ألغي هذا المنشور وحلّ محلّه العدد (Rev. 1) No. 17-T.

العدد ١٧ من سلسلة الأمن النووي الصادرة عن الوكالة

دليل مرجعي
للإرشادات التقنية

الأمن الحاسوبي في المرافق النووية

IAEA
الوكالة الدولية للطاقة الذرية

سلسلة الأمن النووي الصادرة عن الوكالة

تعالج منشورات **سلسلة الأمن النووي الصادرة عن الوكالة** قضايا الأمن النووي المتعلقة بمنع وكشف أفعال السرقة والتخريب والوصول غير المأذون به والنقل غير المشروع وسائر الأفعال الإيذائية المتعلقة بالمواد النووية والمواد المشعة الأخرى والمرافق المرتبطة بها، والتصدي لتلك الأفعال. وتتسق هذه المنشورات مع الصكوك الدولية المتعلقة بالأمن النووي، مثل اتفاقية الحماية المادية للمواد النووية، بصيغتها المعدلة، ومدونة قواعد السلوك بشأن أمان المصادر المشعة وأمنها، وقراري مجلس الأمن الدولي ١٣٧٣ و١٥٤٠، والاتفاقية الدولية لقمع أعمال الإرهاب النووي، وتكمِّل تلك الصكوك.

الفئات في سلسلة الأمن النووي الصادرة عن الوكالة

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

- **أساسيات الأمن النووي:** تحتوي على أهداف الأمن النووي ومفاهيمه ومبادئه، وتوفر الأساس للتوصيات الأمنية.
- **التوصيات:** تعرض أفضل الممارسات التي ينبغي أن تعتمدها الدول الأعضاء في تطبيق أساسيات الأمن النووي.
- **أدلة التنفيذ:** تقدم المزيد من التفصيل عن التوصيات في مجالات واسعة، وتقترح تدابير لتنفيذها.
- منشورات **التوجيه التقني:** تشمل ما يلي: **الأدلة المرجعية**، التي تحتوي على تدابير و/أو توجيهات تفصيلية بشأن كيفية تطبيق أدلة التنفيذ في مجالات أو أنشطة محددة؛ و**الأدلة التدريبية**، التي تتناول المنهج و/أو الأدلة الخاصة بالدورات التدريبية التي تعقدها الوكالة في مجال الأمن النووي؛ و**الأدلة الخدمية**، التي تقدم توجيهات بشأن تنفيذ بعثات الأمن النووي الاستشارية ونطاقها التي تنظمها الوكالة.

الصياغة والاستعراض

يساعد خبراء دوليون أمانة الوكالة على صياغة هذه المنشورات. وفيما يخص أساسيات الأمن النووي والتوصيات وأدلة التنفيذ، تعقد الوكالة اجتماعا تقنيا مفتوح العضوية (أو اجتماعات) لتتيح للدول الأعضاء المهتمة والمنظمات الدولية ذات الصلة فرصة مناسبة لاستعراض مسودة النص. وإضافة إلى ذلك، ولضمان مستوى عال من الاستعراض وتوافق الآراء على الصعيد الدولي، تقدم الأمانة مسودات النصوص إلى جميع الدول الأعضاء لمدة ١٢٠ يوما لاستعراضها رسميا. ويتيح ذلك للدول الأعضاء فرصة للتعبير الكامل عن وجهات نظرها قبل نشر النص.

وتوضع منشورات التوجيه التقني بالتشاور الوثيق مع خبراء دوليين. ولا يلزم عقد اجتماعات تقنية، ولكنها قد تُعقد، حيثما تعتبر ضرورية، للحصول على مجموعة واسعة من وجهات النظر.

وتُراعى في عملية صياغة واستعراض المنشورات في سلسلة الأمن النووي التي تصدرها الوكالة اعتبارات السرية، ويُسلَّم بأن الأمن النووي يرتبط ارتباطا لا ينفصم بشواغل الأمن القومي العامة والمحددة. ومن الاعتبارات التي تستند إليها العملية أن الأنشطة ذات الصلة التي تقوم بها الوكالة في مجالي معايير الأمان والضمانات ينبغي أن توضع في الاعتبار في المحتوى التقني للمنشورات.

الأمن الحاسوبي في المرافق النووية

أُلغي هذا المنشور وحلَّ محلَّه العدد .No. 17-T (Rev. 1)

الدول التالية أعضاء في الوكالة الدولية للطاقة الذرية:

الاتّحاد الروسي
إثيوبيا
أذربيجـان
الأرجنتين
الأردن
أرمينيا
إريتريا
إسبانيا
أستراليا
إستونيـا
إسرائيل
أفغانستان (جمهورية-الإسلامية)
إكـوادور
ألبانيـا
ألمانيا
الإمارات العربية المتحدة
إندونيسيا
أنغـولا
أوروغواي
أوزبكستان
أوغنـدا
أوكرانيا
إيران (جمهورية - الإسلامية)
أيرلندا
آيسلنـدا
إيطاليـا
بابوا غينيا الجديدة
باراغواي
باكستان
بالاو
البحرين
البرازيل
البرتغـال
بلجيكـا
بلغاريـا
بليز
بنغلاديش
بنمـا
بنـن
بوتسوانا
بوركينا فاصو
بوروندي
البوسنة والهرسك
بولندا
بوليفيا
بيرو
بيلاروس
تايلند
تركيـا
ترينيداد وتوباغو
تشاد
توغو
تونـس

جامايكـا
الجبل الأسود
الجزائر
جزر مارشال
جمهورية أفريقيا الوسطى
الجمهورية التشيكية
الجمهورية الدومينيكية
الجمهورية العربية السورية
جمهورية الكونغو الديمقراطية
جمهورية تنزانيا المتحدة
جمهورية كوريـا
جمهورية لاو الديمقراطية الشعبية
جمهورية مقدونيا اليوغوسلافية سابقاً
جمهورية مولدوفـا
جنوب أفريقيا
جورجيا
الدانمرك
دومينيكا
رواندا
رومانيـا
زامبيـا
زمبابـوي
سري لانكا
السلفـادور
سلوفاكيا
سلوفينيا
سنغافورة
السنغـال
السودان
السويد
سويسرا
سيراليون
سيشيل
شيلي
صربيا
الصين
طاجيكستان
العـراق
عُمان
غابـون
غانا
غواتيمـالا
فرنسا
الفلبيـن
فنزويلا (جمهورية-البوليفارية)
فنلندا
فيجي
فييت نام
قبـرص
قطـر
قيرغيزستان
كازاخستان
الكاميرون

الكرسي الرسولي
كرواتيـا
كمبوديـا
كنـدا
كوبا
كوت ديفوار
كوستاريكـا
كولومبيـا
الكونغو
الكويـت
كينيـا
لاتفيـا
لبنـان
لختنشتاين
لكسمبرغ
ليبيا
ليبيريـا
ليتوانيـا
ليسوتو
مالطـة
مالـي
ماليزيا
مدغشقـر
مصر
المغرب
المكسيك
ملاوي
المملكة العربيّة السعوديّة
المملكة المتّحدة لبريطانيا العظمى وآيرلندا الشماليّة
منغوليـا
موريتانيا (جمهورية- الإسلامية)
موريشيوس
موزامبيق
موناكو
ميانمـار
ناميبيـا
النرويج
النمسا
نيبال
النيجـر
نيجيريا
نيكاراغوا
نيوزيلنـدا
هايتـي
الهند
هندوراس
هنغاريـا
هولنـدا
الولايات المتحدة الأمريكية
اليابان
اليمـن
اليونان

وافق المؤتمر الخاص بالنظام الأساسي للوكالة الدولية للطاقة الذرية الذي عُقد في المقر الرئيسي للأمم المتحدة بنيويورك في ٢٣ تشرين الأول/أكتوبر ١٩٥٦ على النظام الأساسي للوكالة الذي بدأ نفاذه في ٢٩ تموز/يوليه ١٩٥٧. ويقع المقر الرئيسي للوكالة في فيينا. ويتمثّل هدفها الرئيسي في "تعجيل وتوسيع مساهمة الطاقة الذرية في السلام والصحة والازدهار في العالم أجمع".

أُلغي هذا المنشور وحلَّ محلَّه العدد (Rev. 1) No. 17-T.

العدد ١٧ من سلسلة الأمن النووي الصادرة عن الوكالة

الإرشادات التقنية

الأمن الحاسوبي في المرافق النووية

دليل مرجعي

الوكالة الدولية للطاقة الذرية
فيينا، ٢٠١٣

ملاحظة بشأن حقوق النشر

Sales and Promotion Unit
Publishing Section
International Atomic Energy Agency
Vienna International Centre
P.O. Box 100
1400 Vienna, Austria
Fax: +43 1 2600 29302
Tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/Publications/index.html

طُبِع من قِبَل الوكالة الدولية للطاقة الذرية
آذار/مارس ٢٠١٣
STI/PUB/1527
ISBN 978–92–0–642210–6
ISSN 1816–9317

تمهيد

لا يمكن، في ظل الوضع العالمي الراهن، استبعاد احتمال استخدام مواد نووية أو مواد مشعة أخرى لأغراض شريرة. وقد تصدّت الدول لهذا الخطر بانضمامها إلى التزام جماعي لتعزيز حماية هذه المواد ومراقبتها والتصدّي بفعالية لأحداث الأمن النووي. كما اتفقت الدول على تعزيز الصكوك القائمة، وصاغت صكوكاً قانونية دولية جديدة لتعزيز الأمن النووي في جميع أنحاء العالم. والأمن النووي أمر أساسي في إدارة التكنولوجيات النووية وفي التطبيقات التي تُستخدَم فيها المواد النووية أو المواد المشعة الأخرى أو تُنقَل فيها.

وتقوم الوكالة، من خلال برنامجها الخاص بالأمن النووي، بمساندة الدول من أجل إرساء منظومة أمن نووي فعالة والحفاظ عليها ودعمها. وقد اعتمدت الوكالة نهجاً شاملاً إزاء الأمن النووي. ويُقرّ هذا النهج بأن منظومة الأمن النووي الوطنية الفعالة هي تلك التي ترتكز على ما يلي: تنفيذ الصكوك القانونية الدولية ذات الصلة؛ وحماية المعلومات؛ والحماية المادية؛ وحصر المواد ومراقبتها؛ والكشف عن الاتجار بهذه المواد والتصدي لذلك؛ وخطط التصدّي الوطنية؛ وتدابير الطوارئ. وترمي الوكالة، من خلال سلسلة الأمن النووي الصادرة عنها، إلى مساعدة الدول على تنفيذ منظومة من هذا القبيل ودعمها بطريقة متماسكة ومتكاملة.

وتتألّف سلسلة الأمن النووي الصادرة عن الوكالة من 'أساسيات الأمن النووي' التي تحتوي على أهداف منظومة الأمن النووي الخاصة بالدولة وعلى عناصرها الأساسية؛ كما تتألّف من التوصيات؛ وأدلّة التنفيذ؛ والإرشادات التقنية.

وتتحمّل كلّ دولة كامل المسؤولية عن الأمن النووي، وبالأخص عمّا يلي: الترتيب لأمن المواد النووية وغيرها من المواد المشعة والمرافق والأنشطة ذات الصلة؛ وكفالة أمن هذه المواد خلال استخدامها، أو خزنها، أو نقلها؛ ومكافحة الإتجار غير المشروع والتحريك غير المقصود لهذه المواد؛ والاستعداد للتصدّي لحدث من أحداث الأمن النووي.

يندرج هذا المنشور ضمن فئة الإرشادات التقنية لسلسلة الأمن النووي الصادرة عن الوكالة، ويتناول موضوع الأمن الحاسوبي في المرافق النووية. ويقوم هذا المنشور على أساس الخبرات والممارسات الوطنية وأيضاً على أساس المنشورات الصادرة في مجالات الأمن الحاسوبي والأمن النووي. وتعرض هذه الإرشادات على الدول والسلطات المختصة والجهات المشغّلة لدراستها.

وقد تسنى إعداد هذا المنشور ضمن سلسلة الأمن النووي الصادرة عن الوكالة بفضل مساهمات عدد كبير من الخبراء من الدول الأعضاء. وقد جرت عملية استشارات مكثفة مع جميع الدول الأعضاء وشملت اجتماعات مع استشاريين واجتماعات تقنية مفتوحة العضوية. وتم بعد ذلك تعميم المسودة على جميع الدول الأعضاء لمدة ١٢٠ يوماً سعياً للحصول على مزيد من التعليقات والاقتراحات. وقد خضعت التعليقات الواردة من الدول الأعضاء للاستعراض وتمت مراعاتها في النسخة النهائية من المنشور.

ملاحظة تحريرية

لا يتناول هذا التقرير مسائل المسؤولية، سواء أكانت قانونية أو غير قانونية، عن أفعال أي شخص أو امتناعه عن الأفعال.

وعلى الرغم من الحرص الشديد على الحفاظ على دقة المعلومات الواردة في هذا المنشور، لا تتحمل الوكالة ولا دولها الأعضاء أية مسؤولية عن العواقب التي قد تنشأ عن استخدام تلك المعلومات.

ولا ينطوي استخدام تسميات معيَّنة للبلدان أو الأقاليم على أي حكم من جانب الناشر، وهو الوكالة الدولية للطاقة الذرية، بشأن الوضع القانوني لهذه البلدان أو الأقاليم، أو سلطاتها ومؤسساتها، أو تعيين حدودها.

ولا ينطوي ذكر أسماء شركات أو منتجات محددة (سواء مع الإشارة إلى أنها مسجلة أو دون تلك الإشارة) على أي نية لانتهاك حقوق الملكية، ولا ينبغي أن يفسر على أنه تأييد أو توصية من جانب الوكالة.

المحتويات

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

مقدِّمة

١-١- معلومات أساسية

خلال العقد المنصرم من الزمن، تزايد الاهتمام بالأمن الحاسوبي نظراً لبروز إثباتات جلية ومتكررة عن مواطن الضعف التي تشوب النظم الحاسوبية. وقد تكاثرت حالات الاستغلال الكيدي لمواطن الضعف هذه مخلفةً آثاراً متفاقمة. وفي تصور ذي مستوى متزايد من التعقيد للتهديدات، دفعت إمكانية حصول هجمات إرهابية افتراضية كوسيلة لمهاجمة البنى الأساسية الحيوية لدولةٍ ما عدداً من السلطات الوطنية إلى إعداد نظم دفاعية وإصدار قواعد تنظيمية جديدة. وتحدد هذه القواعد التنظيمية متطلبات الأمن الحاسوبي التي تؤثر في المرافق النووية على مستويات متعددة وخلال مختلف مراحل التشغيل. وبموازاة ذلك، تطور أمن المعلومات بحدّ ذاته تطوراً سريعاً، ممّا أتاح استحداث مجموعة ضخمة من الممارسات الفضلى والوثائق المعيارية الدولية ومن بينها سلسلة معايير المنظمة الدولية لتوحيد المقاييس واللجنة الدولية للتقنيات الكهربائية (ISO/IEC 27000) [١ - ٥] التي تتقدم بسرعة نحو تبوّأ مرتبة الصدارة.

وفيما تعترف الوكالة الدولية للطاقة الذرية (الوكالة) بصحة سلسلة معايير ISO 27000 وغيرها من المعايير الأخرى السارية في مختلف الصناعات وقطاعات الأعمال، إلاّ أنها ترغب في التركيز على الظروف الخاصة المؤثرة بالأمن الحاسوبي في المرافق النووية. من هنا، برزت الحاجة إلى منشور يعترف بصحة الإرشادات ذات الصلة والحلول الملائمة ويجمّعها. ويجمع هذا المنشور بين معارف وخبرات أخصّائيين دأبوا على تطبيق واختبار واستعراض إرشادات ومعايير الأمن الحاسوبي داخل مرافق نووية وغيرها من البنى الأساسية الحيوية. وهو يجمّع ويصف الأحكام الخاصة والممارسات الفضلى والدروس المستفادة التي تنطبق على الميدان النووي ويضعها في سياق برنامج أمني يتساوق مع غيرها من إرشادات الوكالة والمعايير الصناعية السارية.

