سلسلة الأمن النووي رقم 33-T الصادرة عن الوكالة الدولية للطاقة الذرية

إرشادات تقنية

الأمن الحاسوبي لنظُمُ الأجهزة والتحكُّم في المرافق 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، وتكمّلها، 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، تركّز على كيفية العمل بالتوصيات المتعلقة بمجالات واسعة للأمن النووي.
- **الإرشادات التقنية** تقدّم إرشادات عن مواضيع تقنية محدّدة لاستكمال الإرشادات المحدّدة في أدلة التنفيذ. وهي تركّز 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.

وتُعِد 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.

الأمن الحاسوبي
لنُظُم الأجهزة والتحكُّم
في المرافق 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
برواني 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
فيبت 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 المقرّ 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 الرئيسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع".

العدد T-33 من سلسلة الأمن النووي الصادرة عن الوكالة

الأمن الحاسوبي لنُظُم الأجهزة والتحكُّم في المرافق النووية

إرشادات تقنية

الوكالة الدولية للطاقة الذرية
فيينا، 2024

ملاحظة بشأن حقوق النشر

جميع المنشـــورات العلمية والتقنية الصـــادرة عن الوكالة محمية بموجب الاتفاقية العالمية لحقوق التأليف والنشـــر بصـــيغتها المعتمدة في عام 1952 (برن) والمنقحة في عام 1972 (باريس). وقد عمدت المنظمة العالمية للملكية الفكرية (جنيف) لاحقاً إلى توســـيع نطاق حقوق التأليف والنشـــر لتشـــمل الملكية الفكرية الإلكترونية والفرضية. ويجب الحصول على إذن باستخدام النصوص الواردة في منشورات الوكالة بشكلها المطبوع أو الإلكتروني، استخداما كلياً أو جزئياً؛ ويخضع هذا الإذن عادة لاتفاقات متعلقة برسوم الجعالة الأدبية. ويُرحَّب بأية اقتراحات تخص الاستنساخ والترجمة لأغراض غير تجارية، وسيُنظَر فيها على أساس كل حالة على حدة. وينبغي توجيه أية اســـتفســـارات إلى قســـم النشـــر التابع للوكالة (IAEA Publishing Section) على العنوان التالي:

Marketing and Sales Unit
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
https://www.iaea.org/ar/almanshurat

آذار/مارس 2024
STI/PUB/1787
ISBN 978-92-0-628823-8 (نسخة ورقية)
ISBN 978-92-0-628523-7 (نسخة PDF)
ISSN 2520-6923

تصدير

يتمثّـــل هدف الوكالة الرئيسي بموجب نظامها الأساسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع". ويشمل عملنا منع انتشار الأسلحة النووية وضمان إتاحة التكنولوجيا النووية للأغراض السلمية في مجالات مثل الصحّة والزراعة. ومن الضروري التصرف بطريقة مأمونة في جميع المواد النووية والمواد المشعّـــة الأخرى وفي جميع المرافق التي يُحتفَظ فيها بهذه المواد، ومن الضروري حمايتها بصورة مناسبة من الأفعال الإجرامية أو المتعمدة غير المأذون بها.

فالمســـؤولية عن الأمن النووي تقع على عاتق كل دولة على حدة، بيد أنّ التعاون الدولي يعد عاملاً جوهرياً لدعم الدول في إنشاء وتعهُّد نُظم أمن نووي فعّالة. والدور الجوهري الذي تؤديه الوكالة في تيســـير هذا التعاون وتقديم المســـاعدة إلى الدول هو أمر معترف به تماماً. ويعبّر الدور الذي تؤديه الوكالة عن عضـــويتها الواسعة النطاق وولايتها ودرايتها الفريدة وخبرتها الطويلة في تقديم المساعدة التقنية والإرشادات المتخصصة العملية إلى الدول.

وما انفكت الوكالة، منذ عام 2006، تصدر منشورات سلسلة الأمن النووي لمســـاعدة الدول على إنشـــاء نُظم وطنية فعالّة في مجال الأمن النووي. وتُكمّل هذه المنشـــورات الصـــكوك القانونية الدولية المتعلقة بالأمن النووي، 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.

وتُوضع الإرشادات بمشاركة فعّالة من جانب خبراء من الدول الأعضاء في الوكالة، مما يكفل تعبير الإرشادات عن توافق في الآراء بشأن الممارسات الجيدة في مجال الأمن النووي. وتعمل لجنة إرشادات الأمن النووي التابعة للوكالة والتي أنشئت في آذار/مارس 2012 والمكوَّنة من ممثّلي الدول الأعضاء على استعراض مسودات المنشـــورات في ســـلســـلة الأمن النووي الصـــادرة عن الوكالة وتوافق عليها أثناء صياغتها.

وستواصل الوكالة العمل مع دولها الأعضاء لضمان إتاحة مزايا التكنولوجيا النووية السلمية لتحسين صحة، ورفاه وازدهار الناس في جميع أنحاء العالم.

ملحوظة تحريرية

الإرشادات 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 جزءاً لا يتجزأ من المنشور. ويكون للمواد الواردة في أي تذييل نفس صفة المتن. وتُستَخدم المرفقات لتوفير معلومات أو تفسيرات إضافية. ولا تُعتبَر 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 ضمناً 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 مسجَّلة أو دون تلك الإشارة) لا يعني ضمناً وجود أي نية لانتهاك حقوق الملكية، كما لا ينبغي أن يُفسَّر على أنه تأييد أو توصية من جانب الوكالة.

المحتويات

أولا- مقدمة

الخلفية

1-1- تؤدي نظم الأجهزة والتحكم دوراً حاسماً في ضمان التشغيل المأمون للمرافق النووية. ومع استمرار تطور التكنولوجيات الرقمية وزيادة قدرتها، أصبحت تُدمج بشكل متزايد في نظم الأجهزة والتحكم[1]. وتستعين المرافق النووية الجديدة وتصاميم المرافق النووية الحديثة بنظم رقمية للأجهزة والتحكم ذات درجة عالية من التكامل للتعامل بكفاءة وفي وقت واحد مع كميات هائلة من بيانات العمليات، وتتطلب هذه النظم قدراً أقل من المتابعة والتدخل البشري عن نظم الأجهزة والتحكم السابقة. وغالباً ما يؤخذ بالتكنولوجيات الرقمية في نظم الأجهزة والتحكم أثناء تحديث المرافق الحالية. ومع ذلك، فإن تطبيق التكنولوجيات الرقمية في نظم الأجهزة والتحكم جعل هذه النظم عرضة للهجمات السيبرانية.

1-2- والهجوم السيبراني هو عمل شرير يقوم به أفراد أو منظمات يستهدف معلومات حساسة أو أصول معلومات حساسة بقصد سرقة هدف محدد أو تغييره أو منع الوصول إليه أو تدميره من خلال الوصول غير المأذون به إلى نظام حساس (أو ارتكاب أعمال تخريبية في هذا النظام). وتشمل أصول المعلومات الحساسة نظم المراقبة والشبكات ونظم المعلومات وأي وسائط إلكترونية أو مادية. وشن الخصوم هجمات سيبرانية ناجحة موجهة إلى نظم الأجهزة والتحكم، مثل الهجوم السيبراني بالفيروس الحاسوبي ستاكسنت، مما أدى إلى إتلاف المعدات في أحد المرافق النووية [1].

1-3- وقد تهدِّد الهجمات السيبرانية على نظم الأجهزة والتحكم أمان وأمن المرافق النووية. وقد تسهم في التخريب أو تساعد في سحب مواد نووية دون إذن. وقد تؤدي آثار الهجمات السيبرانية على نظم الأجهزة والتحكم المتعلقة بالأمان إلى مجموعة واسعة من العواقب، مثل فقدان مؤقت للتحكم في العمليات أو عواقب إشعاعية غير

[1] تُستخدم عبارة "نظام الأجهزة والتحكم" طوال الجزء المتبقي من هذا المنشور للإشارة إلى نظم الأجهزة والتحكم التي تستخدم التكنولوجيات الرقمية أو تعتمد عليها أو التي تحصل على الدعم من هذه التكنولوجيات.

مقبولة. كما أن الوعي العام بالهجمات السيبرانية التي تؤثر على نظم الأجهزة والتحكم قد يقوض الثقة في أمان وأمن المرافق النووية.

1-4- والحاجة إلى حماية النظم القائمة على الحاسوب (بما في ذلك نظم الأجهزة والتحكم) منصوص عليها في توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرافق النووية [2] (INFCIRC/225/Revision 5)، الفقرة 4-10، التي تنص على ما يلي:

"وينبغي أن تكون النظم 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*".

1-5- ويقدِّم العدد 17 من سلسلة الأمن النووي الصادرة عن الوكالة، الأمن الحاسوبي في المرافق النووية [3]، إرشادات خاصة بالمرافق النووية بشأن تنفيذ برنامج للأمن الحاسوبي لدعم الإرشادات الواردة في المرجع [2]. كما يقدِّم المرجع [3] تفاصيل بشأن المصطلحات الرئيسية مثل "الأمن الحاسوبي" و"أمن تكنولوجيا المعلومات" و"الأمن السيبراني". ويعتبر المصطلحان "أمن تكنولوجيا المعلومات" و"الأمن السيبراني"، لغرض هذا المنشور، مرادفان للأمن الحاسوبي ولن يُستخدما فيما بعد.

1-6- ويجب مراعاة الأمن الحاسوبي بوضوح في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم. ويشير مصطلح "دورة الحياة" (على عكس الفترة العمرية) إلى أن عمر النظام يتسم بالتدوير بالفعل (كما في حالة إعادة التدوير أو إعادة المعالجة)، ولا سيما أن عناصر النظام القديم تستخدم في النظام الجديد. ويحتوي المرجع [4] على قائمة بالأنشطة النموذجية لدورة حياة الأجهزة والتحكم.

1-7- ومن الناحية التاريخية، لم يحظ الأمن الحاسوبي باهتمام كبير في تصميم نظم الأجهزة والتحكم في المرافق النووية لأنه كان يُفترض أن النظم السلكية أو التناظرية لم تكن معرَّضة للهجوم السيبراني بسبب برمجتها الثابتة غير القابلة للتغيير وانعزالها وانفصالها وإلى الغياب شبه التام للاتصالات التفاعلية، ولا سيما مع

الشـــبكات أو النظم الخارجية. ولقد غيَّر الانتقال إلى التكنولوجيا الرقمية طبيعة نظم الأجهزة والتحكم في المرافق النووية من خلال تمكين التوصـــيل البيني بين نظم الأجهزة والتحكم القابلة لإعادة البرمجة (عن بُعد أو في الموقع) والمتمايزة من الناحية الوظيفية.

1-8- وأدى الاستخدام المتزايد للمكونات والأجهزة الرقمية المتعددة الاستخدامات والقابلة للبرمجة إلى تقليل تنوع نظم الأجهزة والتحكم. ويشمل ذلك استخدام العناصر والنُهُج المشـتركة في مجموعة متنوعة من التطبيقات الصـناعية (مثل بروتوكولات الاتصال). كما يمكن أن يمتد تأثير الأعمال الشريرة[2] التي تستهدف هذه التكنولوجيات الشائعة في صناعات أخرى إلى أحد المرافق النووية.

1-9- وقد يتعرض أمان وأمن المرافق النووية للتهديد من الأفراد المأذون لهم بالوصول، كأشخاص داخليين، سواء كانوا في الموقع أو في مكان بعيد، ممن لديهم إمكانية التحكم في نظم الأجهزة والتحكم إما إلكترونيًّا أو من داخل المكان الذي توجد به هذه الأجهزة. وقد يكون هؤلاء الأشـــخاص الداخليون من موظفي المرافق أو الموظفين الذين يســـتعين بهم البائعون أو المتعاقدون أو الموردون وقد يكون لديهم القدرة على استخدام وصولهم المأذون به للقيام بأعمال شريرة. وهناك إقرار بالحاجة إلى حماية النظم الحاسوبية من التهديدات الداخلية في المرجع [5].

الهدف

1-10- الهدف من هذا المنشور هو توفير إرشادات بشأن الأمن الحاسوبي لحماية نظم الأجهزة والتحكم في المرافق النووية من الأعمال الشـــريرة التي يمكن أن تمنع هذه النظم من أداء وظائفها المتعلقة بالأمان والأمن. وفي حين أن هذا المنشور يركِّز على التشغيل الآمن لهذه النظم، فإن تطبيق هذه الإرشادات قد يسهم أيضاً في تحسين الأمان والأداء التشغيلي للمرافق النووية.

1-11- وهذا المنشور موجه إلى السلطات المختصة، بما في ذلك الهيئات الرقابية، فضلاً عن موظفي إدارة المرافق النووية وتشغيلها وصيانتها وهندستها، وبائعي نظم

2 لا تشمل الأعمال الشريرة الأحداث الناجمة عن خطأ بشري أو الأعطال العشوائية التي تحدث في المعدات أو المكونات.

الأجهزة والتحكم ومتعاقديها وموردِيها، ومصممي نظم الأجهزة والتحكم، ومختبرات البحوث، والمنظمات الأخرى المعنية بأمان المرافق النووية وأمنها.

النطاق

1-12- نطاق هذا المنشـــور هو تطبيق تدابير الأمن الحاســـوبي على نظم الأجهزة والتحكم التي توفر الأمـان أو الأمن[3] أو الوظـائف المســـاعدة في المرافق النوويـة. وتهدف هذه التدابير إلى حمايـة نظم الأجهزة والتحكم من الأعمـال الشـــريرة التي يرتكبها أفراد أو منظمات. كما يتناول هذا المنشـــور تطبيق هذه التدابير على بيئات تطوير هذه النظم ومحاكاتها وصيانتها.

1-13- وتنطبق الإرشـادات الواردة في هذا المنشور على نظم الأجهزة والتحكم في المرافق النوويـة الجديدة[4] وعلى نظم الأجهزة والتحكم الجديدة في المرافق القائمـة. ومن المتوقع أن تُنفَّذ الإرشـــادات إلى أقصـــى حد ممكن على نظم الأجهزة والتحكم القديمة في المرافق القائمة، بما في ذلك تلك التي لا تستخدم التكنولوجيا الرقمية.

1-14- وقد تشكِّل نظم التواصـل ونظم تكنولوجيا المعلومات والاتصـالات الأخرى، مثل نظم التحكم في العمل والاتصـالات، مخاطر على نظام (نظم) الأجهزة والتحكم، على الرغم من عدم تناول هذا المنشـور هذه المسـألة صـراحة. ويجب أن تؤخذ هذه المخاطر في الحسبان عند تصـميم تدابير الأمن الحاسوبي لنظم الأجهزة والتحكم في المرفق وعند تنفيذ هذه التدابير. وقد تختلف تدابير الأمن الحاســـوبي لهذه النظم عن تلك المطبقة على نظم الأجهزة والتحكم ويجب تقييمها وتصميمها على نحو مناسب.

1-15- ولا يقدم هذا المنشور إرشـادات شـاملة حول اعتبارات الأمان لنظم الأجهزة والتحكم. ويمكن الاطلاع على هذه الإرشـــادات في المرجعين [4، و6]. وبالإضـــافة إلى ذلك، لا يعرّف هذا المنشور أو يغيّر المصـطلحات التقنية المسـتخدمة في معايير الأمان الصـادرة عن الوكالة وغيرها من منشـورات الوكالة المتعلقة بالأمان. ويُسلِّط

3 تشمل النظم التي توفر الوظائف الأمنية النظمَ المستخدمة للحماية المادية وحصر المواد النووية ومراقبتها.

4 المرفق الجديد هو مرفق لم يُكمل بعدُ مرحلة الإدخال في الخدمة.

الضوء على هذه المصطلحات عند استخدامها في هذا المنشور، ويمكن الاطلاع على تعاريفها في مسرد مصطلحات الأمان الصادر عن الوكالة [7].

الهيكل

1-16- بعد هذه المقدمة، ينقسم هذا المنشور إلى أربعة أقسام. ويقدِّم القسم 2 لمحة عامة عن نظم الأجهزة والتحكم المستخدمة في المرافق النووية ودور الأمن الحاسوبي في حماية هذه النظم من الهجمات السيبرانية. ويعرض القسم 3 العلاقة بين الأمن الحاسوبي وأمان نظم الأجهزة والتحكم. ويقدم القسم 4 إرشادات الأمن الحاسوبي الواجب تطبيقها في مراحل دورة الحياة المختلفة لنظم الأجهزة والتحكم، بما في ذلك أثناء إخراج المرفق من الخدمة.

ثانيا- المفاهيم الأساسية للأمن الحاسوبي لنظم الأجهزة والتحكم

2-1- تُستخدم نظم الأجهزة والتحكم في المرافق النووية لرصد العمليات والمعدات والتحكم فيها. وتشمل هذه النظم ما يلي:

(أ) نظم سكادا (التحكم الإشرافي والحصول على البيانات)؛
(ب) نظم التحكم الموزَّعة؛
(ج) نظم التحكم الرقمية المركزية؛
(د) نظم التحكم المكوَّنة من أجهزة التحكم المنطقي القابلة للبرمجة؛
(هـ) أجهزة التحكم الدقيقة والأجهزة "الذكية"؛
(و) النظم التي تستخدم أجهزة إلكترونية مبرمَجة (مثل مصفوفات البوابات القابلة للبرمجة ميدانيًّا والأجهزة الإلكترونية المعقدة القابلة للبرمجة والدوائر المتكاملة المخصصة لتطبيقات محددة).

وغالباً ما تُسمى النظم المماثلة التي تتحكم في المنشآت الصناعية "نظم التحكم الصناعية".

2-2- وصُـمِّمت نظم الأجهزة والتحكم لضـمان الأمان والأمن والموثوقية والثبات في سير عمل المرفق النووي في كل من ظروف التشغيل العادية وغير العادية[5]. وقد تعود الاعتبارات المتعلقة بالتصـميم والتدابير التي تهدف إلى تحسـين الأمان أيضـاً بفوائد على الأمن. فمثلاً، التدابير المتعلقة بـالتصـــميم مثل ثبات الأداء، وتجنب الأعطال، واكتشـــاف الأعطال، ونهج تحمل الأعطال، وإدارة التكوين، والتحقق المسـتقل والتحقق من الصـحة، وطرق الاختبار المتقدمة الأخرى، قد توفِّر قدراً من الحماية من المحاولات الشريرة لتغيير أسلوب عمل نظم الأجهزة والتحكم.

2-3- ويتضـمن تصـميم الهيكل العام لنظم الأجهزة والتحكم مفاهيم قد تسـهم في الأمن الحاسـوبي من خلال التخفيف من آثار اختلال التشـغيل المتعمد أو العرضـي[6]، مثل الاســتقلال والاســتحاطة والدفاع عن الأمان في العمق والتنوع[7]. ويُســتخدم مصــطلح "الدفاع عن الأمان في العمق" في هذا المنشــور للإشــارة إلى الدفاع في العمق على النحو المحدَّد في مســرد الأمان الصــادر عن الوكالة [7]، لتمييزه عن تطبيق مفهوم "الدفاع في العمق" المماثل الذي يركِّز على الأمن (على النحو المحدَّد في أساسيات الأمن النووي [8]) عند تنفيذ تدابير الأمن الحاسوبي، الوارد في القسم 4.

2-4- وينبغي تقييم تنفيذ هذه المفاهيم في الهيكل العام لنظم الأجهزة والتحكم وتدابير التصميم الأخرى لتحديد مساهمتها في الأمن الحاسوبي. فعلى سبيل المثال، من المرجح أن يؤدي تنوع التصـــميم أو التكنولوجيا إلى الحد من الثغرات الأمنية الشائعة بين النظم الرئيسية للأمان أو التحكم؛ ومع ذلك، قد يضيف هذا التنوع ثغرات أمنية لكل نظام على حدة.

2-5- وتنطبق الإرشـــادات الواردة في هذا المنشـــور على جميع نظم الأجهزة والتحكم المرتبطة بمرفق نووي ما لم يذكر خلاف ذلك.

---

5 يشار إلى عملية التشغيل في الظروف غير العادية في مسرد الأمان الصادر عن الوكالة [7] كمرادف لعبارة "واقعة تشغيلية منتظرة". وفي هذا المنشور، يعتبر المصطلح الأول أيسر في الفهم.

6 يُستخدم مصطلح "اختلال التشغيل" في هذه الوثيقة للإشارة إلى الحالات التي لم تكن محل نظر في السابق (أي ليست وقائع تشغيلية متوقعة)، والتي لا يعمل بسببها نظام الأجهزة والتحكم كما هو متوقع.

7 تشير الاستقلالية والاستحاطة والدفاع عن الأمان في العمق والتنوع هنا إلى مفاهيم محدَّدة مستخدمة في مسرد مصطلحات الأمان الصادر عن الوكالة [7].

