابير التحكم المادي: الحواجز المادية التي تحمي الأدوات والنُظم القائمة على الحاسوب والأصول الداعمة من التلف المادي وتمنع الوصول المادي إليها من دون إذن.

الأصول الرقمية الحساسة: أصول المعلومات الحساسة التي تكون عبارة عن نُظم قائمة على الحاسوب (أو تُشكل أجزاء منها).

المعلومات الحساسة: المعلومات الموجودة في أي شكل من الأشكال، بما في ذلك البرامجيات الحاسوبية، والتي يمكن أن يؤدي إفشاؤها أو تعديلها أو تبديلها أو إتلافها من دون إذن أو الحرمان من استخدامها إلى الإخلال بالأمن النووي.

أصول المعلومات الحساسة: أي معدات أو مكونات تُستخدم لتخزين المعلومات الحساسة أو معالجتها أو التحكم فيها أو إرسالها. وعلى سبيل المثال، تشمل أصول المعلومات الحساسة نُظم المراقبة والشبكات ونُظم المعلومات وأي وسائط إلكترونية أو مادية.

تدابير التحكم التقني: الأجهزة أو البرامجيات المستخدمة لمنع حدوث اقتحام أو عمل ضار آخر وكشفه والتخفيف من عواقبه والتعافي منه.

تقييم التهديد: تقييم للتهديدات - استناداً إلى المعلومات المتاحة من خلال الاستخبارات، وهيئات إنفاذ القوانين، والمعلومات المفتوحة المصدر - يصف دوافع تلك التهديدات ونواياها وقدراتها.

بيان التهديد: وصف لخصم ذي مصداقية (بما في ذلك سماته وخصائصه) يتخذ شكل تهديد محتاط له في التصميم أو بيان تهديد تمثيلي، ويتم إعداده بناءً على تقييم تهديد الأمن النووي الوطني.

IAEA
الوكالة الدولية للطاقة الذرية

رقم 26

طلب شراء المنشورات محليًّا

يمكن شراء المنشورات المسعَّرة الصادرة عن الوكالة الدولية للطاقة الذرية من المصادر المذكورة في القائمة أدناه أو من المكتبات المحلية الكبرى.

أمَّا المنشورات غير المسعَّرة فينبغي توجيه طلبات شرائها إلى الوكالة مباشرة. وترد تفاصيل الاتصال في آخر هذه القائمة.

أمريكا الشمالية

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 613 745 7660
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

سائر بلدان العالم

برجاء الاتصال بالمورّد المحلي المفضّل لديكم، أو بالموزِّع الرئيسي الخاص بنا:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

الطلبات التجارية والاستفسارات:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

الطلبات الفردية:

www.eurospanbookstore.com/iaea

للحصول على مزيد من المعلومات:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

ويمكن توجيه طلبات شراء المنشورات، المسعَّرة وغير المسعَّرة على السواء، مباشرة إلى العنوان التالي:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

يُقدم هذا المنشور إرشادات بشأن إرساء الأمن الحاسوبي وتحسينه وتطويره وتنفيذه والمحافظة عليه واستدامته داخل المرافق النووية. ويتناول استخدام النُهُج القائمة على الإحاطة بالمخاطر لإرساء وتعزيز سياسات وبرامج الأمن الحاسوبي؛ ويصف دمج الأمن الحاسوبي في نظام إدارة المرافق؛ ويضع نهجاً منظماً لتحديد وظائف المرافق وتدابير الأمن الحاسوبي المناسبة التي تحمي المرافق من الهجمات الإلكترونية بما يتوافق مع تقييم التهديد أو التهديد المحتاط له في التصميم. ويتناول هذا المنشور جميع الأصول الرقمية المرتبطة بمرفق نووي وينطبق على جميع مراحل عمر المرفق النووي.

الوكالة الدولية للطاقة الذرية
فيينا