١-٢- الغرض

١-٢-١- أهداف الأمن النووي والأمن الحاسوبي

ينطوي الأمن النووي على منع الأعمال الإجرامية أو المقصودة غير المرخّص بها المنطوية على مواد نووية أو غيرها من المواد المشعة أو المرافق المرتبطة بها أو الأنشطة المرتبطة بها وغيرها من الأعمال المقصودة التي قد تؤدي، مباشرة أو بشكل غير مباشر،

إلى حصول عواقب مضرة بالأشخاص أو الممتلكات أو المجتمع أو البيئة، كما ينطوي على الكشف عن هذه الأعمال والتصدّي لها.

ويؤدي الأمن الحاسوبي دوراً حيوياً متزايد الأهمية في سبيل ضمان تحقيق هذه الأهداف. وبالتالي، فإن هذا المنشور سيتناول موضوع إرساء وتحسين البرامج الرامية إلى حماية هذه النظم والشبكات الحاسوبية وغيرها من النظم الرقمية الضرورية لتشغيل المرفق تشغيلاً آمناً ومأموناً ولمنع أعمال السرقة أو التخريب أو غيرها من الأعمال الكيدية.

وسيتم شمل لجميع النظم الأخرى اللازمة لتشغيل المرفق، أو أي نظام دعم أو نظام أعمال يؤدي تعديله أو تغييره على نحو غير مرخّص به إلى تقويض الوضع الأمني أو إمكانية التشغيل، وذلك عن طريق توسيع نطاق الأحكام الواردة في هذا المنشور ليشمل تلك النظم.

وفي هذا السياق، يمكن تصنيف الأعمال الكيدية التي تنطوي على استخدام النظم الحاسوبية وذات الصلة بالأمن النووي ضمن الفئات التالية:

— هجمات لجمع المعلومات تهدف إلى التخطيط لمزيد من الأعمال الكيدية وتنفيذها؛
— هجمات تعطّل أو تقوّض سمات حاسوب واحد أو عدة حواسيب جوهرية لضمان أمن المرافق أو أمانها؛
— تقويض حاسوب واحد أو عدة حواسيب مقروناً مع أنماط هجومية أخرى متزامنة من قبيل الخرق المادي للمواقع المستهدفة.

يشيع تعريف أهداف الأمن الحاسوبي على أنها تهدف إلى حماية سرية خصائص البيانات الإلكترونية أو النظم والعمليات الحاسوبية، وضمان سلامتها وتوافرها. ويمكن تحقيق الأهداف الأمنية عن طريق تحديد وحماية خصائص البيانات والنظم التي قد يكون لها أثر سلبي على أمان الوظائف المنفذة في المرافق النووية وأمنها.

١-٢-٢- النطاق

يهدف هذا المنشور بشكل رئيسي إلى التوعية بشأن أهمية إرساء الأمن النووي كجزء لا يتجزّأ من الخطة الشاملة للأمن في المرافق النووية.

ويهدف المنشور أيضاً إلى تزويد المرافق النووية بإرشادات خاصة بتنفيذ برنامج للأمن الحاسوبي. ويتم تحقيق ذلك عن طريق تقديم عدد من الاقتراحات بشأن النُهُج والبنى وإجراءات التنفيذ المصممة للمرافق النووية. وتشكل هذه الأمور، فيما بينها، ضرورة

جوهرية لتحقيق مستوى الحماية المحددة في استراتيجية أمن الموقع والحفاظ عليه، وتلبية الأهداف الوطنية للأمن النووي.

ويهدف هذا الدليل المرجعي أيضاً إلى إسداء المشورة بشأن تقييم البرامج القائمة وتقدير قيمة الأصول الرقمية الحرجية وتحديد التدابير الملائمة لتقليص المخاطر.

١-٣- الشروط الخاصة بالمرافق النووية

إن الظروف الخاصة التي تميّز هذه الصناعة تدعم الحاجة إلى إرشادات تتناول الأمن الحاسوبي في المرافق النووية. وتشكل القائمة التالية نموذجاً من هذه الظروف التي سيتم تناولها بشكل كامل في هذا المنشور:

- يجب على المرافق النووية أن تمتثل للمتطلبات المحددة بواسطة هيئاتها الرقابية الوطنية والتي تقوم، مباشرة أم بشكل غير مباشر، بتنظيم النظم الحاسوبية أو وضع الإرشادات.
- ويمكن أن تضطر المرافق النووية إلى الحماية ضد تهديدات أخرى لا تتم مراعاتها عادة في الصناعات الأخرى. ويجوز أيضاً أن تتأتى هذه التهديدات عن الطبيعة الحساسة للصناعة النووية.
- ويجوز لمتطلبات الأمن الحاسوبي في المرافق النووية أن تختلف عن تلك الخاصة بالصناعات الأخرى. ولا تنطوي العمليات التجارية النموذجية سوى على نطاق محدود من المتطلبات. ويلزم للمرافق النووية أن تراعي قاعدة أوسع أو مجموعة من الاعتبارات تختلف تماماً، على سبيل المثال، عن تلك التي تؤثر على التجارة الإلكترونية أو الأعمال المصرفية أو حتى التطبيقات العسكرية. ويسلط القسم ٧ الضوء على هذه الاختلافات ويشرحها بالتفصيل.

١-٤- الهيكل

الإرشادات الواردة في هذا المنشور موجّهة إلى جمهور عريض يشمل صانعي السياسات، ورقباء الأمن النووي، ومدراء المرافق، والموظفين المكلفين بمسؤوليات أمنية، والموظفين التقنيين، والبائعين، والمقاولين. وهي تُطبق على جميع مراحل دورة حياة نظم المرفق، بما فيها نظم التصميم والتطوير والعمليات والصيانة.

وينقسم هذا المنشور إلى جزءين.

— ويهدف الجزء الأول (الأقسام ٢ إلى ٤) إلى توفير الدعم للمدراء لتمكينهم من اتخاذ آراء متوازنة وقرارات مستنيرة بشأن السياسات وبشأن تصميم وإدارة الأمن النووي داخل المرافق. وهو يقدم الإرشادات بشأن التدابير الرقابية والإدارية الخاصة بالأمن الحاسوبي.
— أمّا الجزء الثاني (الأقسام ٥ إلى ٧)، فيتناول الإرشادات التقنية والإدارية الخاصة بتنفيذ خطة شاملة للأمن الحاسوبي.

١-٥- المنهجية

إن المنهجية الأساسية المستخدمة لتنفيذ الأمن النووي تشبه المنهجيات المستخدمة لضمان الأمن والأمان النوويين. ويسلط ذلك الضوء على الحاجة إلى – والفائدة من – إدماج الأمن الحاسوبي ضمن الخطط الشاملة لأمن المرفق منذ البداية.

ويمكن تحقيق الحماية الناجحة للنظم الحاسوبية عن طريق تكييف طرائق وأدوات الممارسات الفضلى المطوّرة ضمن إطار المجتمع الأوسع للأمن الحاسوبي مع مراعاة خصوصيات الصناعة النووية.

ويبرز الإجراء المنطقي التالي، الموصوف بالتفصيل في القسم ٥، كيف يمكن لمرفق نووي أن يطور الأمن الحاسوبي وينفذه ويحافظ عليه ويحسّنه:

— الالتزام بالمتطلبات القانونية والرقابية الوطنية؛
— الاطّلاع على الإرشادات ذات الصلة الصادرة عن الوكالة والإرشادات الدولية الأخرى؛
— تأمين دعم كبار المدراء والموارد الوافية؛
— تحديد إطار محيطي للأمن الحاسوبي؛
— تعيين التفاعلات بين الأمن الحاسوبي وعمل المرفق وبين الأمان النووي وغيرها من جوانب أمن الموقع؛
— وضع سياسة خاصة بالأمن الحاسوبي؛
— إجراء تقييم للمخاطر؛
— اختيار تدابير وقائية للأمن الحاسوبي وتصميمها وتنفيذها؛
— إدماج الأمن الحاسوبي ضمن المنظومة الإدارية للمرفق؛
— إخضاع النظام بشكل منتظم للمراجعة والتنقيح والتحسين؛

سيتطرق هذا المنشور بقدر أكبر من التفصيل إلى خطوات المنهجية التي تنطوي على تدابير خاصة بالمرافق النووية. ويمكن تنفيذ مراحل أخرى من منهجية الأمن

الحاسوبي عن طريق إدراج إشارة مرجعية مباشرة إلى معايير وطنية ودولية قائمة (انظر قائمة المراجع الواردة في نهاية هذا المنشور).

١-٦- أهم المصطلحات

بما أن الكلمات تكتسب معانٍ مختلفة ضمن مجموعات ممارسة مختلفة، يتضمن هذا القسم توضيحاً لمعنى بعض المصطلحات الهامة كما هي مستخدمة في مختلف أجزاء هذا المنشور.

ففي سياق هذا المنشور، يشير مصطلحا حواسيب ونظم حاسوبية إلى أجهزة الحوسبة، والاتصالات، والتجهيزات، وأجهزة التحكم التي تشكل العناصر الوظيفية للمرفق النووي. ولا يشمل ذلك الحواسيب المكتبية والنظم المركزية ووحدات الخدمة الحاسوبية والأجهزة الشبكية فحسب، بل يضم أيضاً مكوّنات ذات مستوى أدنى من قبيل النظم المطمورة وأجهزة التحكم المنطقي القابل للبرمجة. وفي الجوهر، يتعلق هذا المنشور بجميع المكوّنات المعرضة للانتهاك إلكترونياً.

سيستخدم مصطلح **الأمن الحاسوبي**، في مختلف أجزاء هذا المنشور، ليشمل أمن جميع الحواسيب كما هي معرّفة أعلاه وكافة النظم والشبكات المترابطة المكوّنة من مجمل العناصر المعنية. ويعتبر المصطلحان **أمن تكنولوجيا المعلومات** و**أمن الفضاء الإلكتروني**، لأغراض هذا المنشور، على أنهما مرادفان للأمن الحاسوبي ولن يتم استخدامهما في هذا المنشور.

والأمن الحاسوبي، كما هو محدد هنا، هو جزء من مصطلح أمن المعلومات (كما هو محدد، على سبيل المثال، في منشور المنظمة الدولية لتوحيد المقاييس ISO/IEC 27000 [١])، علماً بأن المصطلحين يتشاطران العديد من الأهداف والمنهجيات والمصطلحات.

وترد في نهاية هذا الكتيّب تعاريف مصطلحات إضافية مستخدمة في هذا المنشور.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

الجزء الأول

دليل الإدارة

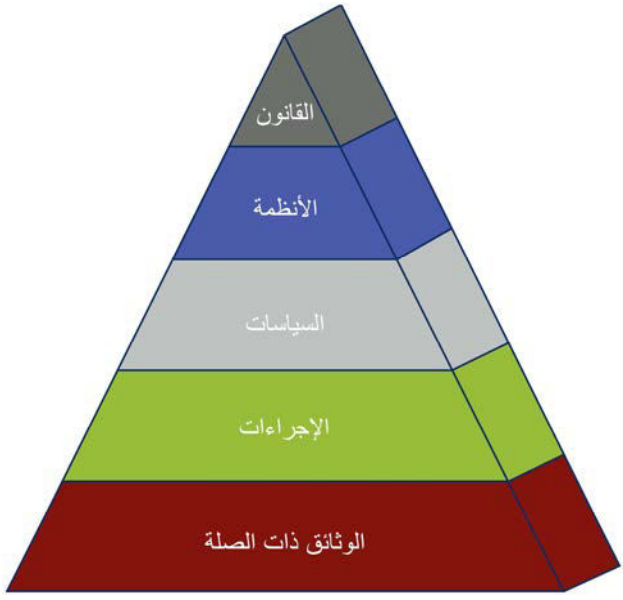
أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

٢- الاعتبارات الرقابية والإدارية

يسلط هذا القسم الضوء على المكوّنات الأساسية للإطار الرفيع المستوى للأمن الحاسوبي في المرافق النووية. وهو يتطرق، بشكل خاص، لمسائل ذات صلة بالهيئات التشريعية والرقابية، فضلاً عن إدارة المرافق واستراتيجيتها الأمنية. ويعرض الشكل ١ تصوراً مبسطاً لتراتبية الصكوك المعيارية ذات الصلة بإرساء وتنفيذ برنامج للأمن الحاسوبي في مرفق نووي.

٢-١- الاعتبارات التشريعية

وينطوي أحد الأدوار الرئيسية التي تضطلع بها الدولة على إرساء الإطار القانوني للأمن النووي بالإضافة إلى الأمن الحاسوبي بوجه عام. وينبغي لهذين الإطارين، في حال تنفيذهما بالشكل الملائم، أن يكونا ذات أثر رئيسي على أمان المرافق النووية وأمنها. وينبغي للنظام القانوني لدولة ما أن يوفّر، على الأقل، الإطار التشريعي والرقابي الذي يشمل حماية المعلومات الحساسة ويتصدّى لأي نشاط من شأنه أن يعجل حصول خروقات في الأمن النووي.



الشكل ١ – الصكوك المعيارية ذات الصلة

نظراً للطابع الخاص الذي تتسم به مسائل الأمن الحاسوبي، ربما يحتاج هذا الأخير إلى أحكام تشريعية خاصة لمراعاة الجرائم الفريدة من نوعها وأنماط التشغيل ذات الصلة بالنظم الحاسوبية. وينبغي للدول أن تتأنى في دراسة ما إذا كانت تشريعاتها الحالية تشمل بالشكل الوافي الأعمال الكيدية التي يمكن ارتكابها بمساعدة الحواسيب. ومن ضمن جملة أمور، تشمل القوانين الهامة التي قد تؤثر في الأمن الحاسوبي وفي تنفيذه ما يلي:

- القوانين المتعلقة بالجنح الحاسوبية؛
- القوانين المتعلقة بالإرهاب؛
- القوانين المتعلقة بحماية البنى الأساسية الوطنية الحرجة؛
- القوانين التي تأمر بالكشف عن المعلومات؛
- القوانين المتعلقة بالخصوصية وبالتعامل مع المعلومات الشخصية.

من الأهمية بمكان إخضاع تشريعات دولة ما للتنقيح والارتقاء الدائمين لإدراج أحكام بشأن الأنشطة الإجرامية الجديدة والناشئة وغيرها من التهديدات المحتملة المحدقة بالأمن النووي.

ونظراً لطبيعة الشبكات الحاسوبية، يمكن للخصوم أن ينفّذوا أعمالاً كيدية داخل دولة ما فيما هم قابعون خارج حدودها المادية وبالتالي يحتمل أن يبقوا بعيدي المنال بالنسبة للنظام القانوني لتلك الدولة. وفي وقت صياغة هذا المنشور، كانت اتفاقية المجلس الأوروبي بشأن الجريمة الصك القانوني الدولي الوحيد الهام المكرّس لتنظيم التعاون الدولي بشأن جرائم الإنترنت.

٢-٢- الاعتبارات الرقابية

ينبغي للهيئة الرقابية أن تراعي التشريعات ذات الصلة في توجيهاتها وتضع في متناول المشغلين الأدوات والوسائل اللازمة لتفسير وتنفيذ الالتزامات القانونية بالشكل الصحيح. ويمكن أيضاً للرقباء أن يختاروا الإرشادات المرجعية ذات الصلة أو أن يشيروا إليها، من قبيل معايير المنظمة الدولية لتوحيد المقاييس أو منشورات الوكالة الدولية للطاقة الذرية.

وينبغي لأنشطة الرقباء ذات الصلة بالأمن الحاسوبي أن تعترف صراحةً بهدف الحماية ضد سرقة المواد النووية والتخريب، ممّا قد يؤدي إلى احتمال حصول انبعاثات إشعاعية. ولذلك، فإنه ينبغي أيضاً مراعاة اللوائح المعنية بالأمن والأمان النوويين عند إعداد اللوائح المعنية بالأمن النووي.

ومن الموصى به أن تتعاون الهيئات الرقابية الحكومية فيما بينها (عندما تكون أكثر من هيئة واحدةٍ معنيةً) للتوصل إلى رؤى متساوقة بشأن المتطلبات اللازمة الواجب إرساؤها.