الأمن الحاسوبي لنظم الأجهزة والتحكم

2-6- تنصّ الفقرة 2-2 من المرجع [2] على ما يلي:

"ينبغي أن تسعى *منظومة الحماية المادية*[8] الخاصة بالدولة إلى تحقيق هذه الأهداف من خلال ما يلي:

— منع ارتكاب عمل *شرير* عن طريق الردع وبحماية المعلومات الحساسة؛

— إدارة محاولة ارتكاب عمل *شرير* أو عمل شرير مرتكب بالفعل من خلال نظام متكامل *للكشف* والتعطيل والتصدي؛

— التخفيف من عواقب العمل *الشرير*".

2-7- وفيما يلي بعض الأمثلة على كيفية تطبيق الأهداف المتعلقة بالمنع والإدارة والتخفيف من العواقب على الأمن الحاسوبي لنظم الأجهزة والتحكم:

— المنع: تثبيت أجهزة مؤمَّنة ضد التلاعب تمنع اتصالات البيانات غير المأذون بها لتقليل احتمالية حدوث هجوم سيبراني قائم على الشبكة من شأنه أن يؤثر سلباً على نظام الأجهزة والتحكم.
— الإدارة، بما في ذلك الكشف والتعطيل والتصدي: من خلال فحص ملفات سجل أحداث النظام، قد يتمكن المشِّغل من كشف الأحداث الممهِّدة للحوادث واستهلال إجراءات وقائية قبل بدء ارتكاب عمل شرير يمكن أن يؤثر سلباً على أمان المرفق أو أمنه.
— التخفيف والتعافي: إذا اكتُشف أن نظام الأجهزة والتحكم مصاب ببرامج خبيثة، فبمجرد إيقاف انتشار هذه البرامج الخبيثة، سيحدِّد المشغِّل ما إذا كانت تدابير التحكم التعويضية (مثل توقيعات مكافحة الفيروسات المحدَّثة، أو تثبيت أو تعزيز نظم منع التسلل أو نظم الكشف أو كليهما) ضرورية

8 كان مصطلح "الحماية المادية" يُستخدم على مر التاريخ لوصف ما يُعرف اليوم بالأمن النووي للمواد النووية والمرافق النووية.

لمنع الإصـــابة مجدَّدا، وإعادة بناء النظام، والتحقق من فعالية تدابير التحكم التعويضـية، واسـتعادة النظام وإعادته إلى الخدمة، بعد إجراء تحليل مفصـل للأمان وأنشطة التحقق من سلامة النظام، إذا لزم الأمر.

2-8- وفي بعض الأحيان، تسـتند حماية نظم الأجهزة والتحكم ضـد الاختراق إلى افتراض أن تدبيراً وقائيًّا واحداً سيكون كافيًّا، مثل عزل النظم عن الشبكات الأخرى. غير أنه من المرجح أن يؤدي هذا الافتراض إلى القصـــور في تطبيق تدابير الإدارة والتخفيف بحيث يؤدي قصـــور هذا التدبير الوحيد للأمن الحاســوبي إلى المســاس بالنظام المحمي.

2-9- وقد وضِـــع العديد من النُهُج والأســـاليب والتقنيات والمعايير والمبادئ التوجيهية المختلفة للأمن الحاسوبي لنظم تكنولوجيا المعلومات والاتصـالات العامة. وبعضــها لا ينطبق مباشـرة على نظم الأجهزة والتحكم في المرافق النووية، التي لها احتياجات محددة للأمن الحاســوبي لا تتشـــارك فيها مع نظم تكنولوجيا المعلومات والاتصالات.

2-10- ومع ذلك، وبما أنه لا يمكن فصــل الأمن الحاسـوبي لنظم الأجهزة والتحكم فصــلاً كاملاً عن الأمن الحاسـوبي لنظم تكنولوجيا المعلومات والاتصــالات، ينبغي للمشـغِّلين والرقابيين وضـع سياسـات ومتطلبات وتدابير وممارسـات للأمن الحاسوبي تراعي نظم الأجهزة والتحكم ونظم تكنولوجيـا المعلومـات والاتصـــالات بطريقـة متكاملة.

2-11- وتتمتع العديد من نظم الأجهزة والتحكم بدورة حياة لعقود، بما في ذلك الفترات التي قد يكون فيها دعم البائعين غير متاح أو غير كاف لتلبية متطلبات الأمن الحاســوبي للنظم[9]. ويشــمل ذلك الدعم المقدَّم من البائع الأصــلي والأطراف الثالثة المرتبطة به. فعلى سبيل المثال، بمرور الوقت، قد لا توفر برامج مكافحة الفيروسات حماية كافية ضــد اســتغلال الثغرات الأمنية في نظم الأجهزة والتحكم، بســبب عدم توافق الأجهزة أو البرامج أو التعذر في الاستمرار في توفير تحديثات التوقيع.

9 في هذا المنشور، تشير "متطلبات الأمن الحاسوبي" إلى متطلبات كتابية محدَّدة تفرضها السلطة المختصة ذات الصلة أو المشغِّل للامتثال للمتطلبات الرقابية.

2-12- وفي معظم التطبيقات، تعمل نظم الأجهزة والتحكم في الوقت الفعلي، وتُنفِّذ إجراءات نظـام الأجهزة والتحكم خلال فترات زمنيـة دقيقـة. ومن الأمثلـة على إجراءات نظم الأجهزة والتحكم في المرافق النوويـة التحكم في العمليـات العـاديـة، والإجراءات الوقائية، وإجراءات التقييد، وإرسال إشارات إنذار إلى المشغِّلين. ويجب ألا تعيق تدابير الأمن الحاســوبي أو تمنع أو تؤخر أداء الإجراءات التشــغيلية أو إجراءات الأمان اللازمة. ويمكن اســتخدام تدابير الأمن الحاســوبي لنظم الأجهزة والتحكم الحديثة لمنع الأعمال الشـريرة واكتشـافها وتعطيلها والتصـدي لها والتخفيف من عواقبها، ولكن يجب توخي الحذر لضــمان أن تدابير التصــدي لا تعيق وظائف الأمان المعتمدة أو تضع النظام خارج أساسه التصميمي[10].

2-13- وقد تؤدي تدابير الأمن الحاسوبي التي تُطبق بأثر رجعي أو تُنفَّذ بشكل سيئ إلى مزيد من التعقيد في تصــميم نظـام الأجهزة والتحكم، ممـا قد يؤدي إلى زيـادة احتمال عطل نظام الأجهزة والتحكم أو سوء تشغيله.

2-14- ويحدِّد العنصـر الأسـاسـي رقم 9 من أسـاسـيات الأمن النووي [8] اسـتخدام النُهُج القائمة على العلم بالمخاطر لتخصــيص الموارد وفي تنفيذ الأنشــطة المتعلقة بالأمن النووي. وقد يكون التصــميم الذي يوضــع باســتخدام نهج قائم على العلم بالمخاطر لمراعاة الاعتبارات الأمنية منذ بداية عملية التصــميم أبســط وأكثر قوة بسبب تكامل السمات الأمنية، أو إزالة الوظائف غير الضـرورية (مثل الوصـول عن بُعد) أو تشديد أمن النظام.

تدابير الأمن الحاسوبي

2-15- تُستخدم تدابير الأمن الحاسوبي لمنع الأعمال الشـريرة واكتشـافها وتعطيلها والتصــدي لها وكذلك للتخفيف من عواقب هذه الأعمال. كما تُســتخدم هذه التدابير

10 يحدَّد في الأساس التصميمي للمفردات ذات الأهمية للأمان القدرات والموثوقية والوظائف اللازمة للحالات التشغيلية ذات الصلة، وذلك فيما يخص الظروف المفضية إلى وقوع حوادث والظروف التي تنشأ من المخاطر الداخلية والخارجية، بهدف تلبية بمعايير القبول المحددة على مدى عمر المرفق النووي. ويرد تعريف الأساس التصميمي بمزيد من التفصيل في مسرد مصطلحات الأمان الصادر عن الوكالة [7]. ويرد وصف الأساس التصميمي لنظم الأجهزة والتحكم بمزيد من التفصيل في القسم 3 من المرجع [4].

لضـــمان أن الأعمال غير الشـــريرة لا تؤدي إلى تدهور الأمن وزيادة تعرض النظم القائمة على الحاسوب للأعمال الشريرة.

2-16- ويمكن تعيين تدابير الأمن الحاســوبي التي تعالج الثغرات الأمنية في النظام أو التي توفِّر طبقات حماية دفاعية إلى واحدة من ثلاث فئات: تدابير التحكم التقني أو تدابير التحكم المادي أو تدابير التحكم الإداري. وينبغي النظر في جميع الفئات الثلاث واختيار مجموعة مناســبة عند تطوير الأمن الحاســوبي المتكامل لنظم الأجهزة والتحكم.

2-17- وتدابير التحكم التقني هي أجهزة و/أو برامج حاســوبية تســتخدم لمنع أي تسلل أو أي عمل شرير آخر واكتشافه وتخفيف عواقبه والتعافي منه. وينبغي النظر في قدرة تدابير التحكم التقني على توفير إجراءات وقائية مســتمرة وتلقائية عند تقييم فعاليتها مقارنة بتدابير التحكم المادي أو الإداري.

2-18- وتدابير التحكم المادي هي حواجز مادية تحمي الأجهزة والنظم القائمة على الحاسوب والأصول الداعمة من الضرر المادي والوصول المادي غير المأذون به. وتشــمل تدابير التحكم المادي الأقفال والأغلفة المادية وأجهزة اكتشــاف التلاعب وغرف العزل والبوابات والحرَّاس.

2-19- وتدابير التحكم الإداري هي السياسات والإجراءات والممارسات المصممة لحماية النظم القائمة على الحاسوب من خلال توفير تعليمات بشأن الإجراءات التي ينبغي للموظفين وموظفي الطرف الثالث اتباعها. وتحدِّد تدابير التحكم الإداري الإجراءات المســموح بها والضــرورية والمحظورة بالنســبة للموظفين وموظفي الطرف الثالث. وتشمل تدابير التحكم الإداري للمرافق النووية تدابير التحكم التشغيلي والإداري.

تطبيق نهج متدرج

2-20- يجب على المشـغِّل فرض متطلبات الأمن الحاسـوبي بناءً على نهج متدرج قائم على العلم بالمخاطر يأخذ في الاعتبار ما يلي:

- أهمية وظائف نظام الأجهزة والتحكم لكل من الأمان (أي تصنيف الأمان) والأمن؛
- التهديدات التي جرى تحديدها وتقييمها فيما يخص المرفق؛
- جاذبية نظام الأجهزة والتحكم للخصوم المحتملين؛
- الثغرات الأمنية في نظام الأجهزة والتحكم؛
- بيئة التشغيل؛
- العواقب المحتملة التي يمكن أن تنجم بشكل مباشر أو غير مباشر عن المساس بالنظام.

ويمكن أن يستند هذا النهج إلى نتائج تقييم مخاطر الأمن الحاسوبي.

2-21- وفي النهج المتدرج، تحدَّد متطلبات الأمن الحاسوبي بشكل متناسب مع العواقب المحتملة للهجوم. وتُرتَّب العواقب المحتملة لاختراق وظيفة نظام الأجهزة والتحكم من الحالات الأسوأ إلى الحالات الأفضل:

- الوظيفة غير محدَّدة. تؤدي تأثيرات الاختراق إلى تغيير غير ملحوظ في تصميم النظام أو وظيفته.
- تعتري الوظيفة سلوكيات أو إجراءات غير متوقعة يمكن للمشغِّل ملاحظتها.
- تعطُّل الوظيفة.
- تعمل الوظيفة كما هو متوقع، مما يعني أن الاختراق لا يؤثر سلباً على وظيفة النظام (أي أنها تتحمل الأعطال).

2-22- ويجب تطبيق مستويات الأمن الحاسوبي كما هو موضح في هذا المنشور على نظم الأجهزة والتحكم للسماح بتنفيذ نهج متدرج للأمن الحاسوبي.

2-23- ويرد مثال على تنفيذ نهج متدرج باستخدام مستويات الأمن[11] في المرجع [3]. وفي المقابل، يرد مثال على تنفيذ نهج متدرج للأمان في المرجع [9].

11 طوال هذا المنشور، الإشارة إلى "مستويات الأمن" و"نطاقات الأمن" تعني مستويات الأمن الحاسوبي ونطاقات الأمن الحاسوبي.

مستويات الأمن الحاسوبي

2-24- مستويات الأمن الحاسوبي وفئات الأمان هي مفاهيم متمايزة ولكنها ذات صلة. ويعتمد تصنيف الأمان لأحد المفردات المهمة للأمان على أهمية وظيفته بالإضافة إلى العواقب المحتملة عند تعطُّله.

2-25- ويُعيَّن مستوى الأمن الحاسوبي لكل وظيفة من وظائف نظام الأجهزة والتحكم المرتبطة بالمرفق بشكل عام للإشارة إلى درجة حماية الأمن الحاسوبي التي تحتاجها. وسيحتاج كل مستوى إلى مجموعات مختلفة من تدابير الأمن الحاسوبي لتلبية متطلبات الأمن الحاسوبي ذات الصلة. وغالباً ما تُحدَّد مستويات الأمان بناءً على الأهداف الأمنية للمنظمة. ويوفِّر المرجع [10] مزيداً من المعلومات حول تنفيذ المستويات ونطاقات الأمن.

2-26- وتُحدَّد النظم الفرعية ومكونات نظم الأجهزة والتحكم التي يمكن أن يؤثر سوء تشغيلها على الأمان النووي (بما في ذلك التخفيف من الحوادث) والأمن النووي وحصر المواد النووية ومراقبتها، وتُعيَّن إلى مستويات الأمن وفقاً لمساهمتها في وظيفة نظام الأجهزة والتحكم.

2-27- ويعين المشغِّل مستوى الأمن لنظام الأجهزة والتحكم أو لنظام فرعي تابع له أو لأحد مكوناته بناءً على العواقب المحتملة لتعطُّله أو سوء تشغيله، بما في ذلك سوء التشغيل بطريقة تختلف عن تصميمه أو أنماط الأعطال التي يمكن تصورها وتلك التي ستُحدَّد عند تحليل أمان المرفق. ويتمتع مستوى الأمن الحاسوبي المعيَّن لنظام الأجهزة والتحكم أو لنظام فرعي تابع له أو لأحد مكوناته بالاقتصار على نفسه والاستقلال عن بيئته.

نطاقات الأمن الحاسوبي

2-28- يتضمن مفهوم نطاق الأمن التجميعَ المنطقي و/أو المادي للنظم القائمة على الحاسوب التي تشترك في متطلبات عامة للأمن الحاسوبي، بسبب الخصائص المتأصلة للنظم أو اتصالاتها بالنظم الأخرى. وجميع النظم الموجودة في نطاق واحد محمية بنفس مستوى الأمان، أي المستوى المعيَّن لوظيفة نظام الأجهزة والتحكم ذات

أعلى مستوى من الصرامة للأمن في هذا النطاق. وقد يؤدي تجميع نظم الأجهزة والتحكم في نطاقات أمنية إلى تبسيط تطبيق وإدارة تدابير الأمن الحاسوبي.

2-29- وينبغي أن تستوفي اعتبارات تنفيذ نطاقات الأمن المعايير التالية:

- النظم التي تنتمي إلى نفس النطاق تتشابه في احتياجات تدابير الأمن الحاسوبي.
- تشكل النظم التي تنتمي إلى نفس النطاق منطقة موثوقة للاتصالات الداخلية بين تلك النظم (أي نطاق منطقة داخلية موثوقة).
- يضم كل نطاق نظماً لها نفس الأهمية أو أهمية مماثلة لأمن وأمان المرفق، أو تنتمي إلى منطقة نطاق داخلية موثوق بها.
- تُراعى متطلبات هيكل أمان النظام (مثل الاستحاطة والتنوع والفصل الجغرافي والكهربائي ومعيار العطل الفردي).
- تنفَّذ تدابير التحكم التقنية على حدود النطاقات لتقييد تدفق البيانات والاتصال بين النظم الموجودة داخل نطاقات مختلفة (مثل الموقع البعيد) أو المعيَّنة لمستويات أمنية مختلفة.
- تُستخدم الوسائط القابلة للإزالة والأجهزة المحمولة وغيرها من المعدات المؤقتة التي تحتاج إلى وصول إلكتروني أو مادي إلى نظام ما فقط داخل نطاق واحد أو مجموعة محدَّدة من النطاقات.
- يمكن تقسيم النطاقات إلى نطاقات فرعية لتحسين النسق.

2-30- وعند استخدام نطاقات الأمن في أحد المرافق، يمكن تعيين بعض نظم أو مكونات الأجهزة والتحكم لنطاق قد عُيّن له مستوى أمن أكثر صرامة من مستوى الأمن المتأصل في هذه النظم أو المكونات. فعلى سبيل المثال، يمكن تعيين نفس مستوى الأمن لجهاز اتصال يؤدي فقط مستوى أدنى من وظائف تتعلق بالأمان أو الأمن مثل نظام حماية المفاعل، إذا كان هذا الجهاز موجوداً داخل نطاق الأمن الخاص بنظام حماية المفاعل. ويرجع هذا التعيين إلى احتمال الاستخدام الشرير للجهاز لتعريض مكونات نظام حماية المفاعل للاختراق، وهذه المكونات ذات أهمية كبيرة للأمان. وعلاوة على ذلك، فإن استخدام نطاق أمن نظام حماية المفاعل يسمح

بإنشاء نطاق داخلي موثوق به، مما يضمن عدم الحاجة إلى تنفيذ تدابير أمن حاسوبي إضافية بين مكونات نظام حماية المفاعل وجهاز الاتصال.

ثالثا- النهج القائم على العلم بالمخاطر على الأمن الحاسوبي لنظم الأجهزة والتحكم

3-1- لتحديد الثغرات الأمنية التي تعتري نظم الأجهزة والتحكم في المرفق والتي قد تستهدفها الهجمات السيبرانية وتحديد العواقب التي قد تنجم عن الاستغلال الناجح لهذه الثغرات، قد يستعين النهج القائم على العلم بالمخاطر على الأمن الحاسوبي في هذه النظم بتقييمات المخاطر. ويمكن بعد ذلك تعيين تدابير الأمن الحاسوبي بناءً على نتائج تقييمات المخاطر.

3-2- ونظراً لأن نظم الأجهزة والتحكم غالباً ما تكون ضرورية لأمان المرافق، فإن فهم الأمان النووي يمكن أن يساعد في تقييم المخاطر، ووضع تدابير الأمن الحاسوبي لنظام الأجهزة والتحكم، وتقييم أوجه التضارب المحتملة بين الأمان والأمن، والنظر في كيفية حلها. وعلى سبيل المثال، يمكن للخصوم تخريب مرفق من خلال هجوم سيبراني على نظم الأجهزة والتحكم في المرفق، مما يؤدي إلى عواقب محتملة على الأمان والأمن. وقد تتسبب هذه الهجمات في حدوث أعطال في نظم الأجهزة والتحكم أو قد تتسبب في عمل نظم الأجهزة والتحكم بطرق تختلف عن سلوكها المقصود أو أنماط الأعطال التي أظهرها تحليل هذه النظم. وقد تؤثر الأعمال الشريرة على نظام منفرد للأجهزة والتحكم أو على نظم متعددة للأجهزة والتحكم. وعلى سبيل المثال، يمكن للأفعال الشريرة أن تتخطى مستويات متعددة من الدفاع عن الأمان في العمق أو تتسبب في إحداث عطل متزامن على هذه المستويات[12]. وقد تجمع الأعمال الشريرة أيضاً بين الهجمات السيبرانية وعناصر الهجوم المادي.

3-3- وقد يؤدي قصور الأمن الحاسوبي أو اختراق نظام الأجهزة والتحكم إلى تعريض أمان المرفق للخطر. فعلى سبيل المثال، إذا تعرَّض نظام الأجهزة والتحكم للاختراق، فقد يحصل الخصم على بيانات توفر المعلومات المهمة اللازمة للتخطيط

12 يرد في المرجع [7] شرح مفصَّل لمستويات الدفاع الخمسة للأمان النووي في العمق.

لهجوم أو تعديل البيانات التي تيسِّـر تخريب نظم المرافق أو سـحب المواد النووية دون إذن. ومن ناحية أخرى، قد يتسبب الهجوم السيبراني الذي يؤدي إلى التخريب في وقوع حادث أو تدهور أداء وظيفة الأمان. وقد يؤدي هذا الهجوم أيضاً إلى تعطُّل النظام.