ويجوز للهيئات الرقابية الحكومية أن تقوم، كحد أدنى، بتوفير بيان رفيع المستوى بشأن المتطلبات الرقابية الخاصة بالأمن الحاسوبي. ويجوز أيضاً لمتطلباتٍ رقابيةٍ أكثر تفصيلاً أن تشمل أحكاماً بشأن ما يلي:

- التزام الإدارة بالأمن الحاسوبي (القسم ٤).
- ملكية برامج الأمن الحاسوبي بما يشمل تحديد أدوار مسؤول (مسؤولي) وفريق (أفرقة) الأمن الحاسوبي (القسم ٤).
- سياسة الأمن الحاسوبي وخطة تنفيذه وخطة إنفاذه (القسم ٥)، بما يشمل:
  - تحديد محيط الأمن الحاسوبي؛
  - تحديد المخاطر؛
  - استراتيجية إدارة المخاطر؛
  - برنامج التدريب والتوعية في ميدان الأمن الحاسوبي؛
  - استمرارية خطة العمليات.
- عملية المراجعة والتنقيح، سواء كانت داخلية أم خارجية أم منفّذة بواسطة الرقباء أنفسهم.

ينبغي للمتطلبات ألاّ تفرض حلولاً تقنية مفصلة لأن التطور قد يؤدي سريعاً إلى تقادم هذه التفاصيل. وبدلاً عن ذلك، يجوز للمتطلبات أن تركز على النواتج المتوقعة إذ يمكن صياغة هذه النواتج بحيث تكون أقل اعتماداً على التكنولوجيا.

ويجوز أن يُطلب من المرافق أن تبرهن عن امتثالها لمتطلبات الأمن الوطني من خلال خطة شاملة معتمدة لأمن الموقع أو أي مجموعة وثائق معادِلة. **وينبغي للهيئات الرقابية الحكومية أن تصدر متطلبات الأمن الحاسوبي كجزء من متطلبات خطة أمن المواقع.**

٢-٣- إطار أمن المواقع

تقع مسؤولية أمن المواقع بشكل أساسي على عاتق الإدارة، وبالتحديد الإدارة العليا، للتحقق من الامتثال التام للمتطلبات التشريعية والرقابية من خلال تنفيذ خطة أمن المواقع.

وتتفاعل جميع الاختصاصات الأمنية (بما فيها أمن الموظفين والأمن المادي وأمن المعلومات والأمن الحاسوبي) فيما بينها وتكمّل بعضها البعض لإرساء الوضع الأمني

لمرفق ما بحسب ما قد يتم تحديده في خطة أمن المواقع (انظر الشكل ٢). وقد يؤثر إخفاقٌ في أي من هذه الاختصاصات الأمنية على المجالات الأخرى ويؤدي إلى متطلبات إضافية مفروضة على الجوانب الأمنية المتبقية. ويشكل الأمن الحاسوبي اختصاصاً متقاطعاً يتفاعل مع جميع المجالات الأمنية الأخرى ضمن مرفق نووي.

وينبغي تطبيق جميع الأحكام الواردة في هذا المنشور مع مراعاة دائمة للإطار الأوسع نطاقاً لخطة أمن المواقع. وعلى النحو ذاته، ينبغي تصميم خطة أمن المواقع مع مراعاة الأمن الحاسوبي منذ اللحظة الأولى.

ويقع أيضاً على عاتق الإدارة ضمان التنسيق الملائم بين مختلف الاختصاصات الأمنية وإدماج الأمن الحاسوبي عند المستوى الملائم.

الشكل ٢ . التفاعل بين مختلف مجالات الأمن.

٢-٣-١- سياسة الأمن الحاسوبي

ينبغي للإدارة أن تدرك أن التكنولوجيا الحاسوبية تستخدم بشكل متزايد للاضطلاع بالعديد من الوظائف الحيوية في المرافق النووية. وقد تمخض هذا التطور عن فوائد متعددة في ميداني الأمان التشغيلي والفعالية. ولكن لضمان سلامة عمل نظامٍ حاسوبي ما، يطلب من الإدارة أن تقيم حواجز أمنية وافية ومتوازنة لتحقيق الحد الأقصى من الحماية ضد الأعمال الكيدية من دون إعاقة عمل النظام بلا داعٍ.

لذلك، ينبغي لجميع المرافق النووية أن تطبق سياسة أمن حاسوبي يدعمها وينفذها أكبر مدراء الموقع. وتحدد السياسة الأهداف الشاملة للأمن الحاسوبي في المرفق.

وينبغي لسياسة الأمن الحاسوبي أن تشكل جزءاً من السياسة الشاملة لأمن المواقع وينبغي التفاوض بشأنها وتنسيقها مع المسؤوليات الأمنية الأخرى ذات الصلة. وعند وضع سياسة للأمن الحاسوبي، ينبغي أيضاً مراعاة أثرها على الموارد القانونية والبشرية.

ويتناول القسم ٥ بقدر أكبر من التفصيل سياسة الأمن الحاسوبي والخطة المرتبطة بها.

٢-٣-٢- النظم الحاسوبية في المرافق النووية

تشمل النظم والشبكات الحاسوبية الداعمة لعمليات المرافق النووية العديد من نظم حوسبة تكنولوجيا المعلومات غير المعيارية من حيث متطلبات الهندسة أو التنسيق أو الأداء. ويجوز أن تشمل هذه النظم نظم تحكم صناعي متخصصة، ونظم تحكم بالوصول، ونظم إنذار وتعقب، ونظم معلومات ذات صلة بالأمان والأمن والتصدّي للطوارئ. وفيما انتقلت نظم التحكم الصناعي من العمليات التنفيذية ذات الملكية الخاصة الصارمة إلى استخدام الهندسة الحاسوبية العامة، ما زالت اختلافات هامة قائمة بين نظم التحكم الصناعي ونظم تكنولوجيا المعلومات المعيارية ويجب مراعاتها عند إعداد خطة أمن المواقع. ويتضمن القسم ٧ مناقشة كاملة لفرادة النظم الحاسوبية المرتبطة بالمرافق النووية.

٢-٣-٣- الدفاع في العمق

ينبغي لمتطلبات الحماية أن تعكس مفهوم الطبقات والطرائق المتعددة للحماية (بنيوية وتقنية وذات صلة بالموظفين وتنظيمية) التي يتعيّن على الخصوم أن يتغلبوا أو يتحايلوا عليها بغية التمكن من تحقيق أهدافهم.

والوسيلة الرئيسية لتجنب عواقب الخروق الأمنية أو التخفيف منها هي 'الدفاع في العمق'. ويُنَفَّذ الدفاع في العمق بشكل رئيسي من خلال الجمع بين عدد من مستويات الحماية المتتالية والمستقلة التي ينبغي لها أن تخفق أو التي ينبغي التغلب عليها قبل إلحاق الضرر بأحد النظم الحاسوبية. وفي حال إخفاق أحد مستويات الحماية أو أحد الحواجز، يحل محله المستوى أو الحاجز التالي. وعند تنفيذ الدفاع في العمق بالشكل السليم، فإنه يضمن ألا يؤدي أي إخفاق تقني أو بشري أو تنظيمي واحد إلى إلحاق الضرر بالنظام الحاسوبي، كما يكفل إلى حد كبير تضاؤل احتمال نشوء مجموعات من الإخفاقات التي قد تؤدي إلى حصول حادثات حاسوبية. وتشكل الفعالية المستقلة لمستويات الدفاع المختلفة عنصراً ضرورياً من عناصر الدفاع في العمق.

٢-٤- تقييم بيئة التهديدات

إن بيئة التهديدات المحدقة بالأمن الحاسوبي هي سيناريو سريع التغيّر والتطور. وفي حين أن برنامجاً جيداً للأمن الحاسوبي يضمن استدامته الخاصة، فإن الضوابط الخاصة القائمة حالياً ضد أكثر التهديدات تفشياً في الوقت الحاضر لا تضمن الحماية ضد التهديدات التي قد تتفشى غداً.

وينبغي للسلطة الحكومية المسؤولة أن تصدر، على أساس دوري، تقييماً للتهديدات يشمل التهديدات المحدقة بالنظم الحاسوبية، كما يشمل معلومات عن توجّهات الهجوم الحالية المرتبطة بأمن النظم الحاسوبية المستخدمة في المرافق النووية. والتهديد المحتاط له في التصميم (انظر القسم ٦–٣–١) هو إحدى الأدوات النموذجية المستخدمة لتحديد مستويات التهديد وكأساس لتطوير وضع أمني.

ومن الحيوي أن تحافظ المرافق على تقييم تهديدات نشط وجارٍ يتم إبلاغه بانتظام للإدارة والعمليات.

ويتضمن القسم ٦ وصفاً مفصلاً، ولكن غير شامل، للمصادر المحتملة للهجمات وما يرتبط بها من آليات الهجوم ذات الصلة بالمرافق النووية، وللمنهجيات المستخدمة لتقييم التهديدات وتحديدها.

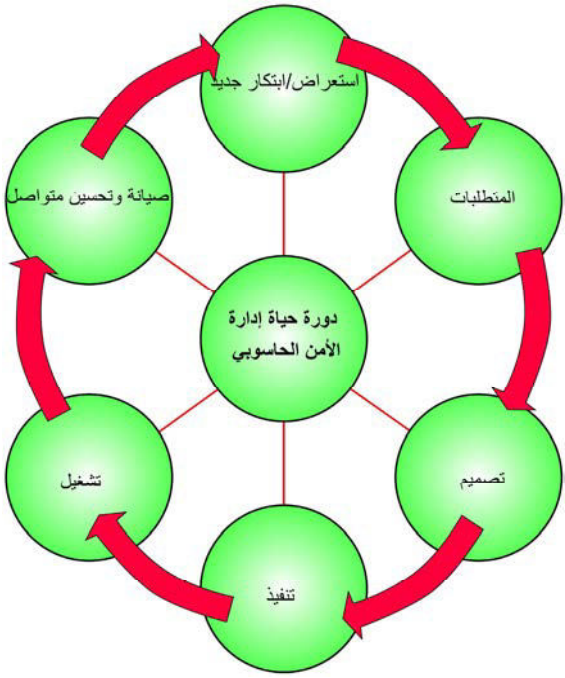
٣- نظم الإدارة

يكون نظام الإدارة مسؤولاً عن إرساء السياسات والأهداف وعن التمكين من تحقيق الأهداف بطريقة تتسم بالكفاءة والفعالية. وتشكل نظم الإدارة عامل دعمٍ حيوي لثقافة أمن نووي. فالعديد من الأنشطة المضطلع بها في المرافق النووية تخضع للتحكم بواسطة نظم الإدارة. وتجمع هذه النظم بشكل مثالي ما بين عوامل الأمن والأمان والصحة والبيئة والجودة والعوامل الاقتصادية ضمن أدارة إدارية واحدة أو ضمن مجموعة من النظم المتكاملة والتي تعزز بعضها البعض [٧، ٨].

ويجب استعراض نظم الإدارة لضمان اكتمالها وامتثالها لسياسات أمن المواقع. وبوجه أكثر عموماً، تكون نظم الإدارة بطبيعتها ديناميكية ويجب أن تتكيّف مع الظروف المتغيرة في المرفق والبيئة؛ ولا يمكن تنفيذها كإجراء ينفّذ مرة واحدة بل إنه يحتاج إلى تقييم وتحسين متواصلين. ويبرز الشكل ٣ دورة حياة العمليات الإدارية.

يهدف هذا القسم إلى تكملة الإرشادات المعنية بنظم الإدارة بالتفاصيل الضرورية لإدارة الأمن الحاسوبي. والعناصر الأساسية التي ينبغي استعراضها أو إضافتها لإدماج الأحكام الضرورية للأمن الحاسوبي هي التالية:

- تعيين أصول المعلومات وتصنيفها؛
- تحليل أساسي للمخاطر؛
- الامتثال التشريعي والرقابي؛



الشكل ٣ . دورة حياة إدارة الأمن.

- المتطلبات التشغيلية للأعمال؛
- متطلبات الكفاءة للأشخاص الأساسيين؛
- استمرارية العمل؛
- إدارة الولوج المنطقي؛
- أمن دورة حياة النظم؛
- إدارة نسق المكونات؛
- تعديل تدابير الأمن الحاسوبي والموافقة عليها؛
- تنفيذ ما تم تحديده من تدابير الأمن الحاسوبي؛
- اعتماد تدابير الأمن الحاسوبي المنفّذة؛
- الامتثال لتدابير الأمن الحاسوبي المعتمدة؛

- التحليل الفوري لحادثات الأمن الحاسوبي والتبليغ الوافي عنها؛
- التبليغ المنتظم عن حالات الامتثال؛
- استعراضات منتظمة لتدابير (مراجعات) الأمن المنفذة بواسطة أطراف داخلية وخارجية؛
- التدريب في ميدان التوعية؛
- المخاطر الجديدة والتغيّرات في المخاطر المحددة؛
- التغيّرات في المتطلبات التشريعية والرقابية؛
- خطط متوسطة الأجل لأمن المعلومات.

ينبغي اعتبار العمليات المذكورة أعلاه على أنها أنشطة جارية يتم تنفيذها في كافة مراحلة دورات حياة النظم. وينبغي إدراج تفاصيل عمليات التنفيذ في خطة الأمن الحاسوبي التي يتناولها القسم ٥.

٤- المسائل التنظيمية

٤-١- الصلاحيات والمسؤوليات

تتضمن الأقسام التالية تفاصيل المتطلبات الدنيا للإدارة والموظفين الأخصّائيين اللازمين للنجاح في إرساء برنامج للأمن الحاسوبي وصونه.

٤-١-١- الشؤون الإدارية

تستهل الإدارة العليا لمرفق ما الأمن الحاسوبي عن طريق إرساء تنظيم ملائم للعمليات والدعم. ولتحقيق ذلك، ينبغي للإدارة أن تقوم بما يلي:

- تحمل المسؤولية الشاملة لجميع جوانب الأمن الحاسوبي؛
- تحديد أهداف المرفق الأمنية؛
- ضمان الامتثال للقوانين واللوائح؛
- تحديد مستوى المخاطر المقبولة بالنسبة للمرفق؛
- إسناد المسؤوليات التنظيمية للأمن الحاسوبي؛
- ضمان التواصل الوافي بين مختلف جوانب الأمن؛
- ضمان إرساء سياسة أمن حاسوبي قابلة للإنفاذ؛
- توفير الموارد الوافية لتنفيذ برنامج أمن حاسوبي مجدٍ؛

- ضمان تنفيذ مراجعات وترقيات دورية لسياسة الأمن الحاسوبي وإجراءاته؛
- كفالة الدعم لبرامج التدريب والتوعية.

على وجه العموم، يُسند تنفيذ عملية الأمن الحاسوبي الدائمة لأخصائيين ضمن المنظمة.

٤-١-٢- مسؤول الأمن الحاسوبي

يمس الأمن الحاسوبي بكافة أنشطة المرفق تقريباً. لذلك، فمن الأهمية بمكان إسناد الإشراف الشامل على الأمن الحاسوبي إلى هيئة واحدة محددة بشكل جيد. ويُستخدم، في هذا المنشور، لقب 'مسؤول الأمن الحاسوبي'؛ وفي حالات أخرى، تجوز الإشارة إلى هذه الوظيفة بمصطلح 'مسؤول أمن تكنولوجيا المعلومات' أو 'مسؤول أمن المعلومات'، أو يجوز أن تُسند إليها أدوار متعددة. وأياً كان النهج المستخدم، ينبغي إخضاع هذه الوظيفة للتنسيق الوثيق على صعيد المرفق ككل، وينبغي إبقاؤها مستقلة عن الإدارات المنفِّذة، كما ينبغي أن تكون لها خطوط واضحة وسهلة الاستخدام لتقديم التقارير إلى الإدارة العليا.

وينبغي لمسؤول الأمن الحاسوبي أن يمتلك معارف معمّقة في ميدان الأمن الحاسوبي ودراية جيدة بالجوانب الأمنية الأخرى في المرافق النووية. وتشمل المتطلبات الإضافية المعرفة بشؤون الأمان النووي وإدارة المشاريع، والقدرة على جمع أشخاص ذوي اختصاصات مختلفة ضمن إطار فريقٍ فعّال.

وتشمل المسؤوليات النموذجية الملقاة على عاتق مسؤول الأمن الحاسوبي أو ما يعادله ما يلي:

- إسداء المشورة لإدارة الشركة بشأن الأمن الحاسوبي.
- قيادة فريق الأمن الحاسوبي.
- تنسيق أنشطة تطوير الأمن الحاسوبي والتحكم بها (من قبيل تنفيذ السياسات والتوجيهات والإجراءات والمبادئ الإرشادية والتدابير الخاصة بالأمن).
- التنسيق مع مجالات الأمن المادي وغيرها من مجالات الأمن والأمان بغية التخطيط لتدابير الأمن والتصدّي للحادثات الأمنية.
- تعيين النظم ذات الأهمية الجوهرية بالنسبة إلى الأمن الحاسوبي ضمن مرفق ما (أي خط الأساس للأمن الحاسوبي). وينبغي إبلاغ مالكي الأصول بدور معداتهم في ميدان الأمن الحاسوبي.
- إجراء تقييمات دورية لمخاطر الأمن الحاسوبي.

- إجراء عمليات تفتيش ومراجعات واستعراضات دورية لخط أساس الأمن الحاسوبي وتزويد الإدارة بتقارير عن حالة هذه العمليات.
- تطوير وتنفيذ أعمال التدريب والتقييم في ميدان الأمن الحاسوبي.
- تطوير وقيادة عمليات التصدي للحادثات في حالات طوارئ الأمن الحاسوبي ذات الصلة، بما يشمل التنسيق مع المنظمات الداخلية والخارجية المعنية.
- التحقيق في حادثات الأمن الحاسوبي وصياغة إجراءات ما بعد الحادثة والأعمال الوقائية.
- المشاركة في مبادرات تقييم أمن المواقع.
- المشاركة في تحليل المتطلبات الخاصة باقتناء/صياغة النظم الجديدة.

٤-١-٣- فريق الأمن الحاسوبي

من الجوهري أن يتاح لمسؤول الأمن الحاسوبي أن يستفيد من الخبرات المتعددة الاختصاصات المرتبطة بالأمن الحاسوبي وأمن المرافق وعمليات المحطات فضلاً عن الأمن المادي وأمن الموظفين. وقد يتكوّن ذلك من فريق أمن حاسوبي مخصص أو من إمكانية الاستفادة بشكل خاص من خبرات معيّنة ضمن إطار المنظمة. ويتمثل هدف هذا الفريق في توفير الدعم لمسؤول الأمن الحاسوبي في الوفاء بمسؤولياته.

٤-١-٤- مسؤوليات إدارية أخرى

على مختلف مستويات الإدارة ضمن منظمة ما أن تكفل المستوى الملائم من الأمن الحاسوبي، كلّ منها ضمن إطار مجالات المسؤولية المناطة به. وتشمل المسؤوليات النموذجية ما يلي:

- العمل ضمن إطار الإرشادات المنصوص عليها في خطة الأمن الحاسوبي للموقع؛
- توفير المتطلبات التشغيلية والتعقيبات إلى مسؤول الأمن الحاسوبي فيما يخص الأمن الحاسوبي وتسوية نقاط التعارض المحتملة بين المتطلبات التشغيلية ومتطلبات الأمن والأمان؛
- إبلاغ مسؤول الأمن الحاسوبي بأية ظروف قد تؤدي إلى إحداث تغييرات في وضع الأمن الحاسوبي، من قبيل التغييرات في الموظفين أو التغييرات في المعدات أو التغييرات في العمليات؛

- كفالة إخضاع الموظفين لتدريبات وافية وإعلامهم بمسائل الأمن الحاسوبي ذات الصلة بأدوارهم؛
- كفالة أن المقاولين من الباطن والباعة الخارجيين الذين يعملون لحساب الوحدة المتعاقدة يعملون ضمن سياق خطة أمن الموقع؛
- متابعة الأحداث ذات الصلة بالأمن ومراقبتها والتبليغ بشأنها؛
- إنفاذ تدابير أمن الموظفين.

٤-١-٥- مسؤوليات فردية

يكون كل شخص ضمن منظمة ما مسؤولاً عن تنفيذ خطة الأمن الحاسوبي. وتشمل المسؤوليات المُحدّدة في هذا الصدد ما يلي:

- معرفة بإجراءات خط الأساس للأمن الحاسوبي؛
- معرفة بإجراءات الأمن الحاسوبي الخاصة بوظيفة معيّنة؛
- العمل ضمن إطار معالم سياسات الأمن الحاسوبي؛
- إبلاغ الإدارة بأي تغييرات من شأنها أن تؤدي إلى تقويض وضع الأمن الحاسوبي؛
- إبلاغ الإدارة بأي حادثات واقعة أو محتملة تنطوي على تعريض الأمن الحاسوبي للخطر؛
- حضور التدريبات الأمنية الأساسية والتذكيرية على أساس منتظم.

٤-٢- ثقافة الأمن النووي

إن اعتماد ثقافة أمن حاسوبي صارمة يعتبر مكوّناً أساسياً لأي خطة أمنية فعالة. ومن المهم للإدارة أن تكفل أن الوعي بخصوص الأمن الحاسوبي مندمج تماماً ضمن ثقافة أمن الموقع الشاملة. وخصائص ثقافة الأمن النووي هي المعتقدات والمواقف والسلوك ونظم الإدارة، ويؤدي الجمع بين هذه العناصر إلى برنامج أمن نووي أكثر فعالية. ويتمثل أساس ثقافة الأمن النووي في الاعتراف – بواسطة الأفراد ذوي دور يؤدونه في تنظيم شؤون المرافق أو الأنشطة النووية أو إدارتها أو تشغيلها، أو حتى الأفراد الذين يمكن أن يتأثروا بتلك الأنشطة – بأن ثمة تهديداً موثوقاً وبأن الأمن النووي مهم. (لمزيد من المعلومات بشأن ثقافة الأمن النووي، انظر المرجع [٩].) وتشكل ثقافة الأمن الحاسوبي جزءاً من ثقافة الأمن الشامل وهي تقوم على أساس تطبيق الخصائص الواردة أعلاه على الوعي بخصوص الأمن الحاسوبي.

وقد برهنت التجارب أن غالبية حادثات الأمن الحاسوبي مرتبطة بالبشر وأن أمن أي نظام حاسوبي يتوقف بشكل كبير على سلوك جميع مستخدميه. ويقدّم المرفق الثالث أمثلة عن الأخطاء البشرية التي قد تؤدي إلى خروقات أمنية. وتُنَمّى ثقافة الأمن الحاسوبي من خلال مجموعة أنشطة عديدة مصممة لإعلام الموظفين ورفع مستوى الوعي بخصوص الأمن الحاسوبي (من قبيل الملصقات، والإشعارات، والمناقشات الإدارية، والدورات التدريبية، والاختبارات، وغيرها). وينبغي إخضاع خاصيات ثقافة الأمن الحاسوبي دورياً للدراسة والاستعراض والتحسين المتواصل. ويمكن استخدام المؤشرات التالية لتقييم ثقافة الأمن الحاسوبي في منظمة ما:

- التوثيق الواضح لمتطلبات الأمن الحاسوبي وشرحها الموظفين لضمان فهمهم الجيد لها.
- وجود إجراءات وبروتوكولات واضحة وفعالة لتشغيل النظم الحاسوبية سواء داخل المنظمة أو خارجها.
- فهم الموظفين وإدراكهم لأهمية التقيّد بالضوابط ضمن برنامج الأمن الحاسوبي.
- صيانة النظم الحاسوبية لكفالة كونها آمنة وضمان تشغيلها وفقاً لخط أساس الأمن الحاسوبي وإجراءاته.
- التزام الإدارة التام بالمبادرات الأمنية ودعمها لهذه المبادرات.

٤-٢-١- برنامج التدريب على الأمن النووي

تتمثل إحدى ركائز ثقافة الأمن الحاسوبي في اعتماد برنامج تدريبي راسخ. فمن الجوهري تثقيف الموظفين والمقاولين والباعة الخارجيين بشأن أهمية التقيّد بالإجراءات الأمنية والحفاظ على ثقافة أمنية.

وينبغي لبرنامج التوعية أن يشمل المتطلبات التالية:

- ينبغي للإكمال الناجح لبرنامج أمن حاسوبي و/أو لبرنامج توعية أن يكون شرطاً مسبقاً قبل إتاحة الوصول إلى النظم الحاسوبية. وينبغي للتدريب أن يكون متكافئاً مع مستويات أمن النظم ومع الدور المتوقع للمستخدمين.
- ينبغي توفير التدريبات/التأهيلات المعززة للأفراد ذوي المسؤوليات الأمنية الرئيسية (من قبيل مسؤول الأمن الحاسوبي، وفريق الأمن الحاسوبي، ومدراء المشاريع، ومديري تكنولوجيا المعلومات).

— وينبغي تكرار التدريب دورياً لجميع الموظفين بحيث يشمل الإجراءات الجديدة والتهديدات الناشئة.
— ينبغي أن يُطلب من الموظفين أن يقروا بأنهم يفهمون مسؤولياتهم الأمنية.

وينبغي لبرنامج التدريب أن يشمل مقاييس تتيح تقييم الوعي بشأن الأمن الحاسوبي، وفعالية التدريب، والعمليات اللازمة للتحسين المتواصل أو إعادة التدريب.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

الجزء الثاني

دليل التنفيذ

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

٥- تنفيذ الأمن الحاسوبي

لا يحدد هذا المنشور معايير دنيا للمخاطر المقبولة أو مجموعة معيّنة من التدابير التخفيفية التي يمكن استخدامها. ومن شأن أي مجموعة من المعايير الخاصة أن تتقادم بسرعة نتيجة تغيير النظم الرقمية، ونشوء تهديدات جديدة، وتوافر أدوات جديدة للتخفيف من الآثار، وتغيّر المتطلبات الرقابية. ويركّز الجزء الثاني من هذا المنشور على تجميع مجموعة من التوصيات المنهجية والملموسة لدعم وترشيد تنفيذ إجراءات الأمن الحاسوبي في المرافق النووية.

ولا تتسم هذه التوصيات بأي طابع آمر أو قطعي وينبغي استخدامها على سبيل الإرشاد؛ وحيثما كان ذلك ملائماً، يجوز اعتماد تدابير بديلة لتحقيق المستوى المرغوب من الدفاع في العمق وغيره من أهداف الأمن النووي الأساسية [١٠–١٢].

٥-١- خطط الأمن الحاسوبي وسياساته

٥-١-١- سياسة الأمن الحاسوبي

كما ورد في القسم ٢–٣–١، تحدد سياسة الأمن الحاسوبي الأهداف الرفيعة المستوى للأمن الحاسوبي في منظمة ما. ويجب على السياسة أن تفي بالمتطلبات الرقابية الملائمة. وينبغي إدراج متطلبات سياسة الأمن الحاسوبي في وثائق ذات مستوى أدنى، وستستخدم هذه الوثائق لتنفيذ السياسة وضبطها. وفضلاً عمّا تقدّم، يجب على السياسة أن تكون:

- قابلة للإنفاذ؛
- قابلة للتحقيق؛
- قابلة للمراجعة.

٥-١-٢- خطة الأمن النووي

تتمثل خطة الأمن الحاسوبي في تنفيذ تلك السياسة على شكل أدوار تنظيمية ومسؤوليات وإجراءات. وتحدّد الخطة بالتفصيل سبلَ تحقيق أهداف الأمن الحاسوبي في المرفق وهي جزء من الخطة الشاملة لأمن المواقع (أو إنها مرتبطة بها).

وينبغي للخطة أن تشمل الأنشطة الأولية من حيث إمكانية التأثر بمواطن الضعف، والتدابير الوقائية، وتحليل العواقب، وتدابير التخفيف من الآثار لإرساء وصون مستوى مقبول من المخاطر المحدقة بالمرفق النووي وتيسير العودة إلى حالة تشغيلية مأمونة.

٥-١-٣- مكوّنات خطة الأمن الحاسوبي

استناداً إلى سياسة الأمن الحاسوبي المقرّرة، يحاول كل من فرادى مكوّنات الخطة تحقيق أهدافه وأغراضه الخاصة. وتتضمن الأقسام الفرعية الواردة أدناه المحتوى الأدنى لخطة الأمن الحاسوبي كما تحدّد بنود هذه الخطة:

(أ) التنظيم والمسؤوليات
(١) الهياكل التنظيمية؛
(٢) الأشخاص المسؤولون ومسؤوليات تقديم التقارير؛
(٣) عملية الاستعراض الدوري والاعتماد.
(ب) إدارة الأصول:
(١) قائمة بجميع النظم الحاسوبية؛
(٢) قائمة بجميع تطبيقات النظم الحاسوبية؛
(٣) رسم بياني للشبكة بما يشمل جميع الوصلات التي تربط الشبكة بنظم حاسوبية خارجية.
(ج) تقييم المخاطر ومواطن الضعف والامتثال:
(١) الطابع الدوري لعمليات استعراض خطة الأمن وإعادة تقييمها؛
(٢) التقييم الذاتي (بما يشمل إجراءات اختبار الاختراق)؛
(٣) إجراءات المراجعة وتعقب أوجه القصور وتصحيحها؛
(٤) الامتثال الرقابي والتشريعي.
(د) تصميم أمن النظم وإدارة النُسُق:
(١) المبادئ الأساسية للهندسة والتصميم؛
(٢) المتطلبات ذات الصلة بمستويات الأمن المختلفة؛
(٣) إضفاء الطابع الرسمي على متطلبات الأمن الحاسوبي لفائدة المورّدين والباعة؛
(٤) الأمن على مدى دورة الحياة.
(هـ) إجراءات الأمن التشغيلي:
(١) التحكم بالوصول؛
(٢) أمن البيانات؛
(٣) أمن الاتصالات؛

(٤) أمن المنصات والتطبيقات (التصليد مثلاً)؛
(٥) مراقبة النظم؛
(٦) صيانة الأمن الحاسوبي؛
(٧) التعامل مع الحادثات؛
(٨) استمرارية العمل؛
(٩) حفظ نسخ عن النظم لأغراض الطوارئ.
(و) إدارة شؤون الموظفين؛
(١) التدقيق؛
(٢) التدريب؛
(٣) التأهيل؛
(٤) الإنهاء/النقل.

توفّر البنود الواردة أعلاه إطاراً لصياغة خطة أمن حاسوبي. وتتوافر مراجع عديدة لملء هذا الإطار، علماً بأن أهم المراجع الدولية هي تشمل الوثيقة ISO/IEC 27001 [٢] بالنسبة لنظم إدارة أمن المعلومات، والوثيقة ISO/IEC 27002 [٣] بالنسبة للتوصيات الخاصة بالتنفيذ.

وفيما تتساوق غالبية المكوّنات المدرجة أعلاه في مختلف خطط الأمن الحاسوبي الخاصة بأي شركة أو صناعة، فإن هناك فوارق معيّنة بالنسبة لتطبيقها ضمن المرافق النووية. ويتضمن القسم ٧ وصفاً أكثر تفصيلاً لمكوّنات خطة الأمن الحاسوبي هذه. ويتناول القسم ٦ مواضيع تقييم المخاطر ومواطن الضعف وحالات الامتثال. أمّا تحليل الأصول فيرد بقدر أكبر من التفصيل في القسم ٥–٣.

٥-٢- التفاعل مع سائر مجالات الأمن

كما ورد في القسم ٢–٣، ينبغي تفعيل خطة الأمن الحاسوبي وصونها ضمن إطار الخطة الشاملة للحماية الخاصة بالمرفق. وينبغي صياغة خطة أمن نووي خاصة بالمرفق المعني بالتشاور الوثيق مع أخصائيين في الحماية المادية، والأمان، والعمليات، وتكنولوجيا المعلومات. ويجب إخضاع خطة الأمن الحاسوبي للاستعراض والترقية الدوريين بغية إبراز الأحداث الأمنية الناشئة عن أي مجال من مجالات الأمن والخبرات التشغيلية الناشئة عن نظام أمن الموقع.

٥-٢-١- الأمن المادي

ينبغي لخطة الأمن المادي وخطة الأمن الحاسوبي أن تتكاملا فيما بينهما. فالأصول المحوسبة تخضع لمتطلبات خاصة بالتحكم بالوصول المادي إليها، وفي المقابل، يمكن للانتهاكات الإلكترونية أن تؤدي إلى تضرر أو فقدان عدد من وظائف الحماية المادية. ويمكن لتصورات الهجوم أن تشمل التنسيق بين الهجمات الإلكترونية والهجمات المادية. وينبغي للفريق المسؤول عن خطة الأمن المادي وذاك المسؤول عن خطة الأمن الحاسوبي أن يتبادلا المعلومات وينسّقا الجهود لكفالة اتساق الخطتين خلال عملية الصياغة والاستعراض.