3-4- وقد تؤدي الهجمات السيبرانية على نظم الأجهزة والتحكم أيضاً إلى عواقب تمكِّن من سـحب مواد نووية دون إذن من المرفق. وقد تتأثر نظم الأجهزة والتحكم التي تؤدي وظائف الحماية المادية أو حصـر المواد النووية ومراقبتها بالهجمات السيبرانية، مما قد يضع المرفق في حالة لم تُراعى في خطة أمن الموقع. ويمكن أن يجمع العمل الشرير أيضاً بين هجوم سيبراني على هذه النظم وعناصر هجوم مادي بهدف سحب مواد نووية دون إذن.

3-5- ولذلك، فإن تدابير الأمن الحاسوبي لنظم الأجهزة والتحكم تحتاج إلى معالجة كل من الهجمات السيبرانية التي تسبب التخريب مباشرة وتلك التي تجمع المعلومات التي يمكن أن تيسِّر تخريب المرفق النووي أو سحب مواد نووية منه دون إذن.

الترابط مع إدارة مخاطر الأمن الحاسوبي في المرفق

3-6- ينبغي أن يكون لدى مشـغِّل المرفق عملية لإدارة مخاطر الأمن الحاسـوبي من أجل تنفيذ الأمن الحاسـوبي لحماية الوظائف التي تؤديها نظم الأجهزة والتحكم. وتُستخدم هذه العملية لتحديد الثغرات الأمنية[13] الموجودة في المرفق التي قد يستهدفها الهجوم السيبراني وتحديد النتيجة المترتبة على النجاح في اختراق وظيفة أو أكثر من الوظائف التي تؤديها نظم الأجهزة والتحكم (والتي قد تشـمل اسـتغلال الثغرات الأمنية).

3-7- وينبغي أن تشمل نواتج عمليات إدارة مخاطر الأمن الحاسوبي في المرفق تحديد الوظائف التي تؤديها نظم الأجهزة والتحكم المرفق، بما في ذلك النظم الداعمة والتكميلية التي يمكن، حال اختراقها، أن تؤثر سلباً على أمان المواد النووية أو أمنها أو إدارة الحوادث. ويمكن استخدام تحليل أمان المرفق كأحد المدخلات لإدارة مخاطر

13 يرد في مسرد مصطلحات الأمان [7] التسلسل الهرمي والتعاريف المتعلقة بالحالات التي تكون عليها المحطة ما لم يذكر خلاف ذلك.

الأمن الحاسوبي في المرفق، ولكن لا يكفي تحليل الأمان وحده لأنه لا يتناول جميع أنماط سوء التشغيل. وقد تؤدي أنماط سوء التشغيل الناجمة عن الهجمات السيبرانية إلى وضع المرفق في ظروف لم يُنظر فيها خلال تحليل الأمان.

3-8- وينبغي أن تحدِّد نواتج عمليات إدارة مخاطر الأمن الحاسوبي في المرافق العواقبَ المحتملة المتعلقة بالأمان النووي والأمن النووي وحصر المواد النووية ومراقبتها نتيجة لاختراق النظام بسبب هجوم سيبراني على نظم الأجهزة والتحكم. وعند تحليل عواقب الهجوم على نظام الأجهزة والتحكم، ينبغي النظر في احتمال أن يكون الهجوم مكوناً من هجوم أكبر يؤثر على نظم متعددة للأجهزة والتحكم أو هجوم سيبراني ومادي معاً. ويمكن بعد ذلك استخدام هذا التحليل لتعيين مستويات الأمان المناسبة لنظم ومكونات الأجهزة والتحكم الفردية بناءً على العواقب المحتملة لتعطلها أو سوء تشغيلها.

3-9- وقد ترتبط مستويات الأمان المعيَّنة لنظم الأجهزة والتحكم بقائمة تسلسل هرمي من العواقب المحتملة على الأمان أو الأمن. فعلى سبيل المثال، يمكن استخدام الحالات التي تكون عليها المحطة، أو عواقب التخريب، أو التسلسل الهرمي لتصنيف المواد النووية أو توليفة من هذه العناصر، كما هو الحال في الأمثلة الواردة في الفقرات من 3-10 إلى 3-13 و3-15.

3-10- ولأسباب تتعلق بالأمان، يمكن استخدام الحالات التي تكون عليها المحطة للدلالة على عواقب الأمان المحتملة للهجوم السيبراني على نظم الأجهزة والتحكم. وعلى سبيل المثال، يمكن ربط الحالات التي تكون عليها المحطة بمستويات الأمان لنظم الأجهزة والتحكم على النحو التالي، مرتبة من الحالات التي يترتب عليها أقل العواقب إلى الحالات التي يترتب عليها أكبر العواقب:

(1) التشغيل العادي: لا يمكن أن يتسبب الهجوم السيبراني على نظم الأجهزة والتحكم في تشغيل المرفق خارج الحدود والظروف المحددة للتشغيل العادي.

(2) واقعة تشغيلية متوقعة: قد يتسبب الهجوم السيبراني على نظم الأجهزة والتحكم في انحراف حالة المحطة عن مسار التشغيل العادي بطريقة متوقع

حدوثها، ولكن في ضوء أحكام التصميم المناسبة لا يتسبب هذا الهجوم في إلحاق أي ضرر كبير بالعناصر المهمة للأمان أو يؤدي إلى وقوع حادث.

(3) حادث محتاط له في التصميم[14]: قد يتسبب الهجوم السيبراني على نظم الأجهزة والتحكم في وقوع حادث يكون محتاطاً له في أساس تصميم المرفق ويكون الضرر الذي يلحق بسببه بالمواد النووية (أو المواد المشعة الأخرى) وانبعاث المواد المشعة ضمن الحدود المأذون بها.

(4) ظروف تمديد التصميم: قد يتسبب الهجوم السيبراني على نظم الأجهزة والتحكم في حوادث لم تُراعى في الحوادث المحتاط لها في الأساس التصميمي، ولكن تُراعى في عملية تصميم المرفق وفقاً لمنهجية أفضل التقديرات، بحيث يجري الإبقاء على انبعاثات المواد المشعة ضمن الحدود المقبولة. ويمكن أن تتضمن ظروف تمديد التصميم ظروف الحوادث الشديدة.

3-11- ويمكن أيضاً ربط عواقب تخريب الوظائف التي تؤديها نظم الأجهزة والتحكم بمستويات الأمن. ومن شأن هذا النهج أن ينطوي على قيام الدولة بتحديد عتبة العواقب الإشعاعية غير المقبولة، على النحو الموصى به في الفقرة 3-44 من المرجع [2]. ويمكن أن يستند تعريف عتبة العواقب الإشعاعية غير المقبولة إلى معايير كمية أو نوعية، يمكن التعبير عنها من حيث انبعاثات النويدات المشعة (مثل الانبعاث الذي يتجاوز قدراً من الكمية المحددة)، أو الجرعات (مثل الانبعاث الذي يؤدي إلى جرعة إشعاعية تتجاوز قدراً من القيمة المحددة لفرد موجود في نقطة محددة، عادة خارج الموقع) أو ظروف المرفق (مثل التخريب الذي قد يسفر عن أضرار كبيرة في قلب المفاعل). وكما هو مذكور في الفقرتين 3-94 و3-95 في المرجع [11]:

"إن الأهداف التي يمكن أن يؤدي تخريبها إلى انبعاث إشعاعي كبير يؤثر تأثيراً كبيراً على السكان والبيئة خارج حدود المرفق النووي تحتاج إلى

14 التسلسل الهرمي والنص المصاحب للحادث المحتاط له في التصميم وظروف تمديد التصميم مستمدة من المرجع [7].

أعلى مستوى من الحماية. ويشار إلى مثل هذا الحدث العنيف ... [في المرجع [2]] بأن له عواقب إشعاعية شديدة.

"ولذلك، ينبغي للدولة أيضاً أن تحدد عتبة العواقب الإشعاعية الشديدة".

3-12- ويُضرب مثال على قائمة هرمية للعواقب المحتملة للتخريب في المرجع [11] ويرد فيما يلي تلخيص لها فيما يخص وظائف نظام الأجهزة والتحكم، مرتبة من أدنى مستويات العواقب إلى أعلى مستويات العواقب:

— العواقب الإشعاعية دون عتبة العواقب الإشعاعية غير المقبولة: تحتاج الأهداف التي تنشأ منها هذه العواقب المنخفضة إلى مستوى منخفض من الحماية في المقابل.
— يمكن تصنيف العواقب الإشعاعية غير المقبولة إلى ثلاث فئات مرتبة من أدنى مستويات العواقب إلى أعلى مستويات العواقب:

- مستوى العواقب جيم: التخريب الذي يمكن أن يؤدي إلى تعريض الأشخاص في الموقع إلى جرعات تستدعي اتخاذ إجراءات وقائية عاجلة لتقليل الآثار الصحية في الموقع.
- مستوى العواقب باء: التخريب الذي يمكن أن يؤدي إلى جرعات أو تلوُّث خارج الموقع يستدعي اتخاذ إجراءات وقائية عاجلة لتقليل الآثار الصحية خارج الموقع (يمكن النظر إليه أيضاً على أنه من العواقب الإشعاعية الشديدة).
- مستوى العواقب ألف: التخريب الذي يمكن أن يؤدي إلى آثار صحية حتمية شديدة خارج الموقع (من المحتمل أيضاً النظر إليه على أنه من العواقب الإشعاعية الشديدة).

3-13- ويمكن أيضاً ربط مستويات الأمن بإمكانية سحب مواد نووية دون إذن. ويمكن ربط العواقب المحتملة للهجمات السيبرانية على نظم الأجهزة والتحكم التي تؤدي وظائف الحماية المادية أو حصر المواد النووية ومراقبتها بمستويات الأمن على أساس فئة المواد التي يمكن أن تخضع للسحب دون إذن. ويقدِّم الجدول الأول

من المرجع [2] معايير تصنيف المواد النووية ويحدِّد كذلك توصيات للحماية المادية استناداً إلى هذا التصنيف.

3-14- ولا يوجد حاليًّا توافق دولي في الآراء بشأن نموذج لتسلسل هرمي متكامل تماماً لجميع عواقب الأمان والأمن الناشئة عن الحوادث والأحداث المتصلة بالأمن النووي الناتجة عن الهجمات السيبرانية. ومع ذلك، ينبغي للمشغِّل أو الدولة أن تضع هذا التسلسل الهرمي على المستوى الوطني.

3-15- ويمكن أيضاً مراعاة العواقب الأخرى، مثل فقدان السمعة، عند تقييم العواقب المجمَّعة للهجوم السيبراني على نظم الأجهزة والتحكم في المرفق. ويمكن الاطلاع على قائمة بالعواقب المحتملة في المرجع [12].

3-16- وتتغير باستمرار تكتيكات وتقنيات الخصوم، وينبغي للمرافق النووية أن تعزز ثقافة الأمن النووي التي تستعرض باستمرار مخاطر الأمن الحاسوبي وتتيح المرونة لبرنامج الأمن الحاسوبي في المرفق. ويرد شرح لثقافة الأمن النووي بمزيد من التفصيل في المرجع [13].

3-17- ويجب تحليل تكوين النظام والأنشطة المرتبطة بنظم الأجهزة والتحكم المعزَّزة بالمعدات الرقمية لتحديد التغييرات في المسارات المنطقية والمادية التي يمكن أن توفر فرصاً يمكن للخصم استغلالها. وتشمل هذه الأنشطة المرتبطة بنظم الأجهزة والتحكم أنشطة الصيانة المؤقتة، وعمليات الشراء، ودعم البائعين، والاتصال بالأجهزة الميدانية، والتحديثات اليدوية للبرامج.

3-18- وإدارة مخاطر الأمن الحاسوبي في المرفق عملية تكرارية ودورية يمكن أن تشمل إجراء تحليل أولي، وتحديد التهديدات وتقييمها، وتحديد مستويات الأمن، واستعراض دوري وتحليل مستكمل. ويجب أن تكون هناك عملية قبول محددة لاستعراض نتائج التحليلات الجديدة أو المستكملة والتحقق منها.

3-19- وبالنسبة للمرافق الجديدة، يجب تنفيذ إدارة مخاطر الأمن الحاسوبي في المرفق كجزء من عملية التصميم وقبولها قبل الانتهاء من المرحلة الأولية للإدخال في الخدمة.

3-20- وبالنسبة للمرافق القائمة، قد تتضمن المدخلات المضافة إلى الطريقة الجديدة أو المستكملة لإدارة مخاطر الأمن الحاسوبي في المرفق تحليل الأمان وتفاصيل الأمان وهيكل العمليات والمخرجات المقبولة سابقاً من طريقة إدارة مخاطر الأمن الحاسوبي في المرفق.

الترابط مع إدارة مخاطر الأمن الحاسوبي في النظم

3-21- يجب أن تستخدم إدارة مخاطر الأمن الحاسوبي في النظام مخرجات إدارة مخاطر الأمن الحاسوبي في المرفق (إن وجِدت) ووثائق الأساس التصميمي لنظم الأجهزة والتحكم كمدخلات لتحديد المخاطر الأمنية التي تشكلها الهجمات السيبرانية على نظم الأجهزة والتحكم الفردية أو المتعددة أو النظم الفرعية أو المكونات التابعة لها. ويجب تحليل وتوثيق مخاطر الأمن الحاسوبي التي جرى تقييمها في نظم الأجهزة والتحكم.

3-22- ويجب على المشغِّل تعيين الأدوار والمسؤوليات طوال دورة حياة نظام الأجهزة والتحكم لتقييم وإدارة مخاطر الأمن الحاسوبي في نظام الأجهزة والتحكم. ويحتاج الأمن الحاسوبي إلى أن تبذل المنظمات والفرق المتعددة التخصصات جهوداً مركَّزة. فعلى سبيل المثال، يجوز للمشغِّل أن ينشئ أفرقة عاملة مسؤولة عن إدارة عمليات وأنشطة الأمن الحاسوبي فضلاً عن الحصول على الأذون.

3-23- ويجب على المشغِّل الاحتفاظ بقائمة جرد لنظام الأجهزة والتحكم، بما في ذلك البرامج والنظم الفرعية والمكونات التابعة لها، تخضع للتحديث والصيانة طوال دورة حياة النظام. ويجب على المشغِّل استخدام قائمة الجرد هذه عند تنفيذ إدارة مخاطر الأمن الحاسوبي في النظام.

3-24- ويجب تقييم مكونات نظام الأجهزة والتحكم وتعيين مستوى الأمان المناسب بناءً على إدارة مخاطر الأمن الحاسوبي في النظام. وبالنسبة لهذه المكونات، يجب تحديد عواقب الأمان والأمن التي يمكن أن تنجم عن سوء التشغيل أو الاختراق. وإذا نُفِّذت نطاقات أمنية داخل المرفق، ينبغي تعيين نطاق الأمن وتحديده.

3-25- وعند تنفيذ إدارة مخاطر الأمن الحاسوبي في النظام، يجب على المشغِّل النظر في إمكانية حدوث هجوم سيبراني في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم. وينبغي للمشغِّل أيضاً أن يأخذ في الاعتبار عند التقييم أن الهجمات السيبرانية قد تؤثر على نظام فردي أو نظم متعددة ويمكن استخدامها بالاقتران مع أشكال أخرى من الأعمال الشريرة التي تسبب أضراراً مادية. ويجب أيضاً مراعاة الأعمال الشريرة التي يمكن أن تغيّر إشارات العملية أو بيانات تكوين المعدات أو البرامج في إدارة مخاطر الأمن الحاسوبي في النظام.

3-26- وبالإضافة إلى ذلك، يجب أن تراعي عملية إدارة مخاطر الأمن الحاسوبي في النظام جميع توجُّهات الهجوم التي يمكن استخدامها لإدخال تعليمات برمجية أو بيانات شريرة في نظام الأجهزة والتحكم. وعلى سبيل المثال، يمكن إدخال التعليمات البرمجية الشريرة في نظام الأجهزة والتحكم عبر وصلات الاتصالات أو المنتجات والخدمات المورَّدة أو الأجهزة المحمولة المتصلة مؤقتاً بالمعدات المستهدفة.

3-27- وينبغي أن تحدِّد عملية إدارة مخاطر الأمن الحاسوبي في النظام احتمال حدوث كل عاقبة من العواقب المحتملة المرتبطة بنظام الأجهزة والتحكم، باستخدام العناصر التالية كمدخلات: توافر توجُّهات هجوم محدَّدة يمكن استخدامها لإدخال تعليمات برمجية أو بيانات شريرة في نظام الأجهزة والتحكم؛ وتطبيق وفعالية تدابير الأمن الحاسوبي؛ وقدرات التهديد؛ وغيرها من المعلومات ذات الصلة.

3-28- وإدارة مخاطر الأمن الحاسوبي في النظام عملية تكرارية ودورية، على غرار إدارة مخاطر الأمن الحاسوبي في المرفق، تتضمن تحليلاً أوليًّا وتنفيذ تدابير الأمن الحاسوبي والاستعراض الدوري والتحليل المستكمل. ويجب النظر في استعراض إدارة مخاطر الأمن الحاسوبي في النظام عند حدوث أحد الأمور التالية:

- تنقيح عملية إدارة مخاطر الأمن الحاسوبي في المرفق أو تحليل أمان المرفق.
- إجراء تعديلات على النظام.
- وقوع أحداث أو حوادث أمنية ذات صلة.
- تحديد تهديدات أو ثغرات أمنية جديدة أو متغيرة.

3-29- ويجب أن تحدِّد عملية إدارة مخاطر الأمن الحاسوبي في النظام الأعمال أو الإغفالات البشرية التي قد تؤثر على الأمان.

تعيين تدابير الأمن الحاسوبي

3-30- تنطبق الإرشادات الواردة في الفقرات 3-31 إلى 3-34 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات التابعة لها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لكل منها.

3-31- ويجب تعيين مستوى أمن لكل نظام من نظم الأجهزة والتحكم أو نظام فرعي أو مكون تابع له وفقاً للعواقب المحتملة لتعطُّله أو سوء تشغيله فيما يخص كل من الأمان والأمن.

3-32- ويجب تحديد تطبيق تدابير الأمن الحاسوبي على كل نظام من نظم الأجهزة والتحكم من خلال مستوى الأمن المعيَّن له أو مستوى الأمن للنطاق الأمني الموجود فيه، أيهما أكثر صرامة.

3-33- ويجب تحديد متطلبات الأمن الحاسوبي وتعريفها في كل مستوى من مستويات الأمن. وينبغي تقييم فعالية التدابير التي تنفذ هذه المتطلبات لضمان توفير الحماية الكافية لنظم الأجهزة والتحكم المعيَّنة في كل مستوى من مستويات الأمن.

3-34- وإذا لم تكن تدابير الأمن الحاسوبي قادرة على توفير حماية كافية لنظم الأجهزة والتحكم في كل مستوى من مستويات الأمن، فينبغي النظر في اتخاذ تدابير إضافية أو بديلة، مثل سمات الحماية المادية على مستوى المرفق، أو الوظائف الإلكترونية المستقلة، أو إعادة تصميم النظام، أو التدابير الإدارية التي تزيل مواطن ضعف محددة أو تقلل من عواقب سوء التشغيل.

أوجه الترابط بين الأمان والأمن

3-35- كما هو مذكور في الفقرة 1-2 في المرجع [8]،

"للأمن النووي والأمان النووي هدفٌ مشـتركٌ، ألا وهو حماية الأشـخاص والممتلكات والمجتمع والبيئة. وينبغي تصـميم وتنفيذ التدابير في مجالي الأمن والأمان بطريقة متكاملة تكفل التآزر بين هذين المجالين، وبحيث لا تُخلُّ تدابير الأمن بالأمان ولا تُخلُّ تدابير الأمان بالأمن".

ويمكن الاطلاع على مزيد من الإرشـادات حول اعتبارات الأمان في نظم الأجهزة والتحكم في المرجعين [4، و6].

3-36- وستعتمد ملاءمة تدبير معين للأمن الحاسوبي على اعتبارات الأمان والأمن والتشـغيل. وهناك حاجة إلى الحصـول على مدخلات من موظفي الأمان والأمن وعمليات التشـغيل لتعيين تدابير الأمن الحاسـوبي لنظم الأجهزة والتحكم. ولا يمكن لتدابير الأمن الحاسـوبي أن توجد بمعزل عن الشـواغل المتصـلة بالأمان، ولا يمكن لسـمات الأمان أن توجد بمعزل عن الشـواغل المتصـلة بالأمن. فعلى سـبيل المثال، ولأسـباب تتعلق بالأمان، قد يلزم تنفيذ بعض وظائف الأمن (مثل جمع سـجلات المراجعة أو توليد الإنذارات الأمنية) في نظم منفصـلة يمكنها رصـد نظام الأجهزة والتحكم دون أن تؤثر سلباً على قدرة النظام على أداء وظائفه الأساسية. ومن ناحية أخرى، فإن أداء عمليات الفحص الأمني النشـطة فقط عندما لا تكون نظم الأجهزة والتحكم قيد الخدمة يمكن أن يحقق الأهداف الأمنية مع الحد من التأثير على النظم العاملة.