٥-٢-٢- موظفو الأمن

إلى جانب الوعي والتدريب، ثمة جوانب أمنية أخرى – يتم التعامل معها عادة ضمن نطاق أمن الموظفين – أساسية لإرساء أمن حاسوبي راسخ. وينبغي للإدارتين المعنيتين بالأمن الحاسوبي وبأمن الموظفين أن تنسّقا، فيما بينهما، التدابير الضرورية لإرساء مستوى ملائم من التدقيق، ومن تعهّدات الحفاظ على السرية، ومن إجراءات الإنهاء، ولتحديد الكفاءات الوظيفية المطلوبة. وبشكل خاص، قد يتطلب الموظفون ذوو المسؤوليات الأمنية الرئيسية (مديرو النظم والفريق الأمني) مستوىً أعلى من التدقيق.

٥-٣- تحليل الأصول وإدارتها

قد يؤثر التفاعل بين النظم الحاسوبية في المرافق النووية على الأمن بطرق غير جلية. لذلك فمن المهم أن تحدد خطة الأمن *جميع الأصول* وأن تشمل *جرداً أكثر شمولاً لتلك الأصول ذات الأهمية الجوهرية بالنسبة لوظائف الأمن والأمن في المرفق*. ويمكن لهذا الجرد أن يشمل بياناتٍ ونظماً حاسوبية وواجهاتها البينية ومالكيها.

وتلبّي المنهجية التالية الاحتياجات الواردة أعلاه:

(أ) ينبغي تجميع معلومات ذات صلة بشأن النظم الحاسوبية القائمة بغية وضع قائمة كاملة للأصول؛

(ب) ينبغي تعيين أوجه الترابط بين الأصول المحدّدة؛

(ج) ينبغي تحديد وتقييم الصلة بالوظائف الأمنية ونظم الأمان المحددة، والنظم ذات الصلة بالأمان، ونظم الأمن.

ويشكل اكتمال كل خطوة شرطاً مسبقاً جوهرياً لتنفيذ الخطوات التالية.

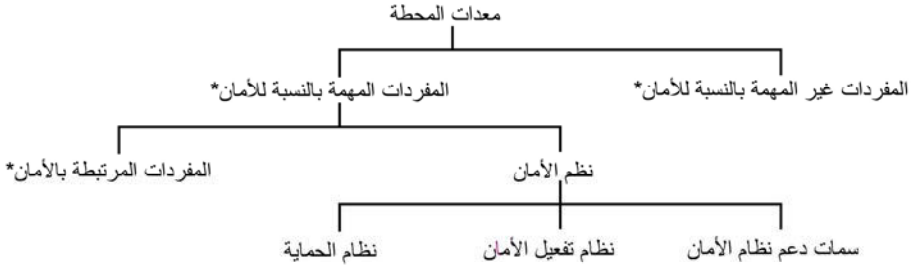
ويشمل التحليل الشامل للنظم الحاسوبية في مرفق نووي ما يلي:

- الوظائف/المهام والأنماط التشغيلية لكافة النظم المحوسبة القائمة؛
- تحديد أوجه الترابط ذات الصلة، بما يشمل إمدادات الطاقة؛
- تحليل تدفق البيانات، لمعرفة ما الذي يتواصل مع ماذا، وكيف ولماذا؛
- الإجراءات التي تستهل الاتصالات وتواتر هذه الاتصالات والبروتوكولات؛
- مواقع النظم الحاسوبية والمعدات؛
- تحليل مجموعات المستخدمين؛
- الملكية (للبيانات والنظم المحوسبة)؛
- المستوى الأمني المناظر (انظر القسم ٥–٥، النهج التدرجي).

ويفترض أن الكثير من المعلومات اللازمة للتحليل متوافرة فعلاً ولكن ينبغي تجميعها ومقارنتها وتنظيمها. وتشمل مصادر المعلومات ذات الصلة مواصفات النظم ووثائقها.

٥-٤- تصنيف النظم الحاسوبية

كما ورد في القسم ١–٦، ففي سياق هذا المنشور، يشير مصطلحا حاسوب ونظم حاسوبية إلى أجهزة الحوسبة، والاتصالات، والتجهيزات، وأجهزة الاستشعار التي تشكل العناصر الوظيفية للمرفق النووي. والوظائف الحاسوبية التي تسترعي الاهتمام الأقصى هي عمليات التحكم ومعالجة البيانات المرتبطة بالأمان والأمن. وقد تشكل وظائف حاسوبية أخرى شواغل على صعيد توفير الدعم لهذه الوظائف، أو التقويض المحتمل للأمن عبر آثار ثانوية أو غير مباشرة، أو الإنتاجية الشاملة للمحطة.



* في هذا السياق، يشير المصطلح 'مفردة' إلى *هيكل أو نظام أو مكون*.

الشكل ٤ – معدات المحطة وفقاً لوظيفتها في ميدان الأمان.

وفيما يلي قائمة غير مستنفذة بالنظم الحاسوبية التي قد تحتوي عليها المرافق النووية، والتي هي ذات صلة بأغراض هذه الإرشادات. وقد تم تصنيفها بشكل منفصل وفقاً لأهميتها بالنسبة للأمان وأهميتها بالنسبة للأمن. وينبغي مراعاة كلا هذين التصنيفين عند تحديد المستوى الأمني الملائم الواجب تطبيقه (القسم ٥-٥) وفي تحليل تقييم المخاطر (القسم ٦–٢). وتجدر الإشارة أيضاً إلى أن بعض الوظائف تتداخل بشكل واضح لتشكل شواغل في ميداني الأمان والأمن معاً.

٥-٤-١- الأهمية بالنسبة للأمان

تصنف معايير أمان الوكالة (المراجع [١٣ – ١٥] على سبيل المثال) معدات المرافق النووية وفقاً لوظائفها، وفقاً لما هو مبيّن في الشكل ٤.

معدات المحطات

- *نظم ذات أهمية بالنسبة للأمان*
  - نظم الأمان
    - نظم الوقاية: نظم الأجهزة والتحكم المستخدمة لما يتم إطلاقه أوتوماتيكياً من أنشطة حماية المفاعل والمحطة.
    - نظم تفعيل الأمان: نظم الأجهزة والتحكم التي تنفّذ أنشطة أمان والتي يتم إطلاقها بواسطة نظم الحماية والتفعيلات اليدوية.
    - سمات داعمة لنظام الأمان: أجهزة وتحكم لنظم احتياطية للإمداد بالكهرباء.
  - نظم متعلقة بالأمان
    - نظم تحكم بالعمليات: نظم أجهزة وتحكم للتحكم بالمحطة.
    - أجهزة وتحكم لغرفة التحكم بما يشمل نظم الإنذار.
    - نظم حاسوبية للعمليات تجمع وتحضّر المعلومات لغرفة التحكم.
    - نظم أجهزة وتحكم لمناولة الوقود وخزنه.
    - نظم الوقاية من الحرائق.
    - نظم التحكم بالوصول.
    - بنية أساسية للاتصالات بالصوت والبيانات.
    - نظم غير مهمة بالنسبة للأمان.
  - نظم تحكم للوظائف غير المهمة بالنسبة للأمان (كإزالة المعادن مثلاً)

وينبغي أيضاً إيلاء الاعتبار للنظم الحاسوبية التي لا تقع بالضرورة ضمن نطاق معدات المحطة ولكنها قد تؤثر، على الرغم من ذلك، على الأمان.

المعدات غير الموجودة في المحطة

— ميكنة العمليات المكتبية

- نظم إجازة العمل ونظم أوامر العمل: نظم تستخدم لتنسيق أنشطة العمل بغية تأمين بيئة عمل سليمة.
- نظم الهندسة والصيانة: نظم لمناولة تفاصيل تشغيل المحطة وصيانتها ودعمها التقني.
- نظم إدارة نسق الحواسيب: نظم مخصصة لمتابعة شؤون أنساق المحطة بما يشمل النماذج والصيغ والأجزاء المركّبة في المرفق النووي.
- نظم إدارة الوثائق: نظم مستخدمة لخزن واسترجاع المعلومات الخاصة بالمحطة، من قبيل الرسوم ومحاضر الاجتماعات.
- شبكة إنترانت الداخلية: نظم تتيح الوصول إلى جميع الوثائق الخاصة بالمحطة – التقنية والإدارية على حد سواء – على أساس الحاجة إلى المعرفة. ويكون الوصول في العادة للقراءة فقط.

— التوصيل الخارجي

- البريد الإلكتروني: نظام مستخدم لنقل المعلومات إلى أطراف خارجية.
- موقع الويب العام: نظام مستخدم لتزويد مستخدمي الإنترنت بمعلومات بشأن المرفق.
- الوصول عن بعد/وصول الأطراف الآخرين: نظم تتيح الوصول إلى بعض الوظائف في موقع ما من الخارج بشكل خاضع لتحكم صارم.

٥-٤-٢- النظم الأمنية أو النظم المتصلة بالأمن

لا يتوافر بعد أي تصنيف أمني ثابت لنظم الأمن بما يشبه تصنيف الأمان. ولكن ينبغي أن يشكل هذا التصنيف جزءاً هاماً من عملية تحليل الأصول بغية تجميع المعلومات اللازمة لوضع تصنيف للنظم الموجودة في المرفق. ويمكن للقائمة التالية أن تدعم تصنيفاً من هذا النوع:

- نظم تحكم بالوصول المادي: نظم مستخدمة للتحقق من أن الأشخاص المرخص لهم فقط قادرون على دخول مناطق الموقع تتلاءم مع الوظيفة التي يؤدونها؛
- بنية أساسية للاتصالات بالصوت والبيانات؛
- قاعدة بيانات التصاريح الأمنية: تستخدم للتحقق من أن الأشخاص يحملون التصاريح الأمنية الملائمة للتمكن من الوصول إلى جزء من الموقع أو إلى معلومات محفوظة في الموقع؛
- نظم لمراقبة الإنذارات الأمنية والتحكم بها: تستخدم لمراقبة جميع الإنذارات الأمنية في الموقع وللمساعدة في تقييم الإنذار؛
- مكونات الأمن الحاسوبي والشبكي؛
- نظم الحصر والتحكم النوويين.

٥-٥- نهج تدرّجي إزاء الأمن الحاسوبي

ينبغي لأمن النظم الحاسوبية أن يقوم على أساس نهج تدرّجي يتم بموجبه تطبيق تدابير الأمن بالتناسب مع العواقب المحتملة لهجوم ما. ويتمثل أحد الأغراض العملية للنهج التدرّجي في تصنيف النظم الحاسوبية ضمن *مناطق*، بحيث يتم تطبيق المبادئ الوقائية التدرّجية على كل من المناطق على أساس *مستوى* المتطلب الأمني المخصص للمنطقة المعنية. وتوزيع النظم الحاسوبية على مستويات ومناطق مختلفة ينبغي أن يتم على أساس صلتها بالأمان والأمن (انظر الفقرة ٥–٤). ولكن **ينبغي إتاحة المجال لعملية تقييم المخاطر أن تقدم تعقيبات على النهج التدرّجي وتؤثّر عليه**.

٥-٥-١- مستويات الأمن

مستويات الأمن هي مفهوم تجريدي يحدد درجات الحماية الأمنية المطلوبة لمختلف النظم الحاسوبية في مرفق ما. وسيتطلب كل مستوى من مستويات النهج التدرّجي مجموعةً مختلفة من التدابير الوقائية للوفاء بالمتطلبات الأمنية الخاصة بذلك المستوى. وينطبق بعض التدابير الوقائية على جميع النظم الحاسوبية أياً كان مستواها، فيما تكون تدابير أخرى مخصصة لمستوى معيّن (مستويات معيّنة).

يتيح نموذج المستويات الأمنية تسهيل إسناد التدابير الوقائية لنظم حاسوبية مختلفة استناداً إلى تصنيف النظام (إسناده إلى مستوى ما) وتحديد مجموعة التدابير الوقائية الملائمة لذلك المستوى.

وينبغي لخطة الأمن الحاسوبي أن تتضمن توثيقاً ملائماً للمستويات وللتدابير الوقائية المرتبطة بها.

٥-٥-٢- المناطق

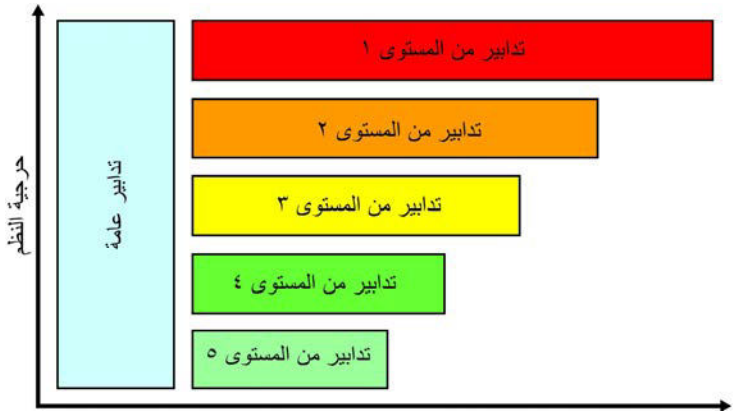
تشكل المناطق مفهوماً منطقياً ومادياً لجمع النظم الحاسوبية لأغراض الإدارة والتواصل وتطبيق التدابير الوقائية. ويتيح نموذج المناطق ضم الحواسيب ذات المستوى نفسه من الأهمية أو ذات مستوى مشابه من الأهمية من حيث التشغيل المأمون والآمن للمحطة ضمن مجموعة واحدة لأغراض الإدارة وتطبيق التدابير الوقائية.

وينبغي لتطبيق أحد نماذج المناطق أن يمتثل للمبادئ الإرشادية التالية:

- كل منطقة تتضمن نظماً لديها الأهمية ذاتها أو أهمية مشابهة بالنسبة إلى أمن المرفق وأمانه؛
- لدى النظم التابعة لمنطقة واحدة متطلبات مشابهة فيما يخص التدابير الوقائية؛
- تبني النظم الحاسوبية المختلفة التابعة لمنطقة واحدة مجالاً موثوقاً للتواصل الداخلي ضمن تلك المنطقة؛
- تتطلب حدود المناطق آليات فصل لتدفق البيانات على أساس سياسات تتوقّف على المناطق؛
- يمكن تقسيم المناطق إلى مناطق ثانوية بغية تحسين الأنساق.

لما كانت المناطق مكوّنة من نظم لديها الأهمية ذاتها أو أهمية مشابهة بالنسبة إلى أمان المرفق وأمنه، يمكن أن يُسند لكل منطقة مستوى معيّن يشير إلى التدابير الوقائية الواجب تطبيقها على جميع النظم الحاسوبية في تلك المنطقة. ولكن العلاقة بين المناطق والمستويات ليست متساوية؛ فيمكن إسناد مستوى واحد لعدة مناطق عندما تتطلب مناطق متعددة الدرجة ذاتها من الحماية. والمناطق هي تجميع منطقي ومادي لنظم حاسوبية، فيما تمثل المستويات درجة الحماية المطلوبة.

وينبغي لخطة الأمن الحاسوبي أن تتضمن توثيقاً ملائماً لنموذج المناطق، بما يشمل لمحة شاملة عن جميع النظم الحاسوبية، وجميع خطوط التواصل ذات الصلة، وجميع المعابر بين المناطق، وجميع التوصيلات الخارجية.



الشكل ٥ – مستوى الأمن/شدة التدابير.

٥-٥-٣- مثال عن تطبيق أحد نماذج المستويات الأمنية

يرد في ما يلي مثال عن التدابير الأمنية المطبقة في مستويات مختلفة. وهذا مجرد تنفيذ واحد ممكن للنهج التدرّجي؛ وينبغي تكييف الخيار الدقيق للمستويات والتدابير الأمنية المكوّنة لها وفقاً للبيئة المعنية، ولخصائص المرفق، ولتحليل المخاطر الأمنية المكرّس.

وفي هذا التنفيذ:

- ينبغي تطبيق مستوى عام من التدابير على جميع النظم الحاسوبية.
- مستويات الأمن تتراوح من المستوى ٥ (أقل مستوى من الحماية اللازمة) إلى المستوى ١ (أعلى مستوى من الحماية اللازمة)، وفقاً لما يرد في الشكل ٥.
- التدابير المناظرة لكل مستوى ليست تراكمية (وبالتالي، فقد تحصل تكرارات).

المستوى العام

للنظم والمستويات المعنية، ينبغي تطبيق التدابير العامة التالية:

- تحديد السياسات والممارسات لكل مستوى.
- صياغة الإجراءات الأمنية الخاصة بالتشغيل لفائدة جميع المستخدمين وقراءتها بواسطتهم جميعاً.

- تمتع الموظفين المجاز لهم الوصول إلى النظام بالمؤهلات والخبرات الملائمة وحملهم للتصاريح الأمنية اللازمة حسب الاقتضاء.
- عدم تمكين المستخدمين من الوصول، داخل النظم المعنية، سوى إلى الوظائف التي تلزمهم للاضطلاع بمهامهم.
- إرساء الضوابط الملائمة للتحكم بالوصول والتحقق من هوية المستخدمين.
- إرساء نظم أو إجراءات الكشف عن الحالات الشاذة.
- مراقبة مواطن الضعف في التنفيذ وفي النظم، واتخاذ التدابير الملائمة.
- التنفيذ الدوري لعمليات تقييم مواطن الضعف التي تشوب النظام.
- وجوب التحكم بالوسائط القابلة للنقل وفقاً لإجراءات الأمن الخاصة بالتشغيل.
- الصون الصارم لمكوّنات الأمن الحاسوبي والشبكي.
- التسجيل والمراقبة الصارمان لمكونات الأمن الحاسوبي والشبكي (من قبيل البوابات الأمنية، ونظم الكشف عن حالات التطفل، ونظم مكافحة حالات التطفل، وخوادم الشبكة الافتراضية الخاصة VPN[1]).
- إرساء إجراءات ملائمة لحفظ نسخ طوارئ/استعادة بيانات.
- تقييد الوصول المادي إلى المكوّنات والنظم وفقاً لوظائفها.

المستوى ١

إلى جانب التدابير العامة، ينبغي استخدام التدابير الوقائية من المستوى ١، من قبيل نظم الحماية، لحماية النظم ذات الأهمية الحيوية بالنسبة للمرفق والتي تتطلب أعلى مستوى من الأمن. ويمكن لهذه التدابير أن تشمل ما يلي:

- ينبغي عدم السماح لأي تدفقات بيانات مشبّكة أياً كان نوعها (كالإشعارات والإشعارات) من نظم ذات مستويات أمنية أضعف بدخول نظم المستوى ١. ولا ينبغي السماح سوى بالاتصالات الخارجة فقط. وتجدر الإشارة إلى أن هذا النوع من الاتصالات الصارمة الأحادية الجانب لا يكفل، بمفرده، الموثوقية والسلامة (ويمكن النظر في إنشاء نظم احتياطية/عمليات تصحيح الأخطاء). وتجدر الإشارة أيضاً إلى أن هذا يستبعد الاعتماد على أي نوع من بروتوكولات 'المصافحة' (بما فيها بروتوكول TCP/IP[2])، حتى ضمن إطار توجيهات اتصالات خاضعة للتحكم. وينصح بشدة عدم السماح بأي استثناءات ولا يجوز

[1] الشبكة الافتراضية الخاصة هي شبكة مبنية باستخدام وسائل الاتصالات العامة للربط بين المحطات الفرعية وهي مجهزة بآليات تشفير وآليات أمنية أخرى للتحقق من أن المستخدمين المرخص لهم وحدهم قادرون على الوصول إلى الشبكة ومن عدم إمكانية اعتراض البيانات.

[2] بروتوكول مراقبة الإرسال/بروتوكول إنترنت – بروتوكولات إرسال البيانات.

النظر فيها سوى على أساس كل حالة على حدة، على أن تكون مدعّمة بتبرير كامل وبتحليل للمخاطر الأمنية.[٣]

- شرح التدابير الكفيلة بضمان سلامة النظم ولياقتها التشغيلية كجزء من حالات الأمان.
- عدم السماح بأي وصول عن بعد لأغراض الصيانة.
- التحكم الصارم بالوصول المادي إلى النظم.
- إبقاء عدد الموظفين المجاز لهم بالوصول إلى النظم عند أدنى حد ممكن.
- تطبيق قاعدة الشخصين لأي تعديلات معتمدة يتم تنفيذها ضمن النظم الحاسوبية.
- حفظ سجلات بجميع الأنشطة ومراقبتها.
- الموافقة على كل عملية إدخال بيانات في النظم والتحقق منها على أساس كل حالة على حدة.
- تطبيق إجراءات تنظيمية وإدارية صارمة على أي تعديلات، بما فيها عمليات صيانة الأجهزة والارتقاء بها والتعديلات المُدخلة على البرامج الحاسوبية.

المستوى ٢

إلى جانب التدابير العامة، ينبغي استخدام التدابير الوقائية من المستوى ٢، من قبيل نظم التحكم التشغيلي، لحماية النظم التي تتطلب مستوى عالٍ من الأمن. ويمكن لهذه التدابير أن تشمل ما يلي:

- عدم السماح سوى بتدفق مشبّك للبيانات نحو الخارج، باتجاه واحد، من نظم المستوى ٢ إلى نظم المستوى ٣. وحدها رسائل الإشعارات الضرورية أو رسائل الإشارات الخاضعة للتحكم يمكن قبولها في الاتجاه المعاكس (نحو الداخل) (بالنسبة إلى TCP/IP مثلاً).
- إجازة السماح بالوصول عن بعد لأغراض الصيانة على أساس كل حالة على حدة، ولفترة عمل محددة. وعند القيام بذلك، يجب حماية النظم بواسطة تدابير مشددة، كما أن على المستخدمين الالتزام بسياسة أمنية محددة (تعاقدية).
- إبقاء عدد الموظفين الحاصلين على إذن بالوصول إلى النظام عند حدّه الأدنى، مع إرساء تمييز دقيق بين المستخدمين والموظفين الإداريين.

[٣] بعض الدول الأعضاء تشعر بشدة أنه ينبغي عدم السماح بأي استثناءات مهما كانت الحالة.

- التحكم بشكل صارم بالتوصيلات المادية بالنظم.
- التحقق من اتخاذ جميع التدابير المعقولة لكفالة سلامة النظم ولياقتها التشغيلية.
- قد يؤدي تقييم مواطن الضعف المنطوي على إجراءات تؤثر في النظم إلى عدم استقرار المحطة أو العمليات المعنية، وينبغي بالتالي عدم التفكير في القيام به سوى عند استخدام قيعان اختبارات، أو نظم احتياطية، أو خلال اختبارات القبول في المصنع، أو خلال فترات الانقطاع الطويلة المخطط لها.

المستوى ٣

إلى جانب التدابير العامة، ينبغي استخدام التدابير الوقائية من المستوى ٣ لنظم الإشراف الآني غير المطلوبة للعمليات، من قبيل نظم الإشراف الآني على العمليات في إحدى قاعات التحكم، ذات مستوى متوسط من الخطورة حيال التهديدات الإلكترونية المتنوّعة. ويمكن لهذه التدابير الوقائية أن تشمل ما يلي:

- عدم السماح بالوصول إلى الإنترنت من نظم المستوى ٣.
- مراقبة السجلات وإجراءات المتابعة الخاصة بالموارد الرئيسية.
- تنفيذ بوابات أمنية لوقاية هذا المستوى من حركة المرور غير الخاضع للتحكم من جانب نظم المستوى ٤، والسماح فقط بأنشطة معيّنة ومحدودة.
- التحكم بالتوصيلات المادية بالنظم.
- إتاحة الوصول عن بعد لأغراض الصيانة على أساس كل حالة على حدة، شرط إخضاع هذا الوصول لرقابة صارمة؛ ويجب على الحاسوب البعيد ومستخدمه أن يلتزما بالسياسة الأمنية المحددة، التي يتم الاتفاق عليها بموجب عقد.
- التحكم بوظائف النظم المتاحة للمستخدمين من خلال آليات تحكم بالوصول، وعلى أساس مبدأ الحاجة إلى المعرفة. ويجب إخضاع أي شذوذ عن هذا المبدأ للدراسة المتأنية، كما ينبغي كفالة الحماية باستخدام وسائل أخرى (كالوصول المادي مثلاً).

المستوى ٤

إلى جانب التدابير العامة، ينبغي اعتماد تدابير المستوى ٤ لنظم إدارة البيانات التقنية المستخدمة لأغراض إدارة أنشطة الصيانة أو التشغيل المرتبطة بالمكونات أو النظم المطلوبة بموجب المواصفات التقنية للتشغيل (مثل رخصة العمل، وأمر العمل، والفصل

التـام للـنظم، وإدارة الوثـائق)، ذات مسـتوى أمنـي معتـدل حيـال التهديـدات الإلكترونيـة المتنوّعة. وتشمل تدابير المستوى ٤ ما يلي:

- عـدم السـماح بإدخـال تعـديلات علـى الـنظم سـوى للمسـتخدمين المعتمـدين والمؤهلين وحدهم.
- إجـازة إتاحـة الوصـول إلـى الإنترنـت مـن نظـم المستوى ٤ للمستخدمين علـى شرط تطبيق تدابير وقائية وافية.
- تنفيـذ بوابـات أمنيـة لحمايـة هـذا المسـتوى مـن حركـة البيانـات غيـر الخاضـعة للتحكم من جانب شبكات شركة خارجية أو موقع خـارجي، والسماح بالأنشطة الخاصة الخاضعة للتحكم.
- التحكم بالتوصيلات المادية بالنظم.
- السـماح بالوصـول عـن بعـد لأغـراض الصـيانة والـتحكم بـه؛ ويجـب علـى الحاسـوب البعيـد ومسـتخدمه أن يلتزمـا بالسياسـة الأمنيـة المحـددة، التـي يـتم الاتفاق عليها والتحكم بها بموجب عقد.
- التحكم بوظـائف النظم المتاحـة للمستخدمين من خـلال آليات تحكم بالوصـول. ويجـب إخضـاع أي شـذوذ عـن هـذا المبـدأ للدراسـة المتأنيـة، كمـا ينبغـي كفالـة الحماية باستخدام وسائل أخرى.
- إتاحـة الوصـول الخـارجي عن بعد للمستخدمين المعتمدين شرط تطبيق آليات وافية للتحكم بالوصول.

المستوى ٥

ينبغـي اسـتخدام تـدابير المسـتوى ٥ للـنظم التـي لا تتسـم بأهميـة مباشـرة فيمـا يخـص التحكم التقني أو الأغراض التشغيلية، من قبيل نظم الأتمتة المكتبية، ذات مستوى منخفض من الخطورة حيال التهديدات الإلكترونية المتنوعة. وتشمل تدابير المستوى ٥ ما يلي:

- عـدم السـماح بإدخـال تعـديلات علـى الـنظم سـوى للمسـتخدمين المعتمـدين والمؤهلين وحدهم.
- إتاحة الوصول إلى الإنترنت من نظم المستوى ٥ شرط تطبيق تدابير وقائية وافية.
- إتاحـة الوصـول الخـارجي عن بعد للمستخدمين المرخص لهم شرط تطبيق ضوابط وافية.

٥-٥-٤- مناطق منع التقارن

حدود المناطق المختلفة تتطلب آليات لمنع التقارن فيما يخص تدفق البيانات من أجل الحؤول دون حالات الوصول غير المرخص بها، وأيضاً لتفادي تفشّي الأخطاء من منطقة ذات متطلبات وقائية دنيا إلى منطقة أخرى ذات متطلبات وقائية أعلى.

والتدابير التقنية والإدارية التي تكفل عدم التقارن بين المناطق يجب أن تُكيّف وفقاً للمتطلبات الفردية الخاصة بالمستويات الوقائية. وينبغي عدم السماح بوجود ممر توصيلي مباشر يربط ما بين عدة مناطق.

٦- إدارة التهديدات ومواطن الضعف والمخاطر

تعرض الفقرة أدناه المفاهيم الأساسية المستخدمة في إدارة المخاطر المرتبطة بالنظم الحاسوبية. تتسم إدارة المخاطر بالأهمية بالنسبة لجميع مراحل دورة حياة نظم المرفق، بما فيها نظم التصميم والتطوير والعمليات والصيانة. وتقدم الفقرة ٦–٢ لمحة شاملة عن الخطوات الضرورية في منهجية شاملة لإدارة المخاطر. أمّا الفقرتان ٦–٣ و٦–٤، فتركّزان على المراحل التي تتميّز فيها الصناعة النووية بخصائص معيّنة.

٦-١- المفاهيم والعلاقات الأساسية

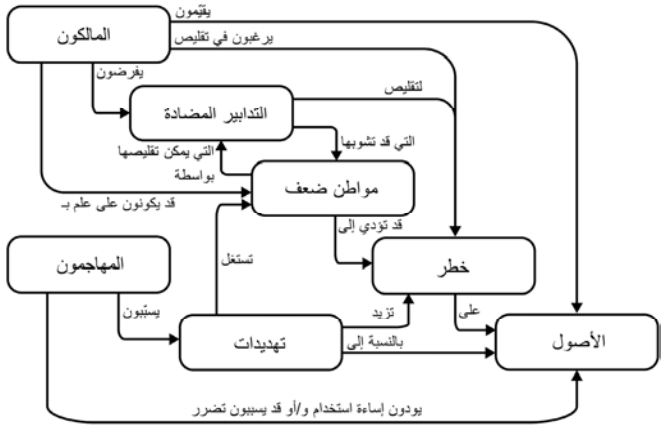
الخطر في سياق الأمن الحاسوبي هو احتمال قيام تهديد معيّن باستغلال نقاط ضعف أحد الأصول أو مجموعة من الأصول، وبالتالي إلحاق الضرر بالمنظمة. وتقاس المخاطر/الأخطار على أساس المزج بين احتمال حصول حدث ما وبين فداحة عواقبه.

والشكل ٦ هو كناية عن رسم بياني يعرض أوجه الترابط المتعددة بين مفاهيم التهديدات ومواطن الضعف والمخاطر [١٦].

٦-٢- تقييم المخاطر وإدارتها

يشكل تقييم المخاطر أداةً هامة لتحديد أفضل مكان لتخصيص الموارد والجهود الرامية إلى التصدّي لمواطن الضعف ولاحتمالات استغلالها.

وهي عملية يتم من خلالها تعيين وتوثيق توليفات محددة من التهديدات ومواطن الضعف والآثار، واستحداث الضوابط الوقائية الملائمة. ويوفّر تقييم التهديدات ومواطن الضعف أساساً لإعداد التدابير المضادة المطلوبة لتفادي الهجمات ضد النظم الحاسوبية أو التخفيف من آثارها.



الشكل ٦ – مفاهيم الأمن والعلاقات بين عناصره (مكيّفة عن المعيار ISO 13335–I 2004 [٦١]).

وتتكوّن منهجية تقييم المخاطر وإدارتها من الخطوات الأساسية التالية:

- تحديد المحيط والسياق؛
- تحديد التهديدات وتصنيفها؛
- تقييم مواطن الضعف؛
- صياغة سيناريوهات الهجوم؛
- احتمالات الاستغلال الناجح؛
- تقييم مستوى الخطر؛
- تعيين التدابير المضادة.

لتنفيذ تحليل وتقييم منهجي ومتساوق للمخاطر، يجب استخدام عملية ذات معالم واضحة قادرة على الامتثال للمعايير القائمة. وقد بلغ العديد من منهجيات تقييم المخاطر أو إدارتها مرحلة النضوج وبات في إمكانها هيكلة عملية من هذا النوع بشكل فعال، وقد حظيت بالتالي بقبول جمهور عريض. وتقوم غالبية هذه المنهجيات على أساس ما هو سائد من مفاهيم ومنطق. والمعيار الدولي الحالي هو ذاك الصادر عن المنظمة الدولية لتوحيد المقاييس وعن اللجنة الدولية للتقنيات الكهربائية بالرقم ISO/IEC 27005 بعنوان إدارة مخاطر أمن المعلومات [٤]. ويرد في المرفق الثاني مثال معيّن آخر عن إحدى هذه المنهجيات. وقد تطلب السلطات الوطنية استخدام منهجية أو سياسة معيّنة لتقييم المخاطر، كما يجوز أن يكون للمرافق منهجيات إضافية خاصة بها.