3-37- ويمكن لتدابير الأمن الحاسوبي غير الملائمة من ناحية التصميم أن تتسبب في أنماط محتملة للأعطال في النظام، وتزيد من احتمال التشـغيل الزائف وتعرقل قدرة النظام على أداء وظيفة الأمان على نحو موثوق. وعلى سـبيل المثال، يمكن أن يؤدي التنفيذ المصـمم بشـكل غير ملائم لنظام الكشـف عن البرامج الخبيثة أو الفيروسـات داخل نظام الأجهزة والتحكم إلى زيادة تعقيد نظام الأجهزة والتحكم، وزيادة كُمون نظام الأجهزة والتحكم وأن يصـبح نظام الأجهزة والتحكم عرضـة للاستغلال. ومع ذلك، يمكن أن تتحسن قدرة هذا النظام على أداء وظيفة الأمان بشكل موثوق مع توفير فوائد أمنية كبيرة عند إجراء عملية تحكم تقني مصممة بشكل ملائم تضـمن السماح فقط بتشـغيل البرامج المتحقَّق منها ومن صـحتها على نظام الأجهزة والتحكم .

3-38- وقد يكون للعديد من الوظائف المصممة في نظم الأجهزة والتحكم لأسباب تتعلق بالأمان فوائد أمنية أيضاً. ومن الأمثلة على ذلك عملية التحقق من صحة البيانات المستلمة وصحتها وسلامتها قبل استخدامها في وظيفة نظام الأجهزة والتحكم.

3-39- وقد تكون هناك حالات لا يمكن فيها تنفيذ تدبير الأمن الحاسوبي وفقاً لمستوى الأمن المعيَّن لنظام الأجهزة والتحكم، على سبيل المثال، بسبب أوجه التعارض مع وظائف الأمان الأساسية، ولكن يجب تحليل هذه الاستثناءات وتبريرها بدقة.

3-40- ويجب أن تعمل المجموعة الكاملة من تدابير الأمن الحاسوبي لنظام الأجهزة والتحكم معاً وتمنع (أو لا تتسبب في) نقطة أعطال واحدة.

3-41- وقد يكون لاستراتيجية الأمان القدرة على التأثير سلباً على الأمن. وعلى سبيل المثال، ففي كثير من الأحوال ينطوي التصميم لأغراض الأمان على تخصيص وظائف لنظم فرعية (أو معالجات) مختلفة من أجل عزل آثار الأعطال، وعلى مراعاة الوفرة الاحتياطية والتنوع في النظم بحيث لا تؤدي فرادى الأعطال إلى الإخلال بوظائف مهمة. وتؤدي هذه الاستراتيجيات إلى زيادة عدد النظم الفرعية في نظم الأجهزة والتحكم، مما يؤدي بدوره إلى زيادة عدد النقاط التي يستهدفها الهجوم السيبراني. ولذلك، ينبغي اتخاذ تدابير للحد من خطر أن يؤدي الهجوم السيبراني إلى فقدان تنوع النظام أو وفرته الاحتياطية. ويجب ألا تؤدي تدابير الأمن الحاسوبي إلى ظهور ثغرات أمنية جديدة قد تؤدي إلى أعطال راجعة لأسباب شائعة في هذه النظم ذات الوفرة الاحتياطية والتنوع.

اعتبارات الأمان في تدابير الأمن الحاسوبي

3-42- تنطبق الإرشـــادات الواردة في الفقرات 3-43 إلى 3-52 على جميع نظم الأجهزة والتحكم المهمة للأمان.

3-43- ويجب ألا يؤثر تنفيذ تدابير الأمن الحاســـوبي ســـلباً على وظائف الأمان الأساسية وأداء نظام الأجهزة والتحكم.

3-44- ولا ينبغي أن يؤثر التشغيل العادي أو الشاذ لأي إجراء أمني حاسوبي سلباً على قدرة نظام الأجهزة والتحكم على أداء وظيفة الأمان.

3-45- ويجب على المشـــغِّل تحديد وتوثيق والنظر في تحليلات مخاطر النظام في أنماط أعطال تدابير الأمن الحاسوبي وكيف ستؤثر أنماط الأعطال على وظائف نظام الأجهزة والتحكم.

3-46- ويجب ألا تؤثر تدابير الأمن الحاســـوبي التي تحمي الواجهة البينية بين الإنسان والنظام سلباً على قدرة المشغِّل على الحفاظ على أمان المرفق. ويجب على المشغِّل أيضاً النظر في الآثار الضارة مثل اعتراض وتعديل بيانات العملية المرسلة إلى الواجهة البينية بين الإنسان والنظام (مثل الانتحال) بهدف منع أو تأخير المشغِّل عن تشغيل وظيفة الأمان (مثل إيقاف العملية يدويًّا).

3-47- ويجب تنفيذ تدابير الأمن الحاســـوبي التي لا يمكن دمجها عمليًّا في نظام الأجهزة والتحكم بشكل منفصل عن نظام الأجهزة والتحكم. وقد يكون من الضروري اتخاذ مزيد من تدابير التحكم إدارية لاستخدام هذه الأجهزة المنفصلة وصيانتها.

3-48- ويجب تطوير تدابير الأمن الحاســـوبي المدمجة في نظم الأجهزة والتحكم وفقاً لإرشـــادات نظم الإدارة الواردة في المرجع [14] أو نظام إدارة بديل مكافئ ومؤهل لنفس مستوى النظام الذي توجد فيه تدابير الأمن الحاسوبي.

3-49- وإذا كان هناك تعارض بين الأمان والأمن، فيجب الحفاظ على اعتبارات التصـــميم المتخذة لضـــمان الأمان بشـــرط أن يبحث المشـــغِّل عن حل متوافق لتلبية متطلبات الأمن الحاســـوبي. ويجب تنفيذ تدابير الأمن الحاســـوبي التعويضـــية لتقليل المخاطر إلى مستوى مقبول ودعمها بتبرير شـامل وتحليل للمخاطر الأمنية. وينبغي ألا تعتمد التدابير المنفَّذة على تدابير التحكم الإداري فقط لفترة طويلة. ولا ينبغي أبداً قبول عدم وجود حل أمني.

3-50- ويجب أن يحدد المشغِّل بوضوح المسؤولية الرئيسية عن تصميم واختيار وتنفيذ تدابير الأمن الحاسوبي، ولكن يجب أن يتعاون في هذا العمل الموظفون المسؤولون عن الأنشطة التي تنطوي على تصميم نظام الأجهزة والتحكم وصيانته وأمانه وأمنه.

3-51- ويجب أن يوضح تحليل تصميم نظام الأجهزة والتحكم أن تدابير الأمن الحاسوبي المدمجة في نظام الأجهزة والتحكم وتلك التي يتم تنفيذها كأجهزة منفصلة لن تؤثر سلباً على وظائف الأمان المعتمدة في النظم والمكونات المهمة للأمان.

3-52- ويجب ألا تؤثر صيانة تدابير الأمن الحاسوبي سلباً على توافر نظم الأجهزة والتحكم.

رابعا- الأمن الحاسوبي في دورة حياة نظام الأجهزة والتحكم

4-1- ينبغي إدارة تصـــميم نظم الأجهزة والتحكم للمرافق النووية من خلال نظام الإدارة المتكامل[15] في المرفق لضـــمان مراعاة جميع متطلبات الأمن الحاســـوبي وتنفيذها في جميع مراحل دورة حياة نظام الأجهزة والتحكم، وتلبية متطلبات الأمن الحاسوبي هذه في التصميم النهائي. ويحدِّد المرجع [14] متطلبات الأمان العامة لنظم إدارة المرافق النووية. وبالإضافة إلى ذلك، تشير الفقرة الفرعية 3-12(أ) في المرجع [8] إلى أهمية نظم الإدارة المتكاملة للأمن النووي. ويوفر المرجع [3] مزيداً من النقاش بشأن العلاقة الشاملة بين نظم الإدارة والأمن الحاسوبي.

4-2- وتنصّ الفقرة 2-13 من المرجع [4] على ما يلي:

"في نظم الأجهزة والتحكم الرقمية، يعتمد إثبات أن المنتج النهائي مناسب لغرضه بشكل كبير، ولكن ليس حصريًّا، على استخدام عملية تطوير عالية الجودة توفر مواصفات منضبطة وتنفيذ متطلبات التصميم".

وتضيف الفقرة 2-14 ما يلي:

"في مجال القوى النووية وكذلك في المجالات الأخرى ذات الأهمية الحاســـمة للأمان مثل الفضـــاء الجوي، طُبِّقت عمليات تطوير تمثِّل عادة كنماذج لدورة الحياة، وهي تصـــف أنشـــطة تطوير النظم الإلكترونية والعلاقات بين هذه الأنشطة. ... وعادة ما توضع الأنشطة المتعلقة بخطوة تطويرية معينة ضمن مجموعة واحدة في نفس المرحلة من دورة الحياة".

ويجب مراعاة الأمن الحاسوبي في جميع مراحل دورة حياة نظام الأجهزة والتحكم.

15 وفقاً للمرجع [7]، فإن نظام الإدارة هو "مجموعة عناصر مترابطة أو متفاعلة فيما بينها (نظام) لوضع السياسات والأهداف وللتمكين من تحقيق الأهداف بطريقة تتسم بالكفاءة والفعالية". وفي هذا المنشور، يشمل ذلك الهيكل التنظيمي والثقافة التنظيمية والسياسات والعمليات، بما في ذلك تلك المتعلقة بتحديد وتخصيص الموارد (مثل الموظفين والمعدات والبنية الأساسية وبيئة العمل) لتطوير نظم الأجهزة والتحكم.

4-3- وكما هو مذكور في الفقرة 1-17 في المرجع [4]،

"هناك حاجة إلى ثلاثة مستويات أساسية لدورات الحياة لوصف تطوير نظم الأجهزة والتحكم:

- دورة حياة شاملة لهيكل الأجهزة والتحكم؛ [16]
- دورة حياة واحدة أو أكثر من دورات حياة نظام الأجهزة والتحكم الفردية؛
- دورة حياة مكون فردي واحد أو أكثر: عادة ما تُدار دورات حياة المكونات في إطار تطوير المنصة وبشكل مستقل عن مستوى الهيكل العام ودورات حياة فرادى مستويات النظام. وتنقسم دورات حياة مكونات النظم الرقمية عادة إلى دورات حياة منفصلة لتطوير الأجهزة والبرامج".

4-4- وبشكل عام يُحدَّد مطورو النظام ومشغِّلوه تعريف نماذج دورة الحياة والأنشطة المجمعة في كل مرحلة من مراحل دورة الحياة بشكل عام، ولكن يجب أن يكون العمل على التعريف والتنفيذ جهداً متعدد التخصصات يشمل العديد من المجالات الأخرى، بما في ذلك الأمن الحاسوبي. وبشكل عام، يتحمل المطورون المسؤولية الرئيسية عن نظم الأجهزة والتحكم حتى تُنقل إلى المنظمة التي ستعمل بها لتركيبها وتحقيق تكاملها وتشغيلها.

4-5- وبالنظر إلى أن نظم الأجهزة والتحكم لدورة الحياة يمكن أن تمتد لعدة عقود، فقد تؤدي المنظمات المختلفة دور المطورين أو الأدوار الأخرى خلال دورة حياة النظام. وعلى سبيل المثال، من الشائع أن يتولى البائع التطوير الأصلي وأن يتولى المشتري تطوير التعديلات في وقت لاحق، خاصة إذا كانت التعديلات طفيفة. ومسألة أن هذه التعديلات طورتها منظمات مختلفة لا تستبعد الحاجة إلى تنفيذ تدابير الأمن الحاسوبي في جميع مراحل دورة حياة نظام الأجهزة والتحكم.

16 كما هو محدَّد في الفقرة 3-10 في المرجع [4]، "هيكل الأجهزة والتحكم الشاملة هو الهيكل التنظيمي لنظم الأجهزة والتحكم في المحطة".

4-6- ويجب في أقرب فرصة تخطيط الأمن الحاسوبي بشكل متماسك لجميع دورات حياة هيكل الأجهزة والتحكم والنظام والمكونات. ويجب أن يحدِّد هذا التخطيط تدابير الأمن الحاسوبي التي سيجري تطبيقها في كل مرحلة لحماية هيكل الأجهزة والتحكم ونظمها ومكوناتها من الهجمات السيبرانية التي قد تعرض الوظائف المهمة للأمان للخطر. وينبغي النظر في إمكانية تغيير وظائف الأمان أو تدابير الأمن الحاسوبي خلال مراحل لاحقة.

4-7- ويجب أن تسعى عملية تطوير نظام الأجهزة والتحكم إلى تقليل الثغرات الأمنية ومواطن الضعف المحتملة في الأمن الحاسوبي وتحديد الثغرات الأمنية ومواطن الضعف المحتملة المتبقية في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم.

4-8- وبينما يمكن تنظيم نماذج دورة الحياة بعدة طرق، تُستخدم مراحل دورة الحياة الافتراضية التالية في هذا المنشور كإطار لوصف اعتبارات الأمن الحاسوبي خلال دورة حياة الأجهزة والتحكم:

- تخطيط العملية؛
- الأساس التصميمي؛
- الهيكل الشامل للأجهزة والتحكم وتخصيص الوظائف؛
- مواصفات متطلبات نظام الأجهزة والتحكم؛
- اختيار المفردات المطوَّرة مسبقاً؛
- التصميم والتنفيذ بالتفصيل؛
- تكامل النظام؛
- اعتماد النظام؛
- التركيب والتكامل والتشغيل؛
- التشغيل والصيانة؛
- التعديل؛
- الإخراج من الخدمة.

4-9- وبالإضـــافة إلى هذه المراحل، تتضـــمن دورة حياة نظام الأجهزة والتحكم أيضـاً العديد من الأنشطة المشتركة في جميع مراحل دورة الحياة. والأنشطة الشائعة المهمة للأمن الحاسوبي هي كما يلي:

- توكيد الجودة؛
- إدارة نسق المكونات؛
- التحقق والاعتماد[17]؛
- تقييم الأمن؛
- التوثيق.

4-10- وينبغي أن تكون متطلبات وأنشـــطة الأمن الحاســـوبي في كل مرحلة من مراحل دورة الحياة متناســبة مع العواقب الناجمة عن الوصـــول غير المأذون به أو غير المناسب إلى نظام الأجهزة والتحكم أو استخدامه أو الكشف عنه أو التلاعب به أو تعطيله أو تدميره. وينبغي أيضـاً إيلاء الاعتبار لاختراق أي نظام أو نظام دعم أو معلومات قد تؤثر سلباً على الأمان أو الأمن.

4-11- وينقسـم الجزء المتبقي من هذا القسـم إلى أقسـام فرعية تناقش الإرشـادات العامة للأمن الحاســـوبي التي تنطبق على جميع مراحل دورة الحياة، وإرشـــادات الأمان الخاصـة بمراحل دورة الحياة الفردية. وفي هذه المناقشـة، تُناقش المراحل مرة واحدة فقط ولكن يجب تطبيق الإرشادات على أي دورة حياة تحدث فيها المرحلة.

الإرشادات العامة للأمن الحاسوبي

4-12- تحدد ســياســة الأمن الحاســوبي في المرفق النووي الأهداف العامة للأمن الحاســوبي في المرفق. وفيما يتعلق بتخطيط الأمن الحاســوبي في المرافق والنظام، تُحدَّد هذه الأهداف في الســياســة بمصــطلحات واضــحة ومحددة، وقابلة للقياس إن

17 يعرّف مسرد مصطلحات الأمان الصادر عن الوكالة [7] كلاً من التحقق والاعتماد. التحقق من النظام الحاسوبي هو "عملية التأكد من أن مرحلة في دورة حياة *النظام* تفي بالمتطلبات التي تفرضها عليها المرحلة السابقة". واعتماد النظام الحاسوبي هو "*عملية* اختبار وتقييم *النظام* الحاسوبي المتكامل (الأجهزة والبرامج) لضمان الامتثال لمتطلبات الوظائف والأداء والترابط".

أمكن. وتُترجم أهداف المرفق إلى أهداف النظام. ويوفِّر المرجع [3] مزيداً من الإرشادات بشأن الأمن الحاسوبي في المرافق النووية.

4-13- ويجب أن تتضمن سياسة الأمن الحاسوبي عناصر تتناول أمن نظم الأجهزة والتحكم، وبالتالي، يجب أن تنطبق السياسة على أي منظمة مسؤولة عن الأنشطة في دورة حياة نظام الأجهزة والتحكم. وتشمل هذه المنظمات المشغِّلين والبائعين والمتعاقدين والمورّدين الذين يتولون تصميم وتنفيذ وشراء نظم الأجهزة والتحكم والبرامج والمكونات.

4-14- ويجب على كل منظمة مسؤولة عن أنشطة دورة حياة الأجهزة والتحكم تحديد وتوثيق المعايير والإجراءات التي تتوافق مع سياسات الأمان المعمول بها لضمان تقليل الأجهزة والبرامج والبرامج الثابتة إلى الحد الأدنى من التعليمات البرمجية غير الموثقة (مثل تشفير الباب الخلفي) والتعليمات البرمجية الشريرة (مثل التدخلات والفيروسات والديدان وأحصنة طروادة والقنابل المنطقية) وغيرها من الوظائف أو التطبيقات غير المرغوب فيها أو غير الضرورية أو غير الموثَّقة، بهدف تقليل عدد المسارات المحتملة التي يمكن من خلالها حدوث هجوم سيبراني.

4-15- ويجب أن تتناول سياسة الأمن الحاسوبي والبرنامج والمعايير المرتبطة به والإجراءات المعمول بها كل مرحلة فردية من دورة حياة نظام الأجهزة والتحكم لحماية نظم الأجهزة والتحكم في المرفق من الاختراق.

4-16- ويجب أن تفي سياسات وبرامج ومعايير وإجراءات الأمن الحاسوبي وكذلك جميع تدابير الأمن الحاسوبي بالمتطلبات الرقابية ومتطلبات الأمن الحاسوبي.

4-17- وقد تُوفَّر سياسات ومعايير وإجراءات الأمن الحاسوبي في برنامج أمن الأجهزة والتحكم في المنظمة أو قد تُدمج في خطط دورة حياة نظام الأجهزة والتحكم. وفي الممارسة العملية، غالباً ما يُتبَّع نهج مختلط.

جوانب سياسة الأمن الحاسوبي المتعلقة بنظم الأجهزة والتحكم

4-18- ينبغي أن تصف سياسة الأمن الحاسوبي في المرافق النووية تطبيق نهج متدرج لتنفيذ تدابير الأمن الحاسوبي لنظم الأجهزة والتحكم. ويجب تطبيق النهج المتدرج وفقاً لأهمية الأمان والأمن لكل وظيفة من وظائف نظام الأجهزة والتحكم (على سبيل المثال وفقاً لمستوى الأمن المعيَّن في كل نظام). ويجب على الإدارة وضع وإنفاذ أهداف واضحة لسياسة الأمن الحاسوبي بما يتفق مع الأهداف العامة لأمان وأمن المرافق، ومعالجة أمن نظم الأجهزة والتحكم على وجه التحديد. ويرد في المرجع [3] مزيد من التفاصيل عن الاعتبارات العامة المتعلقة بسياسة وبرنامج الأمن الحاسوبي.

4-19- ويجب أن تتضمن سياسة الأمن الحاسوبي اعتبارات مهمة لنظم الأجهزة والتحكم، مثل:

- التحكم في الوصول، بما في ذلك التحكم في الوصول المادي والمنطقي، واستخدام مبدأ أقل الامتيازات.
- التكوين وإدارة الأصول، بما في ذلك إدارة كلمات المرور، وإدارة التصحيح، واستخدام النظام، وتحصين النظام، والتحكم في التكوين، والقيود المفروضة على استخدام الأجهزة المحمولة والوسائط القابلة للإزالة، والأجهزة والشبكات اللاسلكية والوصول عن بُعد؛
- أنشطة التحقق من سلامة النظام والمكونات؛
- عمليات الشراء؛
- إدارة المخاطر والتهديدات، بما في ذلك عمليات جمع وتحليل وتوثيق وتبادل المعلومات مع الجهات الأخرى التي تحتاج إلى معرفة المعلومات المتعلقة بالثغرات الأمنية ومواطن الضعف والتهديدات والتصرف بناءً عليها)؛
- التصدي للحوادث والتعافي منها؛
- المراجعة والتقييمات.

4-20- ويجب أن تعيّن سياسة الأمن الحاسوبي الأدوار والمسؤوليات للمنظمات أو الأفراد الذين يؤدون أنشطة دورة حياة نظام الأجهزة والتحكم.

برنامج الأمن الحاسوبي

4-21- يجب على كل منظمة مسؤولة عن تنفيذ أنشطة دورة حياة نظام الأجهزة والتحكم تطوير وتنفيذ برنامج متكامل أو منفصل للأمن الحاسوبي يتناول نظم الأجهزة والتحكم.

4-22- ويجب أن يحدد برنامج الأمن الحاسوبي الأدوار والمسؤوليات لكل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم في كل نظام من نظم الأجهزة والتحكم.

4-23- ويجب أن يحدد برنامج الأمن الحاسوبي أن المنظمات المسؤولة تطبق مفهوم الدفاع في العمق، وأن يحدد تدابير الأمن الحاسوبي المطبقة على نظم الأجهزة والتحكم وفقاً لمستوى الأمن المعيَّن لها.

4-24- وينبغي أن يحدد برنامج الأمن الحاسوبي تنفيذ تدابير الأمن الحاسوبي الرامية إلى الحماية من الأعمال الشريرة التي يرتكبها أشخاص داخليون والتلاعب بنظام المعلومات والاتصالات (بما في ذلك سلامته) في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم.

4-25- ويجب أن يحدد برنامج الأمن الحاسوبي أن الوصول إلى نظم الأجهزة والتحكم ومكوناتها وبرامجها وبيانات التكوين وأدواتها يخضع للتحكم خلال جميع مراحل دورة حياة نظام الأجهزة والتحكم. ومن الأمثلة على ممارسات التحكم في الوصول هي مبدأ أقل الامتيازات والحاجة إلى المعرفة.

4-26- وينبغي أن يتناول برنامج الأمن الحاسوبي سرية تدابير الأمن الحاسوبي، بما في ذلك حماية الوثائق ذات الصلة، بما يتسق مع مستوى أمن نظم الأجهزة والتحكم المشار إليها في الوثائق.

4-27- وينبغي أن يعالج برنامج الأمن الحاسوبي الثغرات الأمنية ومواطن الضعف المحتملة في الأمن الحاسوبي في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم.

4-28- ويجب أن يحدد برنامج الأمن الحاسوبي العملية التي يتم من خلالها تصنيف معلومات أمن نظام الأجهزة والتحكم، مثل التفاصيل المتعلقة بالثغرات الأمنية الموجودة في نظم الأجهزة والتحكم في المرفق أو وسائل الدفاع المحددة المستخدمة لحماية النظم، على أنها معلومات حساسة ومجزأة[18]. ويعرّف المرجع [8] المعلومات الحساسة بأنها "المعلومات، بأي شكل من الأشكال، بما في ذلك البرامج الحاسوبية، التي يمكن أن يؤدي إفشاؤها أو تعديلها أو تبديلها أو إتلافها أو رفض استخدامها دون إذن إلى تقويض الأمن النووي".

4-29- وتُشجَّع المرافق النووية والمنظمات المرتبطة بها بقوة على تبادل المعلومات الأخرى غير الحساسة عن الثغرات الأمنية حتى تكون المرافق مستعدة بشكل أفضل في حالة توزيع المعلومات المتعلقة بالثغرات الأمنية في نظم الأجهزة والتحكم وتبادلها فيما بين الخصوم المحتملين. وترد في المرجع [15] إرشادات بشأن أمن المعلومات النووية (بما في ذلك التصنيف).

4-30- وينبغي أن يحدد برنامج الأمن الحاسوبي لنظم الأجهزة والتحكم إجراء استعراضات وتقييمات دورية للأمن الحاسوبي وتوثيقها في كل مرحلة من مراحل دورة الحياة.

4-31- وينبغي أن يحدد برنامج الأمن الحاسوبي تدابير الأمن الحاسوبي التي توفر بيئة آمنة يمكن أن تُجرى فيها أنشطة التطوير.

4-32- وبالنسبة لنظم الأجهزة والتحكم القديمة، قد يكون هناك اعتماد أكبر على تدابير التحكم الإداري والعزل أكثر من النظم المعاصرة. وينبغي لبرنامج الأمن

18 التجزئة تعني تقسيم المعلومات إلى أجزاء تخضع للتحكم المنفصل لمنع الأشخاص الداخليين من جمع جميع المعلومات اللازمة لمحاولة القيام بعمل شرير.

الحاسـوبي أن يحدد ويدعم مزيداً من التدابير الأمنية التعويضـية للأمن الحاسـوبي اللازمة لضمان الأمن الحاسوبي لنظم الأجهزة والتحكم القديمة.

البيئة الآمنة للتطوير

4-33- تنطبق الإرشـادات الواردة في الفقرات 4-34 إلى 4-40 على تطوير جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات التي يطبق عليها نهج متدرج للأمن الحاسوبي وفقاً لمستوى الأمن المعيَّن لها.

4-34- ويجب تطوير نظام الأجهزة والتحكم في بيئة تطوير آمنة. وينطبق هذا على كل من المواقع الداخلية والخارجية. ويجب أن يُراعى عند تعيين مسـتوى الأمن في هذه البيئة مسـتوى أمن النظام في البيئة المسـتهدفة، ومسـتوى أمن النظم الأخرى المطوَّرة أو المخزَّنة داخل بيئة التطوير المشـتركة وأدوات التطوير. ويجب تقييم تدابير الأمن الحاسـوبي في هذه البيئة لضـمان التوافق مع متطلبات مسـتوى الأمن المعيَّن.

4-35- وينبغي أن تتضـمن بيئة التطوير الآمنة تدابير للتحكم الإداري، مثل التحكم في التكوين وإدارة الأصول.

4-36- وينبغي اسـتخدام تدابير التحكم المادية للتحكم في الوصـول إلى بيئات تطويرية آمنة.

4-37- ويجب التحقق من معدات الاختبار والدعم المسـتخدمة في بيئات تطوير الأجهزة والتحكم للتأكد من أن استخدام هذه المعدات لا يتيح مسارات لإدخال تعليمات برمجية أو بيانات شريرة في بيئة التطوير الآمنة.

4-38- ويجب وضع تدابير الأمن الحاسوبي للتحكم في حركة البيانات والأجهزة في جميع مراحل التطوير لضمان عدم إدخال التعليمات البرمجية أو البيانات الشريرة في بيئات التطوير الآمنة ولحماية المعلومات الحساسة المرتبطة بنظم الأجهزة والتحكم. ويجب أن تتضـمن تدابير الأمن الحاسـوبي تدابير التحكم الإدارية والتقنية مثل قيود الاسـتخدام وإجراءات التحكم في الوسـائط القابلة للإزالة والأجهزة المحمولة. ويجب

الاعتراف ببيئة التطوير الآمنة كبيئة متميزة منفصلة ماديًّا ومنطقيًّا عن بيئات الأعمال التشغيلية والشركات.

4-39- وينبغي تنفيذ تدابير الأمن الحاسوبي لحماية سلامة بيئة التطوير الآمنة وكذلك أمن مدخلات ونواتج التصميم (مثل البيانات وملفات التكوين وتحديثات البرامج وتصحيحات البرامج الحاسوبية) أثناء عمليات النقل التي تتم بين بيئة التطوير الآمنة والبيئة المستهدفة. ويمكن أن تشمل هذه التدابير نظم تكوين الأصول المؤتمتة التي أكد التحليل تمتعها بميزة أمنية للتطوير الآمن والبيئات المستهدفة.

4-40- ويجب اختبار أدوات الطرف الثالث أو البائع المُستخدمة لتطوير نظام الأجهزة والتحكم والتحقق منها وحمايتها بما يتناسب مع مستوى الأمن المعيَّن في بيئة التطوير.

خطط الطوارئ

4-41- ويجب على المنظمات التي تُنفِّذ نشاطاً أو أكثر من أنشطة دورة حياة نظام الأجهزة والتحكم إعداد خطط وإجراءات طوارئ لمنع تصاعد السلوك الشاذ وتفاقمه وللتعافي من الحوادث المتصلة بالأمن الحاسوبي. وينبغي استعراض خطط وإجراءات الطوارئ هذه وممارستها بصورة دورية وتحديثها عند اكتشاف أوجه قصور.

4-42- ويجب على المشغِّل وضع خطة تصدي للحوادث المتصلة بالأمن الحاسوبي تتكون من إجراءات تعرّف وتحدد وتتصدى للسلوك غير الطبيعي أو المشبوه المحتمل المكتشف في نظم الأجهزة والتحكم والنظم المرتبطة بها.

4-43- ويجب أن تتناول خطة التصدي للحوادث المتصلة بالأمن الحاسوبي جمع المعلومات والمتطلبات القانونية للحفاظ على الأدلة أثناء وقوع الأحداث المتصلة بالأمن لدعم التحليل الاستقصائي.

4-44- ويجب أن تعيّن خطة التصدي للحوادث المتصلة بالأمن الحاسوبي أفراد فريق التصدي المعني بالحوادث المتصلة بالأمن الحاسوبي في المرفق. ويجب أن

يكون هذا الفريق متاحاً في المرفق للتصدي لأي حادث متصل بالأمن الحاسوبي يجري تحديده. وقد يشمل الأفراد المعينون من لديهم خبرة خاصة في نظام الأجهزة والتحكم أو في مجال الأمن الحاسوبي.

4-45- ويجب أن تشتمل النسخ الاحتياطية ونسخ استعادة البيانات لنظام الأجهزة والتحكم ذات الأهمية لخطط وإجراءات الطوارئ على البرامج والبيانات الأساسية وملفات التكوين. ويجب تخزين هذه النسخ في مكان مادي منفصل عن المكان المصدر للحماية من الأعطال الراجعة لأسباب شائعة. ويجب استخدام تدابير الأمن الحاسوبي لحماية هذه النسخ من السرقة والعبث والحذف أو التدمير.

بائعو ومتعاقدو وموردو نظم الأجهزة والتحكم

4-46- في الفقرات 4-47 إلى 4-53، "البائعون" و"المتعاقدون" و"الموردون" هم من يضطلعون بتزويد المرفق النووي بمعدات وبرامج حاسوبية وخدمات رقمية لنظم الأجهزة والتحكم التي يُطبَّق عليها نهج متدرج للأمن الحاسوبي وفقاً لمستوى الأمن المعيَّن في النظام. وينبغي للمشغِّل أن يفرض تطبيق الإرشادات الواردة في الفقرات 4-47 إلى 4-53 من خلال إبرام العقود مع البائعين أو المتعاقدين أو الموردين المعنيين.

4-47- ويجب أن يكون لدى منظمات البائعين والبائعين من الباطن عمليات أمن حاسوبي قوية ويمكن التحقق منها.

4-48- ويجب على البائعين والمتعاقدين والموردين تلبية جميع متطلبات الأمن الحاسوبي المعمول بها. ويشمل ذلك تطبيق تدابير الأمن الحاسوبي التي يحددها المشغِّل، أثناء الدعم المقدم في الموقع أو في مكان عمل البائع أو المتعاقد أو المورد وأثناء أي نقل أو تخزين للبضائع المشتراة.

4-49- ويجب أن يكون لدى البائع أو المتعاقد أو المورد عملية لإدارة الأمن الحاسوبي.

4-50- وينبغي أن يحدد المشغِّل بشكل واضح وفي العقود متطلبات الأمن الحاسوبي المنطبقة في المواقع التي ينفِّذ فيها البائع أو المتعاقد أو المورد أنشطة في نظم الأجهزة والتحكم استناداً إلى مستوى الأمن المعين في النظام أو النظام الفرعي أو المكون.

4-51- وينبغي أن تكون هناك عملية لتمكين المشغِّل والبائع أو المتعاقد أو المورد من إبلاغ بعضهما بعضاً بالثغرات الأمنية وتنسيق جهود التصدي والتخفيف من حدة الأحداث.

4-52- وينبغي للبائع أو المتعاقد أو المورد أن يثبت أن لديه آلية موثوقة لتلقي التقارير عن الثغرات الأمنية وتقييمها وإبلاغ المرفق النووي بها طوال فترة خدمته التعاقدية. وقد يمتد هذا الاعتبار إلى ما بعد أي فترة ضمان عادية لدعم دورة حياة المعدات المُركَّبة. وفي هذه الحالات، ينبغي إدراج هذه الآلية للفترة الممتدة ضمن الالتزامات التعاقدية التي يوافق عليها البائعون أو المتعاقدون أو الموردون.

4-53- ويجب إجراء عمليات مراجعة وتقييم للبائعين أو المتعاقدين أو الموردين المسؤولين عن تصميم الأجهزة والتحكم وتطويرها وتكاملها وصيانتها وإبلاغ المشغِّل بالنتائج.

التدريب على الأمن الحاسوبي

4-54- يجب أن يتلقى جميع العاملين الذين يؤدون أعمالاً تتعلق بنظم الأجهزة والتحكم، بما في ذلك العمل الذي يتضمن معلومات حساسة مرتبطة بهذه النظم، تدريباً دوريًّا على الوعي بالأمن الحاسوبي وإجراءاته.

4-55- ويجب أن يكون جميع العاملين الذين لديهم وصول مادي أو منطقي إلى نظم الأجهزة والتحكم مؤهلين بما يتفق مع مسؤولياتهم المتعلقة بالأمن الحاسوبي ويجب أن يتلقوا تدريباً متخصصاً في مجال أمن نظم الأجهزة والتحكم بناءً على أدوارهم ومسؤولياتهم للحفاظ على تأهلهم.

4-56- ويجب تدريب جميع العاملين الذين لديهم وصـــول مادي أو منطقي إلى نظم الأجهزة والتحكم على مستوى الكفاءة المناسب لأدوارهم لدعم مهام الأمن الحاسوبي والتعرف على الحوادث المحتملة المتصـــلة بالأمن الحاســـوبي. ويمكن إبلاغ هؤلاء الأفراد بتـــأثير التغييرات المجراة على نظـــام الأجهزة والتحكم أو تـــدابير الأمن الحاسوبي المرتبطة به والتي يتمتعون بإمكانية الوصول إليها.

4-57- ويجب أن يتلقى العاملون المحدَّدون كأعضـــاء في فريق التصـــدي للحوادث المتصـــلة بالأمن الحاســـوبي تدريباً على تحديد الحوادث المتصـــلة بالأمن الحاســـوبي والتصـــدي لها. وقد ينطوي ذلك على اســـتخدام منصـــة اختبار نظم الأجهزة والتحكم كعنصر من عناصر برنامج التدريب على أمن نظم الأجهزة والتحكم.

4-58- ويجب تدريب موظفي أعمال الهندسة والعمليات والصيانة على الحفاظ على وظائف الأمان والأمن في نظم الأجهزة والتحكم.

4-59- وينبغي أن يتلقى موظفو تصـــميم الأجهزة والتحكم تدريباً على التصـــميم والبرمجة الآمنة لنظم الأجهزة والتحكم في المرافق النووية (مثل كيفية مراعاة الأمن في تصميم البرامج الحاسوبية).

العناصر المشتركة في جميع مراحل دورة الحياة

4-60- في معظم الحالات، توفر متطلبات الأمان في نظام الإدارة [14] والإرشادات العامة الواردة في أدلة الأمان ذات الصـــلة [16، و17] إرشـــادات كافية عن أنشـــطة نظام الإدارة المتعلقة بالأمن الحاســـوبي في جميع مراحل دورة حياة نظام الأجهزة والتحكم. ومع ذلك، هناك عدد قليل من المجالات التي تتطلب إرشادات أكثر تحديداً.

النظم الإدارية

4-61- تنطبق الإرشـــادات الواردة في الفقرات 4-62 إلى 4-70 على جميع المنظمات التي تضطلع بنشاط واحد أو أكثر من أنشطة دورة الحياة ذات الصلة بنظم الأجهزة والتحكم التي يطبق عليها نهج متدرج للأمن الحاسـوبي وفقاً لمسـتوى الأمن المعيَّن للنظام.

4-62- ويجب الرجوع إلى متطلبات الأمان الواردة في المرجع [14] من الرقم 6 إلى الرقم 8 بشـــأن نظم الإدارة، الفقرات 4-8 إلى 4-20، عند صـــياغة المتطلبات الرقابية و/أو متطلبات الأمن الحاسوبي المتعلقة بنظم الإدارة.

4-63- ويجب على كل منظمة مســـؤولة عن تطوير نظم أو مكونات الأجهزة والتحكم أو نشرها أو تشغيلها أو صيانتها أو تحديد تقادمها النظر في الأمن الحاسوبي لنظم الأجهزة والتحكم في نظام الإدارة المتكامل المُتَّبع في هذه المنظمة.

4-64- ويجب أن يدعم نظام الإدارة المتكامل للمرفق عمليات وإجراءات الأمن الحاسوبي.

4-65- وينبغي الاضطلاع بأنشطة دورة الحياة في إطار نظام إدارة يوفر ترتيبات كافية لأمن نظم الأجهزة والتحكم ومكوناتها.

4-66- ويجب وضـــع عمليات وإجراءات قابلة للمراجعة للتأكد من أن نظم الأجهزة والتحكم والنظم الفرعية والمكونات ذات الأهمية للحفاظ على الأمن الحاســـوبي تواصل أداء وظائفها الأمنية طوال فترة حياتها التشغيلية.

4-67- وينبغي اتخاذ الترتيبات اللازمة لإجراء فحوص أمنية لنظم الأجهزة والتحكم (مثل عمليات التفتيش لأغراض التكوين) طوال دورة حياة نظام الأجهزة والتحكم بأكملها لإثبات اتباع الإجراءات الأمنية وتحقيق معيار الحرفية المطلوب (على سبيل المثال، عدم إضافة مكونات إضافية).

4-68- ويجب إجراء عمليات تفتيش مســـتقلة[19] للتحقق من تنفيذ عمليات وإجراءات الأمن الحاسوبي كما هو موضح في خطة المشغِّل لتوكيد الجودة.

4-69- وينبغي إعداد وصون سجلات مفصَّلة عن أنشطة دورة الحياة بطريقة تسمح باستعراض هذه السجلات ومقارنتها بمتطلبات الأمن الحاسوبي في أي وقت. ويجب

19 "مستقلة" تعني أن التفتيش يجريه فرد أو منظمة مختلفة عن الطرف الخاضع للاستعراض.

أن تتضـمن هذه السـجلات جميع الحوادث المتصـلة بالأمن الحاسـوبي وإجراءات التصدي أو الإجراءات الاحترازية المتخذة بعد وقوع الحوادث.

4-70- ويجب أن يخضـع الأفراد المأذون لهم الذين يتمتعون بامتياز الوصـول المنطقي أو المادي إلى نظم الأجهزة والتحكم لتقييم الجدارة بالثقة والتدريب على الأمن الحاسـوبي والمراقبة السـلوكية بما يتفق مع برنامج التخفيف من التهديدات الداخلية في المرفق أو البرامج المماثلة له (انظر المرجع [5]).

استعراضات ومراجعات الأمن الحاسوبي

4-71- تنطبق الإرشـادات الواردة في الفقرات 4-72 إلى 4-77 على جميع المنظمات التي تضطلع بنشاط واحد أو أكثر من أنشطة دورة الحياة ذات الصلة بنظم الأجهزة والتحكم التي يطبق عليها نهج متدرج للأمن الحاسوبي وفقاً لمستوى الأمن المعيَّن لها.

4-72- وينبغي إجراء استعراضات ومراجعات للأمن الحاسوبي في نظم الأجهزة والتحكم والأنشـطة المرتبطة بها على أسـاس منتظم للتحقق من الامتثال للوائح وسياسة الأمن الحاسوبي والممارسات الجيدة لأمن نظم الأجهزة والتحكم.

4-73- ويجب أن تكون استعراضات الأمن الحاسوبي لنظم الأجهزة والتحكم مستقلة وأن يجريها مراجعون مؤهلون من الداخل و/أو الخارج.

4-74- وينبغي تحديد وتوثيق السـياسـات والإجراءات، بما في ذلك الأدوار والمسؤوليات المتعلقة بإجراء هذه الاستعراضات.

4-75- ويجب أن تتحقق استعراضات الأمن الحاسوبي في نظم الأجهزة والتحكم من تنفيذ وفعالية تدابير الأمن الحاسوبي المرتبطة بهذه النظم.