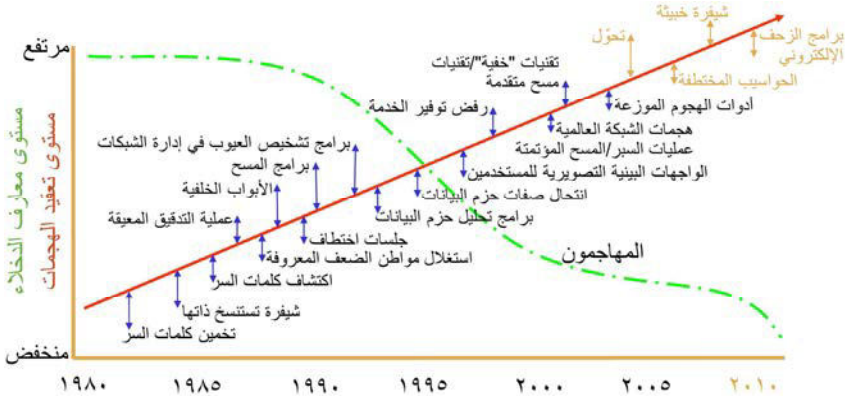
واضطلعت الوكالة الأوروبية لأمن الشبكات والمعلومات (إنيسا) بصوغ سلسلة مثيرة للاهتمام من طرائق وأدوات تقييم المخاطر، وقد كرّست صفحة ويب خاصة لهذا المسح [١٧].

وتتوقف ضرورة تقييم النظم، وعمق هذا التقييم، وتواتر عملية الارتقاء بتحليلات المخاطر على أهمية النظم من حيث وظائفه المرتبطة بالأمان وبالأمن. ويجب إيلاء الاعتبار للاضطلاع بتحليل جديد أو، على الأقل، تنفيذ استعراض كلما أدخلت تعديلات على النظام. وقد يتم الوفاء بهذا الشرط عن طريق إدخال معدات أو برامج حاسوبية أو إجراءات جديدة، أو عند إجراء تغيير رئيسي في مجموعة مهارات المشغلين. وفي العادة، يشهد عدد التهديدات ومواطن الضعف المحتملة ارتفاعاً عند الانتقال من النظم القائمة بذاتها إلى النظم المترابطة فيما بينها.

وعندما لا يكون من العملي تنفيذ تحليل للمخاطر ضد تهديدات معيّنة، يوصى باستخدام الممارسات الفضلى والمبادئ الهندسية الجيدة.

٦-٣- تحديد التهديدات وتصنيفها

يسلّط الشكل ٧ الضوء على التوجه المتواصل نحو ارتفاع مستوى تعقيد الهجمات وتراجع مستوى المعارف المطلوب لإطلاق هجمات من هذا النوع. وينبغي لبرامج الأمن الحاسوبي أن تسعى جاهدة إلى الحفاظ على مستوىً من التقييم يغطي مجموعة واسعة جداً من سيناريوهات الهجوم الممكنة.



الشكل ٧ – التعقيد المتفاقم للتهديدات نتيجة تكاثر المهاجمين.[٤]

[٤] هـ.ف. ليبسون، تعقّب ومتابعة الهجمات الإلكترونية: التحديات التقنية ومسائل السياسات العالمية، تقرير خاص رقم 10 (2000) CMS/SEI-2002-SR-009.

تتمخض أهم أحداث قرصنة الحواسيب بانتظام عن منشورات تتطرق إلى مواضيع مواطن الضعف التي تشوب نظم التحكم الصناعي. وباعتبار أنها تعطي، على وجه العموم، صورة مؤخّرة عن الوضع الراهن لمهارات واهتمامات القراصنة الفعليين، ينبغي لها أن تشكل عاملاً إضافياً لرفع مستوى الوعي. وفضلاً عن ذلك، بدأت الأفرقة الوطنية المعنية بالتصدّي للطوارئ الحاسوبية مؤخراً بنشر مواطن الضعف التي تشوب البرامج الحاسوبية لنظم التحكم الصناعي، ممّا يعزز الانكشاف أمام الرأي العام وأمام الأوساط المعنية بالأمن الحاسوبي، ويركّز الاهتمام على الحلول من هذا النوع وعلى مواطن ضعف المنتج.

وبالتالي، بعد الانتهاء من إرساء ما يكفي من وسائل الدعم والموارد، ينبغي للخطوات الأولية في عملية صياغة برنامجٍ للأمن الحاسوبي أن تركّز على فهم التهديدات المحتملة على أساس توصيفات مهاجمين وسيناريوهات هجوم ذات مصداقية. وقد تتمثل إحدى الخطوات الأولى الممكنة في وضع مصفوفة لتوصيف المهاجمين تتضمن قائمة بالمهاجمين ذوي المصداقية ودوافعهم وأهدافهم المحتملة. ويمكن بعد ذلك استخدام مصفوفة توصيف المهاجمين لصوغ سيناريوهات هجوم معقولة؛ وتتطرق الفقرات الفرعية التالية لهذه العملية بقدر أكبر من التفصيل.

٦-٣-١- التهديد المُحتاط له في التصميم

التهديد المحتاط له في التصميم هو أداة هامة يشيع استخدامها لتحديد مستويات التهديد وكأساس لتطوير وضعٍ أمني. وهذا التهديد المحتاط له في التصميم هو كناية عن بيان بشأن سمات الخصوم المحتملين (داخليين و/أو خارجيين) وخصائصهم. ويُستمدّ التهديد المحتاط له في التصميم من معلومات استخباراتية ذات مصداقية، ولكن لا يُقصد منه أن يكون بياناً بشأن التهديدات الفعلية السائدة. استناداً إلى بيئة التهديد الحالية، يمثل التهديد المحتاط له في التصميم أعظم تهديد معقول ينبغي لمرفق ما أن يتوقع الدفاع عن نفسه ضده. وتستخدم الدول التهديدات المحتاط لها في التصميم في نظامها الرقابي لتحديد الموارد الوافية المخصصة لحماية المواد النووية والمرافق النووية ضد الأعمال العدائية. (لمزيد من المعلومات بشأن التهديدات المحتاط لها في التصميم، انظر المرجع [٩].)

وينبغي إيلاء الاعتبار لتضمين هذه السيناريوهات تهديداتٍ إمّا من الهجمات الفردية باستخدام/ضد النظم الحاسوبية أو الهجمات المنسّقة التي تشمل استخدام النظم الحاسوبية.

٦-٣-٢- توصيفات المهاجمين

يبرز الجدولان ١ و٢ مجموعة ممكنة من توصيفات المهاجمين. ويركّز الجدول ١ على التهديدات الداخلية أو التي يرتكبها أشخاص داخليين (انظر أيضاً المرجع [١٩] لمناقشة التهديدات الناشئة عن أشخاص داخلين)، فيما يحدد الجدول ٢ بعض التهديدات الخارجية المحتملة. ويربط الجدولان ما بين الأنواع العامة من المهاجمين وبين مواردهم، وطول مدة الهجوم، والأدوات التي يحتمل استخدامها، ودوافع المهاجم. ويجب تكييف التوصيفات وفقاً لكل مرفق على حدة. ولذلك، فمن المطلوب اعتماد عملية وافية لجمع المعلومات بغية كفالة اكتمال مصفوفة مهاجمي كل مرفق ووثاقة صلتها بالواقع.

٦-٣-٣- سيناريوهات الهجوم

عند استحداث سيناريوهات هجوم، يجوز للمرء التمييز بين عدة إمكانات. ويمكن لمهاجمة المرفق النووي أن تهدف إلى ما يلي:

- العمل على التخطيط لهجوم منسّق لاحق يهدف إلى تخريب المحطة و/أو إلى إزالة مواد نووية؛
- تعريض أمان البشر أو البيئة للخطر؛
- شن هجوم على موقع آخر؛
- خلق حالة من الارتباك والخوف؛
- تحقيق كسب نقدي لصالح مجموعة إجرامية من الناس؛
- التسبب بحالات عدم استقرار هامة في السوق وتحقيق مكاسب لعدد مختار من الجهات الفاعلة في السوق.

ورهناً بأغراض الهجوم أو أهدافه، سيحاول المهاجم استغلال مختلف مواطن الضعف التي تشوب النظام. وقد تؤدي هذه الهجمات إلى ما يلي:

- الوصول غير المأذون به إلى المعلومات (فقدان السرية)؛
- اعتراض المعلومات أو البرامج الحاسوبية أو الأجهزة الحاسوبية أو غيرها وإدخال التغييرات عليها (فقدان السلامة)؛

الجدول ١ – التهديدات الداخلية

المهاجم	الموارد	المدة الزمنية	الأدوات	الدافع
عميل سري	’هندسة اجتماعية‘ ميسّرة. الوصول إلى النظام عند مستوى معيّن. توافر وثائق النظام وخبراته.	متفاوتة، ولكن لا يمكن، على وجه العموم، تكريس ساعات طويلة لذلك.	طريق وصول قائم، معارف بالبرمجة وبهندسة النظام: – إمكانية معرفة كلمات السر القائمة؛ – إمكانية إدخال أبواب خلفية و/أو فيروسات؛ – طروادية مصاغة لأغراض محددة؛ إمكانية توافر دعم من جانب خبرات خارجية.	سرقة المعلومات التجارية، والأسرار التكنولوجية، والمعلومات الشخصية. تحقيق مكاسب اقتصادية (بيع المعلومات إلى جهات منافسة) الابتزاز.
موظف/مستخدم ساخط	موارد متوسطة/قوية. الوصول إلى النظام عند مستوى معيّن. توافر وثائق النظام وخبراته بشأن الأعمال التجارية الخاصة وعمليات النظم.	متفاوتة، ولكن لا يمكن، على وجه العموم، تكريس ساعات طويلة لذلك.	طريق وصول قائم، معارف بالبرمجة وبهندسة النظام. إمكانية معرفة كلمات السر القائمة. قدرة على إدخال أدوات أو سكريبتات ’صبيانية‘ (يحتمل أن تكون أكثر إتقاناً في حال تمتع القرصان بمهارات حاسوبية خاصة)	ثأر، خراب، فوضى. سرقة المعلومات التجارية. إحراج رب العمل/موظف آخر. تلويث السمعة أو تقويض الثقة.

الجدول ٢ – التهديدات الخارجية

المهاجم	الموارد	المدة الزمنية	الأدوات	الدافع
قرصان يسعى إلى التسلية	مهارات متفاوتة ولكنها، على وجه العموم، محدودة. معرفة ضئيلة بالنظام خارج ما هو في نطاق المعلومات العامة.	الكثير من الوقت، ولكن القليل من الصبر.	سكريبتات وأدوات متوافرة عموماً. يجوز تطوير بعض الأدوات.	التسلية، المكانة. استهداف الفرصة السانحة. استغلال 'الثمار السهلة المنال'.
مناضل مناوئ للقوى النووية	موارد محدودة، ولكن يمكن أن يحظى بالدعم المالي عن طريق قنوات سرية. قدرة الاستفادة من أدوات الأوساط الناشطة في ميدان الإنترنت. معرفة ضئيلة بالنظام خارج ما هو في نطاق المعلومات العامة.	قد تستهدف الهجمات أحداثاً معروفة سابقاً (من قبيل الاحتفالات أو الانتخابات). الكثير من الوقت، صبور وذو دوافع.	المهارات الحاسوبية متوافرة. دعم ممكن من جانب أوساط القرصنة الحاسوبية. 'هندسة اجتماعية'.	القناعة بأنه ينقذ العالم. التأثير على الرأي العام بشأن مسائل محددة. إعاقة العمليات التجارية.
موظف/مستخدم ساخط (لم يعد قيد التوظيف)	موارد محدودة إذا لم يكن منخرطاً في مجموعة أكبر من الناس. ربما لا تزال بعض وثائق النظام في حوزته. قد يستخدم طريق وصول سابقة غير خاضعة للإدارة. روابط محتملة مع موظفي المرفق.	متفاوتة وتتوقف على مجموعة الناس المعنية.	إمكانية معرفة كلمات السر القائمة. قد يستخدم طريق وصول سابقة غير خاضعة للإدارة. ربما يكون قد استحدث أبواباً خلفية إلى النظام عندما كان لا يزال موظفاً. 'هندسة اجتماعية'.	ثأر، خراب، فوضى. سرقة المعلومات التجارية. إحراج رب العمل/موظف آخر. تلويث السمعة أو تقويض الثقة.

الجدول ٢ – التهديدات الخارجية (تابع)

المهاجم	الموارد	المدة الزمنية	الأدوات	الدافع
الجريمة المنظمة	موارد ضخمة. توظيف خبراء في ميدان الإنترنت.	متفاوتة، ولكنها في الغالب قصيرة الأمد.	سكريبتات، أدوات مصنوعة محلياً. إمكانية توظيف 'قراصنة للإيجار'. إمكانية الاعتماد على موظف سابق/حالي. 'هندسة اجتماعية'.	الابتزاز. سرقة مواد نووية. الابتزاز (الكسب المالي). اللعب على المخاوف المالية والمفاهيمية التي تعاني منها الأعمال. معلومات للبيع (تقنية أو تجارية أو شخصية).
دولة قومية	موارد وخبرات ضخمة. أنشطة جمع معلومات. إمكانية تدريب/خبرة تشغيلية على النظام.	متفاوتة.	فرق من خبراء الإنترنت المدرّبين. أدوات متطورة. إمكانية الاعتماد على موظف سابق/حالي. 'هندسة اجتماعية'.	جمع معلومات. بناء نقاط وصول لأعمال لاحقة. سرقة التكنولوجيا.
إرهابي	مهارات متفاوتة. إمكانية تدريب/خبرة تشغيلية على النظام.	الكثير من الوقت، صبور جداً.	سكريبتات، أدوات مصنوعة محلياً. إمكانية توظيف 'قراصنة للإيجار'. إمكانية الاعتماد على موظف سابق/حالي. 'هندسة اجتماعية'.	جمع معلومات. بناء نقاط وصول لأعمال لاحقة. فوضى. ثأر. التأثير على الرأي العام (الخوف).

— قطع خطوط إرسال البيانات و/أو إغلاق النظم (فقدان اللياقة التشغيلية)؛
— اختراق غير مأذون به لنظم اتصالات البيانات أو الحواسيب (فقدان الموثوقية).

يمكن لجميع هذه الجوانب أن تتمخّض عن عواقب وتأثيرات هائلة على سلامة عمل النظم الحاسوبية، ممّا قد يؤدي، مباشرة أم بشكل غير مباشر، إلى تقويض أمان المرفق وأمنه. عند وضع سيناريوهات الهجوم، ينبغي مراعاة التوجّهات التكنولوجية وسهولة وصول تكنولوجيات الهجوم. ويتضمن المرفق الأول صياغةً لعدد من السيناريوهات التي تستعرض هجمات خيالية، ولكنها واقعية.

٦-٤- النواتج المبسّطة لتقييم المخاطر

يقدم الجدول ٣، لأغراض توضيحية فحسب، أمثلة عن نظم قد تتواجد في مرفق نووي. وهو يحدد الآثار التي يحتمل أن تنجم عن هجمات ناجحة على النظم المعنية، والآثار المناظرة على المرفق، وأمثلة عامة عن التدابير المضادة الملائمة.

ولا يتطرّق هذا الجدول إلى دراسة مفهوم الاحتمالية الذي يتسم بأهمية جوهرية بالنسبة إلى تقييم المخاطر. ويتوقف احتمال نجاح الهجمات، وعواقبها المحتملة أيضاً، على السياق وعلى المرفق الخاضع للدراسة. وفضلاً عن ذلك، ينبغي إجراء تقييم أكثر شمولاً لمتطلبات السرية والسلامة واللياقة التشغيلية لكل نظام تجري دراسته ضمن إطار تقييم المخاطر.

٧- الاعتبارات الخاصة بالمرافق النووية

نظراً للطبيعة الفريدة التي تتسم بها الصناعة النووية، يجب على الأمن الحاسوبي للمرافق النووية أن يتناول قدراً من الشواغل يفوق قدر شواغل الأمن الحاسوبي لشبكات تكنولوجيا المعلومات في مجال الأعمال أو حتى نظم التحكم بالعمليات المشابهة خارج إطار الصناعة النووية. وتصف الفقرات التالية بعض هذه الشواغل ذات الصلة بالصناعة النووية.