4-76- ولا ينبغي إجراء اختبار التقييم الاقتحامي على نظم الأجهزة والتحكم العاملة. ويتضمن اختبار التقييم الاقتحامي محاولة استغلال ثغرة أمنية (على سبيل المثال كما هو الحال في اختبار الاختراق) قد تغير إما ظروف التشـغيل أو تكوين نظام الأجهزة والتحكم خارج أساسه التصميمي. وينبغي للمشغِّل أن ينظر في استخدام

أســـاليب خاضـــعة للتحكم من أجل إجراء اختبارات خالية من التحميل عندما يكون المرفق في حالة لا تكون العواقب الإشـــعاعية غير المقبولة مفعَّلة فيها؛ على ســـبيل المثال، إذا كان المرفق في حالة إغلاق أو حالة إفراغ من الوقود. ويجب أن تتناول ســـياســـات وإجراءات المرفق إجراء وأداء هذه الاختبارات. ويجب تصـــميم هذه الاختبارات خصيصاً لكل نظام. ويجب أن يشارك فريق التصدي المعني بالحوادث المتصلة بالأمن الحاسوبي في اختبارات التقييم الاقتحامية.

4-77- ويجب أرشـفة سـجلات اسـتعراضـات الأمن الحاسـوبي وبيانات التحليل المرتبطـة بهـا والاحتفـاظ بهـا وحمـايتهـا طوال دورة حيـاة نظـام الأجهزة والتحكم بأكملها.

إدارة تكوين الأمن الحاسوبي

4-78- تنطبق الإرشـــادات الواردة في الفقرات 4-79 إلى 4-87 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-79- وقد تسـاعد أنشـطة التحكم في تكوين البرامج الحاسـوبية في منع الحوادث المتصلة بالأمن الحاسوبي وكشفها، رغم أن الغرض الأساسي من هذه الأنشطة ليس معالجة أهداف محددة للأمن النووي. وينبغي تحليل الفوائد المتحققة للأمن الحاسـوبي من أداء هذه الأنشـطة وتأكيدها قبل نسـب هذه الفوائد إلى تلك الأنشـطة. فعلى سـبيل المثال، يمكن الكشـف عن حادث متصـل بالأمن الحاسـوبي من خلال هذه الأنشـطة، ولكن من المرجح أن يكون توقيت بدء التصـــدي لحادث مكتشـــف غير كافٍ لحماية النظام، مقارنة بتوقيت التصدي في نظام أمن حاسوبي يتضـمن تدابير أمن حاسـوبي متعددة الطبقات مقترنة بعناصر تصدي تلقائية.

4-80- والتغييرات غير المدارة في تكوين البرامج مصدر مهم لحدوث ثغرات أمنية جديدة ومواقف غير متوقعة. وعادة ما يكون نظام إدارة التكوين المســـتخدم في نظم الأجهزة والتحكم نظاماً عاماً يدير أيضـــاً العديد من أنواع النظم الأخرى. ومع ذلك، ينبغي اســـتخدام نظام إدارة التكوين بطريقة تتضـــمن المعرفة بكل من نظم الأجهزة والتحكم وتدابير الأمن الحاسوبي الخاصة بها.

4-81- وتعتمد إدارة التكوين على إدارة التغيير، وهي عملية تسعى إلى ضمان استخدام عمليات التصميم المعتمدة والتحقق والاعتماد المناسبين عند تغيير نظام حاسوبي. وتشمل هذه الإدارة أيضاً التحكم في الوثائق التي تدعم هذه العمليات. وتنص الفقرة 5-26 من المنشور المعنون "تطبيق نظام إدارة المرافق والأنشطة"، العدد GS-G-3.1 من سلسلة معايير الأمان الصادرة عن الوكالة الدولية للطاقة الذرية [16]، على ما يلي:

"ينبغي أن تشمل أنواع الوثائق التي يتعين التحكم فيها، على سبيل المثال لا الحصر، الوثائق التي تعرّف نظام الإدارة؛ ومتطلبات الأمان؛ وتعليمات العمل؛ وتقارير التقييم؛ والرسومات؛ وملفات البيانات؛ والمواصفات؛ والشفرات الحاسوبية؛ وأوامر الشراء والوثائق ذات الصلة؛ ووثائق الموردين".

4-82- ويجب أن تكون تدابير الأمن الحاسوبي لنظم الأجهزة والتحكم التي تستخدم عملية إدارة تكوين المرفق متسقة مع متطلبات التحكم في تكوين المرفق المطبقة على نظام الأجهزة والتحكم ذي الصلة.

4-83- ويجب ضمان توافر إدارة تكوين تدابير الأمن الحاسوبي المرتبطة بنظم الأجهزة والتحكم طوال دورة حياة نظم الأجهزة والتحكم.

4-84- ويجب أن تتضمن إدارة تكوين تدابير الأمن الحاسوبي المرتبطة بنظم الأجهزة والتحكم تقنيات وإجراءات لتحليل آثار التغييرات الطارئة على التكوين، والموافقة على إدخال تغييرات على التكوين، وضمان دمج إصدارات البرامج الحاسوبية بشكل صحيح، وإصدار وثائق التصميم والبرامج الحاسوبية للاستخدام، وإنشاء وصون سجل زمني للتغييرات الطارئة على التكوين (على سبيل المثال، إصدارات أدوات البرامج الحاسوبية المستخدمة في نقطة معينة من التصميم).

4-85- وينبغي حماية تحديد مكونات الأجهزة والتحكم وتخزينها وإصدارها واستخدامها وما يرتبط بها من تدابير التحكم التقني من الاختراق.

4-86- ويجب الحفاظ على وثائق تكوين تدابير الأمن الحاسوبي المرتبطة بنظم الأجهزة والتحكم وحمايتها من الوصول غير المأذون به أو الاختراق. ويجب تصنيف هذه المعلومات على أنها معلومات حساسة ويجب أن يقتصر الوصول إليها على أساس الحاجة إلى المعرفة.

4-87- ويجب تطبيق تدابير التحكم التقني للحد من الوصول وضمان السلامة على البرامج وملفات التكوين أثناء التطوير والنقل والتركيب والتشغيل.

التحقق والاعتماد

4-88- تنطبق الإرشادات الواردة في الفقرات 4-89 إلى 4-94 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-89- وتستخدم كل مرحلة من مراحل عملية تطوير نظام الأجهزة والتحكم معلومات من المراحل السابقة وتوفر نتائج لاستخدامها كمدخلات للمراحل اللاحقة. ويجب إجراء عملية التحقق بعد الانتهاء من كل مرحلة من مراحل عملية التطوير وقبل الانتقال إلى المرحلة التالية من عملية التطوير ويجب أن تشمل عملية التحقق تقييم تدابير الأمن الحاسوبي.

4-90- وقبل استكمال مرحلة البدء في عملية تطوير نظام الأجهزة والتحكم، يجب إجراء عملية اعتماد نظام الأجهزة والتحكم بهدف ضمان تلبية متطلبات الأمن الحاسوبي مع الاستمرار أيضاً في الامتثال للمتطلبات الوظيفية ومتطلبات الأداء والترابط. والغرض من ذلك هو توفير درجة عالية من التأكيد على أن النظام سيؤدي وظيفته على النحو المطلوب. ويجب أن تتولى أفرقةٌ أو أفراد أو مجموعات مستقلة عن المصممين والمطورين عمليةَ اعتماد تدابير الأمن الحاسوبي . وعلى سبيل المثال، ينبغي أن يتناسب الاعتماد المستقل ودرجة استقلاليته مع مستوى الأمن المعيَّن للنظام أو المكوّن المعني، سواء تولى عملية الاعتماد موظفون تابعون للبائعين أو المتعاقدين أو الموردين أو خبراء خارجيون مستقلون عن هذه الأطراف الثلاثة.

4-91- ويجب أن تثبت أنشطة التحقق والاعتماد أن نظام الأجهزة والتحكم يفي بمتطلبات الأمن الحاسوبي ذات الصلة.

4-92- ويجب على المشغِّل التحقق من كل إجراء تحكم تقني واعتماده للتأكد من أنه يوفر لنظام الأجهزة والتحكم الحماية المرجوة ولا يقلل من موثوقية وظائف الأمان أو الأمن في هذا النظام.

4-93- ويجب التحقق من تدابير الأمن الحاسوبي واعتمادها ببذل جهد متناسب مع مستوى الأمن المعيَّن لنظام الأجهزة والتحكم ذي الصلة أو ببذل جهد متناسب مع تصنيف أمان نظام الأجهزة والتحكم، أيهما كان أكثر صرامة.

4-94- وينبغي أن تحدد أنشطة التحقق والاعتماد الثغرات الأمنية أو مواطن الضعف أو غيرها من الحالات الشاذة المكتشفة وتسجلها وتوثقها وأن تحدد كيفية حلها. ونظراً لحجم وتعقيد معظم النظم الحاسوبية الحديثة، قد يكون من الصعب ضمان أن تكون نتائج هذه الأنشطة شاملة أو ناجحة في الكشف عن جميع الحالات الشاذة. فعلى سبيل المثال، تعتمد الأدوات المؤتمتة لإجراء استعراضات الثغرات الحاسوبية على المنصة ولغة البرمجة المستخدمة، وقد لا تنجح إلا بشكل جزئي فقط. وبالإضافة إلى ذلك، قد لا يكون من الممكن فحص بعض نظم التشغيل ورمز الجهاز ووظائف المكتبة القابلة للاستدعاء، والتي قد تحتوي على ثغرات أمنية يمكن استغلالها.

تقييمات الأمن الحاسوبي

4-95- تنطبق الإرشادات الواردة في الفقرات 4-96 إلى 4-100 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-96- ويجب إجراء تقييمات الأمن الحاسوبي في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم لتحديد التهديدات المحتملة وكذلك الثغرات الأمنية ومواطن الضعف.

4-97- ويجب رصد المعلومات العامة أو المفتوحة المصدر وكذلك البائعين أو المتعاقدين أو الموردين ومصادر الخبراء لتحديد التغييرات الطارئة على مظاهر التهديدات والثغرات الأمنية الجديدة على الفور.

4-98- ويجب تقييم التهديدات والثغرات الأمنية الجديدة أو المتغيرة لتقييم تأثيرها المحتمل على الأمن الحاسوبي في نظام الأجهزة والتحكم. ويجب اتخاذ إجراءات تصحيحية (مثل السمات الأمنية المعدَّلة) إذا كانت هذه التغييرات يمكن أن تؤدي إلى انتهاكات أمنية محتملة أو مخاطر غير مقبولة على المرفق.

4-99- ويجب على كل منظمة مسؤولة عن تطوير أو نشر أو تشغيل أو صيانة أو إيقاف تشغيل نظم أو مكونات الأجهزة والتحكم إجراء تقييمات ومراجعات دورية للأمن الحاسوبي.

4-100 ويجب استخدام نتائج تقييمات الأمن الحاسوبي لتحديث إدارة مخاطر الأمن الحاسوبي في النظام.

التوثيق

4-101-تنطبق الإرشادات الواردة في الفقرات 4-102 إلى 4-106 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-102-ويساعد توثيق الأمن الحاسوبي في نظام الأجهزة والتحكم على تجنب الالتباس ويسهِّل التشغيل السليم والخالي من الأخطاء للنظام ومراقبته واستكشاف الأخطاء الموجودة به وإصلاحها وصيانته وتعديله وتحديثه في المستقبل وتدريب موظفي المرافق والدعم التقني.

4-103-ويجب إعداد وثائق لتسجيل معلومات كافية تتعلق بالأمن الحاسوبي لنظم الأجهزة والتحكم لإثبات أن طريقة تصميم تدابير الأمن الحاسوبي وتنفيذها وصيانتها تلبي المستوى المطلوب من الحماية بما يتفق مع مستوى الأمن المعيَّن.

4-104-ويجب تحديد وثائق المدخلات والمخرجات المتعلقة بالأمن الحاسوبي في أنشطة كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم.

4-105-ويجب أن تضمن هذه الوثائق إمكانية تتبع متطلبات الأمن الحاسوبي عبر جميع أنشطة دورة حياة نظام الأجهزة والتحكم. ويجب تسجيل كل إضافة وتعديل وحذف يتم في تدابير الأمن الحاسوبي لنظم الأجهزة والتحكم.

4-106-ويجب حماية الوثائق من الكشف غير المأذون به والعبث والحذف والتدمير بما يتناسب مع مستوى الأمن المعيَّن في نظام الأجهزة والتحكم ذي الصلة.

الأساس التصميمي

4-107-تنطبق الإرشادات الواردة في الفقرات 4-108 إلى 4-114 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-108-وتنص الفقرة 3-11 في المرجع [4] على أن: "الأساس التصميمي يحدِّد الوظائف والشروط والمتطلبات المتعلقة بنظم الأجهزة والتحكم عموماً وبكل نظام فردي من هذه النظم". ثم تُستخدم هذه المعلومات لتعيين متطلبات الأمن الحاسوبي في كل نظام من نظم الأجهزة والتحكم وفي نظم الأمن الداعمة. كما يُستخدم الأساس التصميمي لوضع مواصفات تصميم تدابير الأمن الحاسوبي وتنفيذها وإعدادها واختبارها وأدائها.

4-109-ويجب استخدام الأساس التصميمي للهيكل الشامل للأجهزة والتحكم ولكل نظام من نظم الأجهزة والتحكم للاسترشاد به في تصميم تدابير الأمن الحاسوبي التي سيجري تنفيذها لتلبية متطلبات الأمن الحاسوبي الرقابية (بما في ذلك التهديدات المحتاط لها في التصميم أو تقييم التهديدات). ويرد في المرجع [18] مزيد من الإرشادات حول التهديدات المحتاط لها في التصميم (بما في ذلك تقييمات التهديدات وبيانات التهديدات البديلة).

4-110-ويجب أن تُحدَّد في الأساس التصميمي اعتبارات وافتراضات تصميم الأمن الحاسوبي لنظم الأجهزة والتحكم ونظم الأمن الداعمة.

4-111-ويجب أن يُحدَّد في الأساس التصميمي مستوى الحماية الذي سيُطبَّق على كل نظام من نظم الأجهزة والتحكم، بما يتفق مع مستوى الأمن المعيَّن المحدَّد في عملية إدارة مخاطر الأمن الحاسوبي في المرفق والنظام.

4-112-وينبغي أن يحدد الأساس التصميمي متطلبات تدابير الأمن الحاسوبي، بما في ذلك تدابير التحكم التقني والمادي والإداري.

4-113-وينبغي أن يحدد الأساس التصميمي متطلبات الأمان التي تسمح بأنشطة الاعتماد الفعالة، بهدف منع تدابير الأمن الحاسوبي من التأثير سلباً على أداء أمان نظم الأجهزة والتحكم.

4-114-ويجب الحفاظ على الأساس التصميمي وتحديثه بشكل دوري لإظهار التغييرات في المتطلبات الرقابية للأمن الحاسوبي أو المخاطر.

التحكم في الوصول

4-115-تنطبق الإرشادات الواردة في الفقرات 4-116-4-120 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات التي يطبق عليها نهج متدرج للأمن الحاسوبي وفقاً لمستوى الأمن المعيَّن لها.

4-116-ويجب التحكم في الوصول المادي والمنطقي إلى نظم الأجهزة والتحكم بهدف منع الوصول غير المأذون به. ويجب أن يخضع الوصول المميز إلى نظم الأجهزة والتحكم لرقابة صارمة بحيث لا يتمكن سوى الموظفين المأذون لهم من الوصول إلى التكوين والبرامج والأجهزة الحالية أو يمكنهم إجراء تغييرات عليها. قد يُقيَّد هذا الوصول وفقاً لوظيفة عمل الموظفين المأذون لهم، سواء من حيث المدة أو عدد النظم التي يمكنهم الوصول إليها.

4-117-ويجب تقليل عدد نقاط الوصول إلى الشبكات والأجهزة إلى أقل عدد ممكن لتقليل عدد توجُّهات الهجوم المحتملة.

4-118-ويجب أن يقتصر الاتصال الرقمي على الاستخدامات المأذون بها وأن يخضع للرصد بحثاً عن أي نشاط غير طبيعي. ويجب اتخاذ الإجراءات المناسبة عند اكتشاف نشاط غير طبيعي.

4-119-وبالنسبة لنظم الأجهزة والتحكم المعيَّن لها المستوى الأكثر صرامة من مستويات الأمن، يجب النظر في طرق التوثيق المتعددة العوامل حيث تتوافق هذه

الأســـاليب مع التفاعلات المعتمدة على الوقت بين موظفي المرفق ونظام الأجهزة والتحكم.

4-120-ويجب تطوير وتحديث إجراءات إدارة وتعيين الأدوار وحقوق الوصـــول لحسابات النظام والمستخدمين بشكل دوري. وينبغي أن تراعي الإجراءات مبدأ أقل الامتيازات. ويمكن الإشارة إلى هذه العملية أو دمجها في برنامج الأمن الحاسوبي في المرفق ونظام الإدارة المتكاملة في المرفق.

حماية سرية المعلومات

4-121-تنطبق الإرشـــادات الواردة في الفقرات 4-122-4-125 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-122-وعندما لا يُطبَّق القدر الكافي من تدابير الحماية المادية والأمن الحاســـوبي لحماية ســـرية المعلومات، فمن الممكن أن يحدث إفشـــاء غير مأذون به للمعلومات يمكن أن يؤدي إلى اختراق الحماية المادية أو الأمن الحاسوبي في النظام أو المرفق. وينص العدد G-23 من سلسلة الأمن النووي [15] الصادرة عن الوكالة على ما يلي:

> "المعلومات لبنات المعرفة، بغض النظر عن شـــكل وجودها أو طريقة التعبير عنها. وهي تتضـــمن الفِكَر والمفاهيم والأحداث والعمليات والأفكار والوقائع والأنماط. ويمكن تســـجيل المعلومات على مواد مثل الورق أو الأفلام أو الوســـائط المغناطيســـية أو البصـــرية أو يُحتَفَظ بها في النظم الإلكترونية".

4-123-وينبغي تحديد المعلومات المتعلقة بنظم الأجهزة والتحكم (مثل قواعد البيانات والملفات والوثائق المرتبطة بها؛ ومكونات التغيير؛ وأجهزة المحاكاة)، وعند الاقتضاء، تصنيفها على أنها معلومات حساسة وتأمينها بالتدابير المناسبة. ويوفر المرجعان [12، و15] معلومات إضافية بشأن توصيات لحماية المعلومات الحساسة.

4-124-ويجب استخدام تدابير الأمن الحاسوبي لحماية سرية المعلومات المرتبطة بنظم الأجهزة والتحكم، والتي قد تتضمن معلومات حول تصميم وتصنيع وتركيب وتشغيل نظم الأجهزة والتحكم والمعدات المرتبطة بها.

4-125-ويجب على المشغِّل تطبيق تدابير التحكم التقني والمادي والإداري لمنع الإفشاء غير المأذون به عن المعلومات الحساسة المتعلقة بنظم الأجهزة والتحكم أو استخراجها، وكشف هذه الأعمال والتصدي لها.

رصد الأمن

4-126-تنطبق الإرشادات الواردة في الفقرات 4-127-4-130 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-127-ويجب تحديد متطلبات الأمن الحاسوبي لرصد الأمن في نظم الأجهزة والتحكم بما يتفق مع مستويات الأمن المعيَّنة للنظم.

4-128-ويجب أن يستخدم رصد نظم الأجهزة والتحكم الذي يتطلب أعلى مستوى أو مستوى عالٍ من الأمن الاستقلالية[20] أو التنوع في تدابير الأمن الحاسوبي المنشورة للكشف عن الاختراق أو أنماط سوء التشغيل. وينبغي توفير واجهات المستخدم لرصد الأمن، ومؤشرات الاختراق، ووثائق التسجيل، وأجهزة الإنذار في المواقع المناسبة، وينبغي أن تكون مناسبة وكافية لدعم الرصد الفعال للأمن الحاسوبي في جميع الحالات التي تكون عليها المحطة.

4-129-وينبغي وضع متطلبات لرصد حالة تدابير التحكم التقني أو المادي لتيسير اتخاذ أي إجراءات ضرورية للأمان والأمن.

20 فصل نظم الرصد عن نظام الأجهزة والتحكم مما يسمح بفصل الواجبات هو أحد الأمثلة على الاستقلالية .

4-130-ويجب رصد نظم الأجهزة والتحكم وتدابير الأمن الحاسوبي المرتبطة بها وتسجيلها باستمرار. ويجب أن يحدد التحليل الوصول أو التغييرات غير المأذون بها. ويجب حماية سلامة هذه السجلات.

اعتبارات تتعلق بالهيكل الدفاعي العام للأمن الحاسوبي

4-131-تنطبق الإرشادات الواردة في الفقرات من 4-132 إلى 4-140 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-132-ويجب على المشغِّل تحديد هيكل دفاعي شامل للأمن الحاسوبي في نظم الأجهزة والتحكم يُعيَّن فيه مستوى أمن محدَّد لجميع نظم الأجهزة والتحكم وتحظى فيه بالحماية وفقاً للمتطلبات المعمول بها.

4-133-ويجب استخدام الهيكل الدفاعي لتسهيل والحفاظ على قدرة نظم الأجهزة والتحكم على منع الهجمات السيبرانية واكتشافها وتعطيلها وتخفيف عواقبها والتعافي منها. ويشمل الهيكل الدفاعي، على سبيل المثال لا الحصر، الحدود المنطقية أو المادية الشكلية مثل نطاقات الأمن التي تُنشر فيها التدابير الدفاعية.[21] وعند تنفيذ هذا الهيكل، ينبغي للمشغِّلين أن ينظروا في الحد من العناصر الدينامية لكل من الشبكات المركَّبة ونظمها الفردية لزيادة القدرة على توقع سلوك هذه الشبكات والنظم. وقد تساعد هذه الزيادة في القدرة على توقع السلوك على تنفيذ تدابير فعالة للأمن الحاسوبي للكشف عن الحوادث المحتملة المتصلة بالأمن الحاسوبي.

4-134-ويجب تطبيق حدود الأمن الحاسوبي فيما بين نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستويات أمن مختلفة ومحمية باستخدام تدابير مختلفة للأمن الحاسوبي. وحدود الأمن الحاسوبي هي الحدود المنطقية والمادية في نظام أو مجموعة من النظم التي تتمتع بنفس مستوى الأمن، وبالتالي يمكن تأمينها من خلال تطبيق تدابير دفاعية مشتركة (مثل نطاقات الأمن الحاسوبي).

21 من الأمثلة على هذه الهياكل الدفاعية هو الهيكل الدفاعي الذي يتضمن سلسلة من المستويات الدفاعية المتركِّزة لزيادة الأمن ويأخذ في الاعتبار مكونات الأجهزة والبرامج الحاسوبية.

4-135-ويجب التحكم في تدفق البيانات بين نطاقات الأمن المعيَّن لها مستويات أمن مختلفة وبين فرادى نظم الأجهزة والتحكم التي لها نفس مستوى الأمن بناءً على نهج قائم على العلم بالمخاطر لضمان استمرار فعالية الهيكل الدفاعي.

4-136-ويجب توصيل نظم الأجهزة والتحكم التي تتطلب أعلى مستوى من الأمن (أي مستوى الأمن الأكثر صرامة) فقط بالنظم التي تتطلب مستويات أقل من الأمن (أي مستويات أمن أضعف) عبر مسارات اتصال بيانات مؤمنة ضد التلاعب وحتمية السلوك وأحادية الاتجاه.[22] ويجب أن يقتصر اتجاه مسارات البيانات هذه على نقل البيانات من الأجهزة التي تتطلب مستوى أمن أكثر صرامة إلى الأجهزة المعيَّنة لمستويات الأمن الأضعف. وينصح بشدة عدم السماح بأي استثناءات ولا يجوز النظر فيها سوى على أساس كل حالة على حدة، على أن تكون مدعَّمة بتبرير كامل وبتحليل للمخاطر الأمنية.[23]

4-137-ويجب ألا تتجاوز الأجهزة الرقمية أو شبكات الاتصالات المستخدمة في أنشطة الرصد والصيانة والتعافي تدابير التحكم التقني المستخدمة لحماية مسارات الاتصال بين الأجهزة ذات مستويات الأمن المختلفة.

4-138-ويجب وضع النظم المعيَّن لها المستوى الأكثر صرامة من الأمن داخل حدود النطاق الأكثر أمناً. ووظائف الاتصالات اللاسلكية تتسم بالإشكالية عند تنفيذها في نظم الأجهزة والتحكم المعيَّن لها مستوى الأمن الأكثر صرامة حيث يصعب توفير حدود آمنة لمثل هذه الاتصالات.

4-139-وينبغي حماية اتصالات البيانات بين نظم الأجهزة والتحكم في المرفق ومركز الطوارئ (سواء في الموقع أو خارجه) والتحكم فيها من خلال تدابير الأمن الحاسوبي.

4-140-وينبغي أن تستخدم تدابير التحكم التقني المنفذة داخل كل نطاق أمني أو على حدود النطاق الأمني تكنولوجيات مختلفة عن تلك المنفذة في المستويات أو الحدود

22 لا يمكن تنفيذ إمكانية الوصول عن بُعد إلى النظم المطبَّق عليها أكثر مستويات الأمن صرامة بسبب تقييد حركة المرور الصادرة من نظام الأجهزة والتحكم في اتجاه واحد.

23 بعض الدول الأعضاء تشعر بشدة أنه ينبغي عدم السماح بأي استثناءات مهما كانت الحالة.

الأمنية المجاورة. وسيضمن ذلك استخدام تكنولوجيات متنوعة لحماية نظم الأجهزة والتحكم.

الدفاع في العمق ضد الاختراق

4-141-تنطبق الإرشادات الواردة في الفقرات 4-142 إلى 4-151 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-142-وينطوي الدفاع في العمق ضد الاختراق على توفير طبقات دفاعية متعددة من تدابير الأمن الحاسوبي التي يلزم أن تتعطل أو يتم تجاوزها حتى يمكن لأي هجوم سيبراني أن يمضي قدماً ليؤثر على نظام الأجهزة والتحكم. ولذلك، لا يتحقق الدفاع في العمق فقط من خلال وضع طبقات دفاعية متعددة (مثل نطاقات الأمن داخل الهيكل الدفاعي للأمن الحاسوبي)، ولكن أيضاً من خلال إنشاء وصون برنامج قوي لتدابير الأمن الحاسوبي التي تُقيِّم الهجوم على نظام الأجهزة والتحكم وتمنعه وتكشفه وتحمي منه وتتصدي له وتخفف من عواقبه وتساعد على التعافي منه. وعلى سبيل المثال، إذا تعذر منع الهجوم (مثل انتهاك السياسة) أو إذا تم تجاوز آليات الحماية (على سبيل المثال من خلال فيروس جديد لم يُحدَّد بعدُ على أنه هجوم سيبراني)، فستظل هناك آليات أخرى للكشف عن حدوث تغيير غير مأذون به في نظام الأجهزة والتحكم المتضرر والتصدي له.

4-143-ولا ينبغي لأي حالة من حالات التعذر داخل أو عبر الطبقات الدفاعية أن يؤدي إلى الحكم على الأمن الحاسوبي العام في نظم الأجهزة والتحكم بأنه غير صالح أو غير فعال. فعلى سبيل المثال، فإن استغلال ثغرة أمنية حرجة داخل جهاز مشترك لحماية الشبكة يُستخدم في مكانين مرتبطين منطقيًّا ولكنهما منفصلان ماديًّا من شأنه أن ييسر هجوماً يتجاوز طبقات متعددة من تدابير الأمن الحاسوبي.

4-144-ويجب تصميم نظم الأجهزة والتحكم والمكونات الرقمية ذات الصلة وتشغيلها وفقاً لمفهوم الدفاع في العمق ضد الاختراق.

4-145-ويجب أن يُعهد إلى الموظفين أداء الإجراءات الأمنية التي تكمِّل تدابير التحكم التقني. وينبغي تحليل وتبرير التوازن بين النشاط البشري وتدابير التحكم التقني.

4-146-ويجب اتباع نهج منظم لتحديد وتوثيق الإجراءات البشرية التي يمكن أن تؤثر سلباً على أمن الأجهزة والتحكم في كل مرحلة من مراحل دورة حياة نظام الأجهزة والتحكم.

4-147-ويجب استخدام نهج قائم على العلم بالمخاطر لتحديد توفير الأمن المناسب لنظم الأجهزة والتحكم، بما في ذلك تنفيذ تدابير التحكم التقني والدفاع في العمق ضد الاختراق. ويجب تنفيذ طبقات تدابير الأمن الحاسوبي المُستخدمة لتنفيذ الدفاع في العمق ضد الاختراق وفقاً للمرفق وعملية إدارة مخاطر الأمن الحاسوبي في النظام.

4-148-ويجب حماية كل طبقة دفاعية من الهجمات السيبرانية الناشئة في الطبقات المجاورة.

4-149-ويجب أن تخفف آليات الحماية المستخدمة للعزل بين الطبقات الدفاعية من الأعطال الراجعة إلى أسباب شائعة.

4-150-ويجب أن تمنع الطبقات الدفاعية والتدابير المضادة المرتبطة بها تقدم الهجمات أو تؤخره.

4-151-ويجب أن تكون الطبقات الدفاعية فعالة طوال دورة حياة نظام الأجهزة والتحكم ويجب مراعاتها في تصميم مكونات النظام وتكوينها وتعديلها وتعيين البارامترات لها.

أنشطة محدَّدة في دورة الحياة

مواصفات متطلبات الأمن الحاسوبي

4-152-ينبغي تحديد وتوثيق متطلبات الأمن الحاسوبي للهيكل الدفاعي ولفرادى نظم ومكونات الأجهزة والتحكم. ويجب أن تُستمد متطلبات الهيكل الدفاعي من الأساس التصميمي للأجهزة والتحكم.

4-153-ويجب أن تأخذ متطلبات الأمن الحاسوبي لنظم الأجهزة والتحكم والنظم الفرعية والمكونات في الاعتبار المتطلبات الوظيفية والأداء، وتكوين النظام، والتأهيل، وهندسة العوامل البشرية، وتعريفات البيانات والاتصالات، والتوثيق، والتركيب والإدخال في الخدمة، والتشغيل، والصيانة.

4-154-ويجب مراعاة عملية إدارة مخاطر الأمن الحاسوبي في المرفق والنظام عند إعداد متطلبات الأمن الحاسوبي لنظم الأجهزة والتحكم. ويجب استعراض متطلبات الأمن الحاسوبي وتحديثها بناءً على التغييرات التي تطرأ على مخرجات إدارة مخاطر الأمن الحاسوبي في المرفق والنظام.

4-155-ويجب أن يفي الجمع بين متطلبات الأمن الحاسوبي للهيكل الدفاعي وفرادى نظم الأجهزة والتحكم بالأساس التصميمي المحدد للهيكل الشامل للأجهزة والتحكم.

اختيار المفردات المطوَّرة مسبقاً

4-156-تنطبق الإرشادات الواردة في الفقرات 4-157 إلى 4-164 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات التي يمكن تطبيق نهج متدرج عليها.

4-157-وقد تتضمن المفردات المطوَّرة مسبقاً الأجهزة الإلكترونية أو البرامج الحاسوبية المطوَّرة مسبقاً أو المنتجات التجارية المتاحة في السوق أو الأجهزة الرقمية المكونة من الأجهزة والبرامج الحاسوبية (بما في ذلك البرامج الثابتة) أو الأجهزة التي تم تكوينها باستخدام لغة وصف الأجهزة أو الكتل الوظيفية المطوَّرة مسبقاً.

4-158-ويمكن أن تشمل المفردات المطوَّرة مسبقاً الأجهزة والبرامج الحاسوبية المطوَّرة مسبقاً (بما في ذلك البرامج الثابتة) من المنظمات التي ليس لديها برنامج مناسب للأمن الحاسوبي أو التي لا ترغب في مشاركة تفاصيل برنامجها للأمن الحاسوبي. وفي هذه الحالات، من الضروري تحليل خصائص الأمن الحاسوبي للمفردات وتبرير استخدامها إما داخل نظم الأجهزة والتحكم أو النظم المساعدة.

4-159-ومن المحتمل أن تكون منتجات البرامج الحاسوبية المطوَّرة مسبقاً والمنتجات التجارية المتاحة في السوق ذات ملكية خاصة ولا تتوافر عموماً تعليماتها البرمجية المصدر لإخضاعها لأنشطة التحقق المكثفة. وعليه يرجح أنه لا توجد طريقة موثوقة أمام المشغِّل لتحديد الثغرات الأمنية في هذه المنتجات بشكل شامل. وفي مثل هذه الحالات، ستكون هناك حاجة إلى تدابير الأمن الحاسوبي التعويضية ما لم يضطلع مطوِّر التطبيق بتعديل هذه المنتجات.

4-160-ويجب تطبيق تدابير الأمن الحاسوبي لضمان عدم تمكُّن سمات منتجات البرامج الحاسوبية المطوَّرة مسبقاً والمنتجات التجارية المتاحة في السوق من التسبب في أن تخفق نظم الأجهزة والتحكم في تلبية متطلبات الأمن الحاسوبي الخاصة بها. وعلى سبيل المثال، قد تتوافر الإرشادات لتقليل مقدار تشغيل التعليمات البرمجية، لمنع توفر نقاط الدخول للمستخدمين غير المأذون لهم وإزالة الوظائف غير الضرورية، وبالتالي تقليل مواطن الضعف المعرضة للهجوم (أي تحصين النظام). ومع ذلك، لا يمكن الحصول إلا على حماية محدودة من خلال تطبيق تدابير الأمن الحاسوبي، ويجب على المشغِّل تطبيق مزيد من تدابير الأمن الحاسوبي التعويضية.

4-161-ويجب اختيار المكونات أو البرامج المطوَّرة مسبقاً وتكوينها باستخدام عملية تأهيل أمني تتناسب مع مستوى الأمن في نظام الأجهزة والتحكم.

4-162-ويجب التحقق من استخدام منتجات البرامج الحاسوبية المطوَّرة مسبقاً والمنتجات التجارية المتاحة في السوق لضمان تلبية هذه المنتجات لمتطلبات الأمن الحاسوبي في نظام الأجهزة والتحكم.

4-163-ويجب على المشـــغِّل تحديد الوثائق المطلوبة لتأهيل منتجات البرامج الحاســوبية المطوَّرة مســبقاً. وينبغي عدم الاعتماد على تدابير التحكم التقني التي لا يمكن التحقق من فعاليتها.

4-164-ويجب إزالة الوظائف أو الخدمات غير الضـــرورية في منتجات البرامج الحاسوبية المطوَّرة مسبقاً أو المنتجات التجارية المتاحة في السوق القابلة للتكوين.

تصميم وتنفيذ نظم الأجهزة والتحكم

4-165-تنطبق الإرشـادات الواردة في الفقرات 4-166 إلى 4-174 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-166-وفي مرحلة تنفيذ نظام الأجهزة والتحكم (الأجهزة والبرامج المتكاملة)، يُحوَّل تصـميم النظام إلى تعليمات برمجية وهياكل قواعد بيانات وما يتصـل بها من تمثيلات يمكن للجهاز تنفيذها. وتتناول مرحلة التنفيذ تكوين الأجهزة وإعدادها، وتشفير البرامج الحاسوبية واختبارها، وتكوين الاتصـالات وإعدادها (بما في ذلك، عند الاقتضاء، دمج البرامج الحاسوبية المُعاد استخدامها والمنتجات التجارية المتاحة في السوق).

4-167-وفي مراحل تصـــميم وتنفيذ دورة حياة نظام الأجهزة والتحكم، يجب تحديد متطلبات الأمن الحاسوبي لنظم الأجهزة والتحكم والتحقق من تنفيذها.

4-168-ويجب ترجمة المتطلبات المحددة في مواصـفات نظام الأجهزة والتحكم إلى عناصـر تصـميم محددة في وصـف تصـميم النظام. وينبغي أن تتضـمن عناصـر التصـميم المحددة أحكاماً تُنفَّذ في إطار تصـميم نظام الأجهزة والتحكم أو عن طريق تدابير الأمن الحاسوبي المنفذة من الخارج على نظام الأجهزة والتحكم.

4-169-ويجب أن تتطرق عناصـر تصـميم الأمن الحاسـوبي لنظام الأجهزة والتحكم إلى التحكم في الوصول المادي والمنطقي إلى وظائف النظام، واستخدام خدمات نظام الأجهزة والتحكم واتصالات البيانات مع النظم الأخرى.

4-170-ويجب التحكم في الوصول المادي والمنطقي إلى نظام الأجهزة والتحكم بناءً على مستوى الأمن المعيَّن لنظام الأجهزة والتحكم. فعلى سبيل المثال، ستحتاج النظم المعيَّن لها المستوى الأكثر صرامة من مستويات الأمن إلى متطلبات أمن حاسوبية للتحكم في الوصول المتعدد العوامل، مثل التحكم في الوصول الذي يتطلب مجموعة من المعلومات (مثل كلمة السر) والأدوات المقتناة (مثل المفتاح، والبطاقة الذكية) والسمات الشخصية (مثل بصمات الأصابع).

4-171-ويجب تصميم نظم الأجهزة والتحكم بحيث تشمل سمات تمكِّن من الصمود أمام الاختراق أو الحماية منه.

4-172-وينبغي أن توفر تدابير التصميم ثقة كافية بأن أمن النظام المعيَّن له مستوى أمن محدَّد لن يضعف عند توصيله بالنظم المعيَّن لها مستويات أمن أضعف.

4-173-وينبغي تصميم توليفات مناسبة من تدابير التحكم الإداري (مثل برنامج للأمن الحاسوبي) وتدابير التحكم المادي للحد من تعرض نظام الأجهزة والتحكم للهجوم السيبراني.

4-174-ويجب تخصيص مكونات نظام الأجهزة والتحكم وتركيبها في مواقع المرافق التي تؤمن فعليًّا المعدات واتصالات شبكتها مع النظم الأخرى، على سبيل المثال، وضع جميع وصلات بيانات النظم والمكونات داخل حاويات آمنة.

تكامل نظام الأجهزة والتحكم

4-175-تنطبق الإرشادات الواردة في الفقرات 4-176 إلى 4-178 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها.

4-176-وتكامل نظام الأجهزة والتحكم هو عملية الجمع بين الأجهزة والبرامج الحاسوبية لنظام الأجهزة والتحكم (بما في ذلك البرامج الثابتة) في نظام واحد. وفي كثير من الأحيان، يُجري البائعون أو المتعاقدون أو الموردون اختبار تكامل لكل نظام ينتجونه على حدة بالإضافة إلى مجموعة من النظم ضمن نطاق التكامل مع هذا

النظام قبل شحنه إلى موقع المرفق. ويتحقق هذا الاختبار من التنفيذ السليم لمكونات البرنامج الحاسوبي والترابط المناسب بين المكونات داخل نظام الأجهزة والتحكم.

4-177-وخلال مرحلة تكامل النظام في دورة حياة نظام الأجهزة والتحكم، يجب وضع تدابير التحكم التقني المتكاملة وأن يتوافق تكوينها مع المواصفات قبل إجراء الاختبار.

4-178-وأثناء اختبار التكامل، يجب على البائع أو المتعاقد أو المورد التأكيد على أن تدابير الأمن الحاسوبي المتكاملة تعمل على النحو المحدد ولا تؤثر سلباً على قدرة نظم الأجهزة والتحكم على أداء وظائفها الأساسية.

اعتماد النظام

4-179-تنطبق الإرشادات الواردة في الفقرات 4-180 إلى 4-185 على جميع نظم الأجهزة والتحكم والنظم الفرعية والمكونات المعيَّن لها مستوى أمن محدَّد.

4-180-وتُجرى أنشطة اعتماد النظام عادة بالتوازي مع مراحل أخرى من دورة الحياة. وبعد استكمال تكامل النظام، يُجرى تحقق جزئي من اعتماد النظام عادة، على سبيل المثال، باستخدام مدخلات محاكاة. وتستمر أنشطة الاعتماد عادة كجزء من مراحل التركيب وتكامل الأجهزة والتحكم والتشغيل. ويعتبر اعتماد النظام مكتملاً عند تسليمه لكي يبدأ استخدامه في عمليات المرفق العادية.

4-181-وأثناء اعتماد كل نظام من نظم الأجهزة والتحكم ونظمه الفرعية ومكوناته، يجب إثبات تنفيذ متطلبات الأمن الحاسوبي وعناصر التكوين. والهدف من اختبار وظائف الأمن هو التأكد من اعتماد متطلبات الأمن الحاسوبي لنظم الأجهزة والتحكم من خلال تنفيذ اختبارات التكامل والنظام والقبول حيثما كان ذلك عمليًّا وضروريًّا.

4-182-وينبغي أن تؤكد أنشطة اعتماد النظام فعالية تدابير الأمن الحاسوبي وأن تتحقق من الآثار المحتملة، المباشرة أو غير المباشرة، على وظائف الأمان.

4-183-ويجب إثبات أن كل إجراء تحكم تقني يُنفَّذ في نظام الأجهزة والتحكم يعمل بالطريقة المرجوة وأنه لن يزيد من مخاطر الثغرات الأمنية أو يقلل من موثوقية وظائف الأمان.

4-184-ويجب أن يشمل اعتماد تدابير الأمن الحاسوبي في نظام الأجهزة والتحكم تقييماً لتكوين النظام (بما في ذلك جميع التوصيلات الخارجية)، واختبار تأهُّل البرامج الحاسوبية، واختبار تأهُّل النظام، واختبار القبول في مَصنع النظام. ويمكن تدعيم اعتماد تدابير الأمن الحاسوبي باختبارات لنظام الأجهزة والتحكم تحدد الثغرات الأمنية المحتملة أو تحدد خصائص السلوكيات أو الإجراءات غير المتوقعة.

4-185-ويجب إجراء اختبار اعتماد النظام في بيئة آمنة. وعلى سبيل المثال، يجب تأمين أجهزة الاختبار مثل أجهزة المحاكاة أو أجهزة المضاهاة من خلال تدابير الأمن الحاسوبي. ويجب أن تكون صرامة تدابير الأمن الحاسوبي متناسبة مع مستوى الأمن المعيَّن لنظام الأجهزة والتحكم.

تركيب نظم الأجهزة والتحكم وتكاملها الشامل وتشغيلها

4-186-يجب على المشغِّل أثناء عملية تركيب وتشغيل النظام إجراء استعراض لقبول صحة تدابير التحكم المادي والتقني في البيئة المستهدفة مع مراعاة التكامل الشامل لنظام الأجهزة والتحكم[24].

4-187-ويجب تركيب نظام الأجهزة والتحكم وتحقيق التكامل الشامل لنظام الأجهزة والتحكم وتشغيله في بيئة آمنة. ويجب أن يُراعى عند تعيين مستوى الأمن في هذه البيئة مستوى أمن النظام في البيئة المستهدفة ومستوى أمن الأدوات المستخدمة في التركيب والتشغيل.

4-188-وينبغي حماية البيئة الآمنة باستخدام تدابير الأمن الحاسوبي التي تتناسب مع مستوى الأمن المعيَّن لنظام الأجهزة والتحكم والعمليات الأمنية التي يجري الاضطلاع بها من أجل التركيب والتشغيل. وفي بعض الحالات، ينبغي توفير تدابير

24 في هذا المنشور، يشير "التكامل الشامل لنظام الأجهزة والتحكم" إلى تكامل جميع نظم الأجهزة والتحكم في المرفق، وهو يختلف عن "تكامل نظام الأجهزة والتحكم"، الذي نوقش سابقاً في هذا المنشور.

تعويضـية للتحكم الإداري والمادي للتحكم في الوصـول إلى البيئة الآمنة فضـلاً عن المعدات ومصادر البيانات المرتبطة بها.

4-189-ويجب التحقق من المعدات المسـتخدمة في البيئة الآمنة للتأكد من أن استخدامها لا يتيح مسارات لإدخال تعليمات برمجية أو بيانات شريرة في البيئة أو مكونات نظام الأجهزة والتحكم.

4-190-ويجب وضع تدابير للأمن الحاسوبي للتحكم في حركة البيانات والأصول الرقمية ورصدها داخل وخارج البيئة الآمنة.

عمليات التشغيل والصيانة

4-191-تنطبق الإرشادات الواردة في الفقرات 4-192 إلى 4-205 على جميع نظم الأجهزة والتحكم ونظمها الفرعية ومكوناتها التي يمكن تطبيق نهج متدرج عليها وفقاً لمستوى الأمن المعيَّن لها.

4-192-وتستمر أنشطة التشغيل والصيانة طوال دورة حياة الأجهزة والتحكم وقد نوقِشت بالفعل في الأقسام أعلاه التي تتناول تخطيط العمليات والأنشطة المشتركة في جميع مراحل دورة الحياة. ويجب أن تتحمل المنظمة المشغِّلة المسؤولية الكاملة عن الأمن الحاسوبي للأداء المستمر لأنشطة التشغيل والصيانة عند الدخول في مرحلة التشغيل والصيانة لنظام ما.

4-193-وأنشطة الصيانة هي الأنشطة التي يطلبها المشغِّل للحفاظ على النظم أو المكونات في حالة التشغيل الجيدة. وينبغي توسيع نطاق أنشطة الصيانة هذه لتشمل تدابير التحكم التقني والمادي التي توفر الأمن الحاسوبي لنظم الأجهزة والتحكم وقد تشمل ما يلي:

- الصيانة الوقائية أو الاختبار بشكل دوري؛
- إجراءات الكشف عن تدهور المكونات أو منع حدوثه أو التخفيف من عواقبه؛

— إجراءات تشخيص المكونات المتعطِّلة أو إصلاحها أو تجديدها أو استبدالها بمكونات متطابقة.

4-194-ويجب تطبيق تدابير الأمن الحاسوبي على أنشطة التشغيل والصيانة لضمان عدم المساس بالمكونات والنظم.

4-195-وتتضمن مرحلة التشغيل استخدام المشغِّل لنظام الأجهزة والتحكم في بيئته التشغيلية المقصودة. ويجب على المشغِّل خلال مرحلة التشغيل ما يلي:

— التحقق من سلامة أمن نظام الأجهزة والتحكم باستخدام تقنيات مثل الاختبار والرصد بشكل دوري واستعراض سجلات النظام والرصد في الوقت الفعلي، حيثما أمكن ذلك؛
— تقييم تأثير التغييرات الطارئة على نظام الأجهزة والتحكم في بيئة التشغيل على أمن نظام الأجهزة والتحكم؛
— تقييم تأثير أي تغييرات مقترحة على أمن نظام الأجهزة والتحكم؛
— تقييم امتثال إجراءات التشغيل للاستخدام المقصود؛
— تحليل المخاطر الأمنية التي تؤثر على المشغِّل والنظام؛
— تقييم القيود الأمنية الجديدة في النظام؛
— تقييم إجراءات التشغيل للتأكد من صحتها وسهولة استخدامها؛
— إجراء تقييمات ومراجعات ذاتية دورية لأمن النظام الحاسوبي، وهي مكونات رئيسية في أي برنامج أمني جيد؛
— تقييم تقارير الحادثات المتاحة حول التهديدات والثغرات الأمنية الجديدة.

4-196-وينبغي تحليل أنشطة التشغيل والصيانة لضمان تنفيذ تدابير الأمن الحاسوبي لمنع إدخال البرامج الحاسوبية الشريرة إلى نظام الأجهزة والتحكم.

4-197-ويجب أن تتوافق أنشطة الصيانة مع متطلبات الأمن الحاسوبي الحالية في نظام الأجهزة والتحكم ما لم يتم تغيير هذه المتطلبات كجزء من نشاط الصيانة. وفي بعض الحالات، قد يلزم إزالة أو تعطيل إجراءات الأمن الحاسوبي مؤقتاً للسماح

بتنفيذ مهام الصيانة المطلوبة. وخلال الفترة التي لا تتوافر فيها تدابير الأمن الحاسوبي، يكون النظام في خطر أكبر ويجب تنفيذ تدابير تعويضية.

4-198-وقد تتضمن أنشطة المعايرة والاختبار والصيانة استخدام الوسائط القابلة للإزالة والأجهزة المحمولة المتصلة مؤقتاً بنظم الأجهزة والتحكم ومكوناتها الرقمية. وينبغي أن تراعي تدابير الأمن الحاسوبي لهذه الأنشطة ما يلي:

- تنفيذ تدابير التحكم الإداري والتقني الفعالة في التعامل المأمون والآمن مع الأجهزة الرقمية؛
- التحقق من سلامة جميع نقاط مجموعة التحكم بهدف منعها وحمايتها من التغييرات غير المرغوب فيها؛
- استخدام الموظفين المؤهلين (بما في ذلك الأطراف الثالثة) الذين تلقوا تدريباً على أداء هذه الأنشطة بناءً على متطلبات الأمن الحاسوبي.

4-199-ويجب تعطيل واجهات المستخدم أو تقييد الوصول إليها عندما لا تكون هناك حاجة إليها أو تكون غير مستخدمة (مثل توصيل أجهزة حواسيب الصيانة والتطوير).

4-200-ويجب وضع تدابير الأمن الحاسوبي لمنع الوصول غير الضروري أو غير المأذون به.

4-201-ويجب أن تتوافر عمليات الرصد أو التطبيقات للتحقق من تكوين البرنامج الحاسوبي الحالي مقابل التكوينات المعروفة.

4-202-ويجب تقييد الوصول عن بُعد إلى أقصى حد ممكن. وعند الحاجة إلى الوصول عن بُعد، ينبغي النظر في المخاطر الناشئة عن هذه الاتصالات، ويجب تنفيذ تدابير إضافية للأمن الحاسوبي. وينبغي الحفاظ على هذا الاتصال فقط طالما كان ذلك ضروريًّا لتحقيق غرضه المحدد.

4-203-ويجب التحكم بعناية في أنشـــطة التشـــغيل والصـــيانة من خلال عمليات وإجراءات صـــيانة تتم بأوامر عمل رســـمية. وعلى ســـبيل المثال، يجب مراعاة الضـوابط والتوازنات، مثل قاعدة وجود شـخصـين، فيما يخص أداء مهام مثل إجراء تغييرات على تكوين نظم الأجهزة والتحكم العاملة.

4-204-ويجب ألا تتطلب أنشـــطة التشـــغيل إجراء تغييرات على تدابير الأمن الحاسوبي في نظام الأجهزة والتحكم.

4-205-ويجب حماية أدوات تشـغيل وصـيانة النظام التي يمكن اسـتخدامها لاختراق نظام الأجهزة والتحكم بما يتناســب مع مســتوى الأمن ذي الصــلة في نظام الأجهزة والتحكم. وعلى سبيل المثال، يجب عدم استخدام الأدوات المستخدمة في نظام معيَّن له مستوى أمن أكثر صرامة في نظام آخر معيَّن له مستوى أمن أضعف.

تعديل نظم الأجهزة والتحكم

4-206-إن تطبيق تدابير الأمن الحاســـوبي على نظم الأجهزة والتحكم القديمة في مرفق نووي قائم ليس دائماً بالأمر السـهل. وعلى سـبيل المثال، قد تنشـأ الصـعوبات التالية:

- قد لا يكون تغيير هيكل الأجهزة والتحكم القديمة ممكناً دون التأثير على السلوك الحتمي لنظم الأجهزة والتحكم القديمة.
- قد لا تدعم التقنيات الحالية المسـتخدمة للبرامج أو لتخزين البيانات أو واجهات المستخدم أو الاتصالات إجراء التعديلات.
- قد لا تسـمح هياكل المرافق القائمة وتصـميمها باتخاذ تدابير كافية لتوفير الحماية المادية.
- قد لا تكون تدابير التحكم التقني المعاصرة التي توفر وظائف رصد الأمن متوافقة مع التكنولوجيات المطبقة في نظم الأجهزة والتحكم القديمة.

4-207-وعند تحديث مرفق نووي من خلال الاسـتعاضـة عن نظم الأجهزة والتحكم القديمة بنظم أجهزة وتحكم حديثة، ينبغي للمشـــغِّل أن ينظر في إمكانية الإبقاء على

واجهات المستخدم القديمة في النظم الأصلية في المرفق وغيرها من النظم، وإمكانية أن تنشأ ثغرات أمنية ومواطن ضعف جديدة بسبب التكنولوجيا أو التصميم الجديدين.

4-208-تعديلات نظم الأجهزة والتحكم تغيّر النظام أو وثائقه. ويمكن تصنيف هذه التغييرات على النحو التالي:

- التغييرات أو التحسينات (تصحيحية أو تكيفية)؛
- الترحيل (أي نقل النظام إلى بيئة تشغيلية جديدة)؛
- الاستبدال (أي توقف المنظمة المسؤولة عن التشغيل والصيانة عن تقديم الدعم النشط، أو الاستبدال الجزئي أو الكلي بنظام جديد، أو تثبيت نظام مطوَّر).

4-209-وقد تنشأ التعديلات على نظام الأجهزة والتحكم من متطلبات معينة أو أن تكون محدَّدة لتصحيح الأخطاء (تعديلات تصحيحية)، أو للتكيف مع بيئة تشغيل متغيرة (تعديلات تكيفية)، أو لتلبية طلبات أو تحسينات إضافية لدى المشغِّل.

4-210-وعند إجراء تعديلات على نظام الأجهزة والتحكم، يجب إجراء تقييم لأمن نظام الأجهزة والتحكم المعدَّل، على سبيل المثال، عن طريق تحديث إدارة مخاطر الأمن الحاسوبي في النظام.

4-211-ويجب مراعاة الأمن الحاسوبي كجزء من عملية إدارة التغيير. ويتضمن ذلك التغييرات في البرامج الحاسوبية والأجهزة في نظم الأجهزة والتحكم.

4-212-ولضمان عدم التسبب في حدوث ثغرات أمنية في بيئة المرفق عن طريق هذه التعديلات، يجب على المشغِّل تقييم التغييرات المقترحة في نظام الأجهزة والتحكم بما في ذلك تأثيرها على برنامج الأمن الحاسوبي وأمن نظام الأجهزة والتحكم الحالي، وتقييم الحالات الشاذة التي تُكتشف أثناء التشغيل، وتقييم احتياجات الترحيل وتقييم التعديلات المجراة، بما في ذلك أنشطة التحقق والاعتماد.

4-213-وينبغي تقييم تدابير الأمن الحاسوبي على النحو المبين في الفقرات 4-206 إلى 4-212 أعلاه، وينبغي تنقيحها لتبرز متطلبات الأمن الحاسوبي المستمدة من عملية التعديل، حسب الاقتضاء.

4-214-وأثناء التعديل، يجب أن تظل متطلبات الأمن الحاسوبي الحالية في نظام الأجهزة والتحكم مفعَّلة ما لم يتم تغيير هذه المتطلبات كجزء من نشاط التعديل.

4-215-ويجب أن تكون هناك إدارة لتكوين تدابير الأمن الحاسوبي لمنع إدخال برامج غير مأذون بها إلى نظم الأجهزة والتحكم.

4-216-وعند ترحيل النظم، يجب على المشغِّل التحقق من أن النظم التي تُرحَّل تفي بمتطلبات الأمن الحاسوبي في نظام الأجهزة والتحكم.

4-217-ويجب أن تُمسح من النظام الملفات المتبقية من عملية تطويره وتركيبه واختباره وملفات تكوينه قبل البدء في تشغيله.

4-218-ويجب التعامل مع التعديلات على نظم الأجهزة والتحكم على أنها عمليات تطوير ويجب التحقق منها واعتمادها.

4-219-ويجب أن تأخذ جميع التعديلات على نظام الأجهزة والتحكم ومكوناته، بما في ذلك تكوينات البرامج الحاسوبية والأجهزة والنظام، في الاعتبار الثغرات الأمنية والتهديدات المحتملة التي قد تحدث ليس فقط أثناء تنفيذ هذه الأنشطة ولكن أيضاً نتيجة للتعديلات.

4-220-وتتمتع العديد من الأصول الرقمية والمكونات المرتبطة بها، بما في ذلك وسائط التخزين القابلة للإزالة، بالقدرة على الاحتفاظ بالبيانات الرقمية عند إزالتها من النظام. وقد تتضمن هذه البيانات الرقمية بيانات منطقية مبرمجة مسبقاً أو بيانات النظام المتبقية مثل قراءات أجهزة الاستشعار وإشارات التحكم والبيانات التحليلية وحركة المرور في الشبكة. وقد تكون هذه البيانات قابلة للاستخراج من المكونات المهملة.

4-221-وينبغي وضع تدابير للتحكم الإداري والتقني لضمان عدم إمكانية استخدام البيانات المتبقية المتعلقة بالمكونات المهملة بشكل يساعد في تطوير ثغرة لاستغلال الحاسوب. ويجب تدمير المكونات أو إزالة البيانات بشكل آمن، ما لم يتم تقييم البيانات المتبقية في المكونات المراد التخلص منها لمعرفة أن هذه البيانات لا تشكل خطراً باختراق الأمن.

4-222-وبالنسبة للتعديلات التي تنطوي على استبدال نظم الأجهزة والتحكم، يجب على المشغِّل إجراء أنشطة مثل تنظيف البيانات أو إتلاف القرص أو الكتابة الفوقية الكاملة لضمان عدم إمكانية استرداد البيانات من نظام الأجهزة والتحكم المستبدل عند استبعادة من الخدمة.

الإخراج من الخدمة

4-223-في مرحلة الإخراج من الخدمة، وقبل سحب المواد النووية وغيرها من المواد المشعة وإزالة أصول المعلومات الحساسة من المرفق، ينبغي للمشغِّل أن يقيّم أثر استبدال أو إزالة الوظائف الأمنية الحالية في نظام الأجهزة والتحكم من بيئة التشغيل.

4-224-ويجب على المشغِّل أن يدرج في نطاق هذا التقييم تأثير إزالة وظائف أمن النظام على واجهات المستخدم في نظم الأمان وغيرها من النظم غير المتعلقة بالأمان.

4-225-وينبغي للمشغِّل أن يوثق الطرق التي سيتم من خلالها التخفيف من حدة عواقب التغيير في وظائف أمن نظام الأجهزة والتحكم (مثل استبدال وظائف الأمن، والعزل عن نظم الأمان الأخرى وتفاعلات المشغِّل، أو وقف تشغيل وظائف الترابط في نظام الأجهزة والتحكم).

4-226-وإلى أن يُستكمل إخراج المرفق من الخدمة، ينبغي أن تحتفظ الإجراءات الأمنية بالعناصر التي تكفل تطهير المعدات والبيانات.

المراجع

[1] ألبرايت، د.، وبرانان، ب.، وولروند، ك.، البرامجية الخبيثة ستاكسنت ومحطة ناتانز: تحديث للتقرير الصادر عن معهد العلوم والأمن الدولي في 22 كانون الأول/ديسمبر 2010 (2011)،
http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8

[2] الوكالة الدولية للطاقة الذرية، توصيات الأمن النووي بشأن الحماية المادية للمواد النووية والمرفق النووية (INFCIRC/225/Revision 5)، العدد 13 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).

[3] الوكالة الدولية للطاقة الذرية، الأمن الحاسوبي في المرافق النووية، العدد 17 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2011).

[4] الوكالة الدولية للطاقة الذرية، تصميم الأجهزة ونظم التحكم لمحطات القوى النووية، العدد SSG-39 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2016).

[5] الوكالة الدولية للطاقة الذرية، تدابير الحماية والوقاية ضد التهديدات من الداخل، العدد 8 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2008).

[6] الوكالة الدولية للطاقة الذرية، نظم الأجهزة والتحكم والبرامج الحاسوبية المهمة لأمان مفاعلات البحوث، العدد SSG-37 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2015).

[7] الوكالة الدولية للطاقة الذرية، مسرد مصطلحات الأمان الصادر عن الوكالة الدولية للطاقة الذرية: المصطلحات المستخدمة في مجالي الأمان النووي

والوقاية من الإشعاعات (طبعة 2018)، الوكالة الدولية للطاقة الذرية، فيينا (قيد الإعداد).

[8] الوكالة الدولية للطاقة الذرية، الهدف والعناصر الأساسية لمنظومة الأمن النووي الخاصة بالدولة، العدد 20 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2013).

[9] الوكالة الدولية للطاقة الذرية، استخدام نهج متدرج في تطبيق متطلبات الأمان في مفاعلات البحوث، العدد SSG-22 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2012).

[10] اللجنة الدولية للتقنيات الكهربائية، محطات القوى النووية - نظم الأجهزة والتحكم - متطلبات البرامج الأمنية في النظم القائمة على الحواسيب، العدد 62645 الصادر عن اللجنة الدولية للتقنيات الكهربائية: 2014، اللجنة الدولية للتقنيات الكهربائية، جنيف (2014).

[11] الوكالة الدولية للطاقة الذرية، الحماية المادية للمواد النووية والمرافق النووية، العدد G-27 من سلسلة الأمن النووي الصادرة عن الوكالة، فيينا (2018).

[12] المنظمة الدولية لتوحيد المقاييس، تكنولوجيا المعلومات - تقنيات الأمن - إدارة مخاطر أمن المعلومات، المنظمة الدولية لتوحيد المقاييس/اللجنة الدولية للتقنيات الكهربائية: العدد 27005: 2011، المنظمة الدولية لتوحيد المقاييس، جنيف (2011).

[13] الوكالة الدولية للطاقة الذرية، ثقافة الأمن النووي، العدد 7 من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2008).

[14] الوكالة الدولية للطاقة الذرية، القيادة والإدارة فيما يتعلق بالأمان، العدد GSR Part 2 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2016).

[15] الوكالة الدولية للطاقة الذرية، أمن المعلومات النووية، العدد G-23 من سلسلة منشورات الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2016).

[16] الوكالة الدولية للطاقة الذرية، تطبيق نظام إدارة المرافق والأنشطة، العدد GS-G-3.1 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2006).

[17] الوكالة الدولية للطاقة الذرية، نظام إدارة المنشآت النووية، العدد GS-G-3.5 من سلسلة معايير الأمان الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2009).

[18] الوكالة الدولية للطاقة الذرية، إعداد وصف التهديدات المحتاط لها في التصميم واستخدامه وصيانته، العدد 10 من سلسلة الوكالة للأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا (2009).

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 المفضَّل لديكم، أو بالموزّع 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

الوكالة الدولية للطاقة الذرية
فيينا