الجدول ٣ – النظم النموذجية في المرافق النووية

النظام	التأثيرات على الأمن الحاسوبي	التأثيرات المحتملة على المرفق	التدابير المضادة المقترحة
نظام حماية المفاعل	فقدان سلامة البرامج الحاسوبية/البيانات الحرجة بالنسبة للأمان فقدان اللياقة التشغيلية.	حرجة المساس بأمان المحطة، انبعاث إشعاعي.	التدابير الأمنية من المستوى ١
نظام التحكم بالعمليات	فقدان سلامة البرامج الحاسوبية/البيانات الخاصة بالتحكم. فقدان اللياقة التشغيلية.	عالية المساس بتشغيل المحطة.	التدابير الأمنية من المستوى ٢
نظام إجازة العمل ونظام أوامر العمل	فقدان سلامة البيانات واللياقة التشغيلية للنظام.	متوسطة إجراءات خاطئة على المكوّنات. تعطيل التشغيل والصيانة العاديين.	التدابير الأمنية من المستوى ٤
نظام تحكم بالوصول المادي	فقدان اللياقة التشغيلية لنظم الوصول إلى الموقع وسلامتها. فقدان سرية بيانات الوصول إلى الموقع.	عالية إتاحة الوصول لأشخاص غير مأذون لهم. منع أشخاص مأذون لهم من الوصول إلى مناطق يحتاجون إلى الوصول إليها.	التدابير الأمنية من المستوى ٢
نظام إدارة الوثائق	فقدان سرية البيانات وتوافرها وسلامتها.	متوسطة استخدام المعلومات لتخطيط هجمات أكثر خطورة.	التدابير الأمنية من المستوى ٤
البريد الإلكتروني	فقدان السرية، والسلامة، واللياقة التشغيلية.	منخفضة أعباء إدارية. ازدياد صعوبة تنفيذ عمليات يومية.	التدابير الأمنية من المستوى ٥

٧-١- مراحل العمر التشغيلي للمرافق وأنماط تشغيلها

تمتاز المرافق النووية بمجموعة شديدة التنوّع من التصاميم والخصائص التشغيلية. وتشمل أعمارها التشغيلية مراحل وأنماط تشغيل متعددة تشمل ما يلي:

- التصميم والتشييد والإدخال في الخدمة.
- العمليات:
  - عمليات توليد الكهرباء؛
  - بدء تشغيل المحطة؛
  - إغلاق ساخن؛
  - إغلاق بارد؛
  - إعادة تزويد بالوقود وصيانة.
- الإخراج من الخدمة.

وقد تشمل هذه المراحل وأنماط التشغيل المتعددة نظماً مختلفة وبيئات تشغيلية مختلفة أيضاً. وعلى سبيل المثال، غالباً ما تنطوي فترات الصيانة المكثفة على استبدال المعدات وتعديلها واختبارها، أو قد تتطلب مزيداً من فرص وصول الموظفين والأطراف الآخرين/المقاولين. وينبغي لخطة الأمن الحاسوبي أن تراعي هذا التنوّع. وعلى وجه الخصوص، قد تدلّ مراحل العمر التشغيلي المختلفة ضمناً على تنقيحات عميقة يتم إدخالها على خطة الأمن الحاسوبي.

٧-٢- الاختلافات بين نظم تكنولوجيا المعلومات ونظم التحكم الصناعي

النظم الحاسوبية وهندسات التشبيك التي تدعم عمليات المحطات النووية ليست نظماً حاسوبية معيارية من حيث هندستها أو نسقها أو متطلبات أدائها. ويمكن تصنيف هذه النظم باعتبار أنها نظم تحكم صناعي متخصصة. وفيما انتقلت نظم التحكم الصناعي من العمليات التنفيذية ذات الملكية الخاصة الصارمة إلى استخدام الهندسة الحاسوبية العامة، ما زالت اختلافات هامة قائمة بين نظم التحكم الصناعي ونظم تكنولوجيا المعلومات المعيارية ويجب مراعاتها في أي خطة أمن حاسوبي.

ويعرض الجدول ٤، القائم على أساس مواد صادرة عن المعهد الوطني للمعايير والتكنولوجيا [٢٠]، أهم أوجه الاختلاف بين نظم التحكم الصناعي المتخصصة ونظم تكنولوجيا المعلومات التقليدية.

الجدول ٤ – أوجه الاختلاف بين نظم تكنولوجيا المعلومات ونظم التحكم الصناعي المتخصصة [٢٠]

الفئة	نظام تكنولوجيا المعلومات	نظم التحكم الصناعي
متطلبات الأداء	غير آنية الاستجابة يجب أن تكون متساوقة من الإلزامي أن يكون ذا خرج عالٍ التأخير الشديد والقلقلة قد يكونان مقبولين	آني الاستجابة حرجة من حيث الوقت الخرج المتواضع مقبول التأخر الشديد و/أو القلقلة يشكلان مصدر قلق كبير
متطلبات اللياقة التشغيلية	الاستجابات من قبيل إعادة التشغيل مقبولة يمكن في الغالب التسامح عن حالات القصور في اللياقة التشغيلية، رهناً بالمتطلبات التشغيلية للنظام	الاستجابات من قبيل إعادة التشغيل قد لا تكون مقبولة بسبب متطلبات توافر العمليات يجب تخطيط حالات الانقطاع وجدولتها قبل أيام/أسابيع المستوى العالي من اللياقة التشغيلية يتطلب اختبارات مكثفة في فترة ما قبل النشر
متطلبات إدارة المخاطر	تتسم سرية البيانات وسلامتها بأهمية مطلقة تحمّل الأعطال أقل أهمية – الانقطاع المؤقت لا يشكل خطراً رئيسياً الأثر الرئيسي الناجم عن المخاطر هو التأخر في العمليات التجارية	الأهمية المطلقة هي لضمان أمان البشر، وتليه حماية العمليات تحمل الأعطال جوهري، وحتى الانقطاع المؤقت غير مقبول الأثر الرئيسي الناجم عن المخاطر هو عدم الامتثال الرقابي، أو خسارة الحياة، أو المعدات، أو الإنتاج
نقطة تركيز أمن الهندسة	نقطة التركيز الأساسية هي حماية أصول تكنولوجيا المعلومات، والمعلومات المخزونة على هذه الأصول أو المتناقلة فيما بينها حاسوب الخدمة المركزي قد يتطلب مزيداً من الحماية	الهدف الأساسي هو حماية العملاء الطرفيين (كالأجهزة الميدانية من قبيل أجهزة التحكم بالعمليات) حماية حاسوب الخدمة المركزي مهمة أيضاً
العواقب غير المقصودة	الحلول الأمنية مصممة على أساس نظم تكنولوجيا معلومات نموذجية	يجب اختبار الأدوات الأمنية لكفالة عدم تأثيرها سلباً على التشغيل الطبيعي لنظم التحكم الصناعي
التفاعل الذي يتسم فيه الوقت بأهمية حرجة	تفاعل طارئ أقل حرجية يمكن تنفيذ التحكم الصارم بالوصول وفقاً للمستوى الضروري	الاستجابة للتفاعل البشري وغيره من التفاعلات الطارئة جوهرية الوصول إلى نظام التحكم الصناعي ينبغي أن يخضع لتحكم صارم ولكن يجب ألاّ يعيق التفاعل بين البشر والآلات
تشغيل النظم	يتم تصميم النظم لاستخدامها مع نظم التشغيل النموذجية عمليات الترقية غير معقدة مع توافر أدوات النشر المؤتمت	نظم التشغيل المختلفة والمعدّة وفقاً للاحتياجات الخاصة غالباً ما تفتقر إلى القدرات الأمنية يجب التأني في إدخال التغييرات على البرامج الحاسوبية، ويتم في العادة تنفيذها بواسطة باعة البرامج الحاسوبية بسبب ما تنطوي عليه هذه البرامج من خوارزميات تحكم متخصصة وربما من أجهزة وبرامج حاسوبية معدّلة
القيود المفروضة على الموارد	النظم مزوّدة بما يكفي من الموارد لدعم إضافة تطبيقات خارجية من قبيل الحلول الأمنية	النظم مصممة لدعم العمليات الصناعية المرجوة، مع قدر أدنى من موارد الذاكرة والمعالجة لا يسمح بإضافة تكنولوجيا أمنية
الاتصالات	بروتوكولات اتصالات معيارية الشبكات بمعظمها سلكية تتسم بقدر محدود من القدرات اللاسلكية ممارسات تشبيك نموذجية خاصة بتكنولوجيا المعلومات	بروتوكولات اتصالات خاصة ومعيارية عديدة عدة أنواع من وسائط الاتصالات تشمل شبكات سلكية ولاسلكية مكرّسة (إذاعة وأقمار صناعية) الشبكات معقدة وتتطلب في بعض الأحيان خبرات مهندسين متخصصين بالتحكم
إدارة التغيير	تطبق التغييرات في البرامج الحاسوبية في التوقيت الملائم مع اعتماد سياسات وإجراءات أمنية جيدة. غالباً ما تكون الإجراءات مؤتمتة	يجب إخضاع التغييرات في البرامج الحاسوبية لاختبارات مكثفة ونشرها بشكل تدريجي في كافة أقسام النظام لكفالة الحفاظ على سلامة نظام التحكم يجب في الغالب تخطيط حالات انقطاع نظم التحكم الصناعي وجدولتها قبل أيام/أسابيع
الدعم الخاضع للإدارة	يتيح اعتماد أنماط متنوعة من الدعم	دعم الخدمات يقدّم عادة بواسطة بائع واحد فريد
العمر التشغيلي للمكوّنات	يتراوح العمر التشغيلي بين ٣ و٥ سنوات	يتراوح العمر التشغيلي بين ١٥ و٢٠ سنة
الوصول إلى المكوّنات	تكون المكوّنات في العادة محلية ويكون الوصول إليها سهلاً	يمكن للمكوّنات أن تكون معزولة ونائية وتتطلب جهداً مادياً مكثفاً للتمكن من الوصول إليها

٧-٣- الطلب على مزيد من إمكانيات التوصيل وما يرتبط بذلك من عواقب

يتمثل أحد المجالات المثيرة للشواغل المتزايدة بالنسبة لنظم التحكم الصناعي في الرغبة المتزايدة لتحقيق الترابط بين نظم الأعمال والهندسة مع النظم التشغيلية. نتيجة رغبة مقرات الشركات والمخططين والمهندسين في الوصول الآني إلى البيانات الخاصة بالمعامل، يجري العمل على إقامة جسور تربط بين شبكات التحكم المحكمة الإغلاق المسؤولة عن تشغيل المحطة وبين شبكات البيانات غير المغلقة المستخدمة لإتاحة المعاينة بواسطة الإدارة. ويمكن لهذا الجسر أن يشكل بوابة يتم من خلالها اختراق الشبكة.

وتتمثل إحدى السمات الهندسية الفريدة الأخرى في وجود مراكز التشغيل الطارئ عن بعد. وتتيح مراكز التشغيل الطارئ هذه موقعاً بعيداً لمراقبة المحطة وتشغيلها الطارئ في حال بات المركز الأساسي غير صالح للاستخدام نتيجة حدث ما. وتؤدي المتطلبات الخاصة بمراقبة/صون بعض عناصر التحكم بالمحطة إلى بروز الحاجة إلى تدفق البيانات عبر بعض وسائل الاتصالات. وتتيح هذه الوسائل مساراً محتملاً لتقويض النظام الرئيسي والدخول إليه. وفضلاً عن ذلك، تؤدي متطلبات ازدواجية الوظائف إلى بروز الحاجة إلى الالتزام بمتطلبات أمنية متساوقة بين نظامين. ومن شأن التخلف عن صون نظام من النظامين أن يخلق مساراً للاقتحام والحِقن الاستغلالية.

ويمكن أيضاً للحاجة إلى التحليل أو الصيانة أو الارتقاء عن بعد أن تؤدي إلى نقاط ضعف مماثلة. وقبل الموافقة على صلات الترابط الإضافية هذه، يجب إجراء تحليل معمّق للمخاطر.

٧-٤- الاعتبارات بشأن ترقيات البرامج الحاسوبية

العديد من القواعد التنظيمية الحالية الخاصة باعتماد معدات المحطات النووية أو المصادقة عليها صيغ مستهدفاً المعدات التناظرية غير الرقمية. وهذه القواعد التنظيمية لا تتقادم بسرعة. ومن جهة أخرى، فإن الخطط والممارسات الفضلى الخاصة بأمن تكنولوجيا المعلومات تنطوي ضمناً على إجراء عمليات منتظمة لترقية وإصلاح البرامج الحاسوبية والمكوّنات الرقمية نظراً لكون هذه المكوّنات تتقادم بشكل أسرع بكثير.

ولذلك فمن المهم التفكير في التحدي الناشئ عن إصلاحات وترقيات البرامج الحاسوبية في النظم الرقمية للتحكم أو الرقابة النوويين. وفي سيناريو أسوأ الظروف، يمكن اعتبار كل تعديل أو تنقيح في البرامج الحاسوبي على أنه تغيير في النظام وأنه من الممكن أن يؤدي إلى اعتماد خاص للنظام أو حتى إلى إعادة المصادقة على بعض النظم الحرجة. ونظراً للتعقيد الذي ينطوي عليه نهج من هذا النوع، قد يؤدي ذلك إلى تراكم التأخر في

تنفيذ عمليات الإصلاح أو إلى قرار مدروس بتأخير عمليات ترقية البرامج الحاسوبية. وللحد من هذه الآثار، ينبغي التمييز بين الصيانة العادية التي تتفادى هذا النوع من العمليات وبين التعديلات المدخلة على النظام التي تتطلب إعادة اختبار النظم الحرجة أو حتى إعادة المصادقة عليها. وفي جميع الحالات، يجب تنفيذ أي تعديلات على نظم الأمان أو النظم ذات الصلة بالأمان وعلى نظم الأمن وفقاً لإجراءات متفق عليها.

٧-٥- التصميم الآمن للنظم الحاسوبية ومواصفاتها

خلال العملية الأصلية لتصميم وصياغة العديد من النظم والتجهيزات القائمة للتحكم بالعمليات والتحكم الصناعي، لم يكن للأمن الحاسوبي أهمية رئيسية. وقد أدى الطلب مؤخراً على إرساء التواصل بين النظم وبين العمليات، وإدماج النظم الحاسوبية التجارية الجاهزة للاستعمال، وارتفاع معدلات النشاط الحاسوبي الكيدي (كالقرصنة الحاسوبية مثلاً) إلى زيادة الحاجة إلى اعتبار الأمن الحاسوبي كمطلب أساسي عند شراء معدات جديدة.

ونتيجة لذلك، ينبغي إضفاء الطابع الرسمي على المتطلبات الأمنية كجزء من عملية التفاوض التعاقدي مع الموردين. وتشكل الوثيقة الصادرة عن المنظمة الدولية لتوحيد المقاييس بعنوان المعايير المشتركة (الوثيقة ISO 15408) أداةً ممكنة لإضفاء هذا الطابع الرسمي على هذا النوع من المتطلبات الأمنية. وثمة مثال آخر على ذلك يكمن في محاولة تحديد لغة مشتريات لنظم التحكم [٢٢] بواسطة وزارة الأمن الوطني في الولايات المتحدة الأمريكية التي نشرت إرشادات وتوصيات بشأن صياغة متطلبات الأمن الإلكتروني ولغة المشتريات الخاصة لاقتناء نظم التحكم.

٧-٦- عملية مراقبة إمكانية الوصول بواسطة الأطراف الآخرين/الباعة

من الجوهري مراعاة مستوى الأمن الخاص بأي طرف ثالث وبائع. ومن الأهمية بمكان أن تعمل شعبة الأمن بشكل وثيق مع شعبة العقود لضمان إدماج الأحكام الخاصة بالأمن في كل عقد من العقود.

وفي الغالب ما تقوم المنظمات العاملة في القطاع النووي بإسناد العقود إلى كيانات خارجية؛ ويؤدي بعض هذه العقود إلى احتفاظ الشركات المتعاقدة، في مبانيها، بمعلومات أو أصول مؤشرة وقائياً. وفي حال عدم الالتزام بقواعد صارمة عند إسناد هذا النوع من العقود وعند إداراتها اللاحقة، فإن المعلومات والأصول المعنية بالعقد والمؤشر عليها وقائياً قد تتعرض للانتهاك أو للكشف غير المأذون به.

ونظراً للعوامل المذكورة أعلاه، من المهم أن تقوم الإدارة المسؤولة في كل موقع/منظمة في القطاع النووي بالحفاظ على علاقة عمل وثيقة مع الشركة المتعاقدة لكفالة

تناول جوانب الأمن الأساسية في كافة مراحل صياغة العقد وتنفيذه، وخلال عملية التسليم النهائي.

وعند الاقتضاء، ينبغي تنفيذ عمليات التحقق والتدقيق لضمان قيام نظام إدارة المنظمة المتعاقدة بتناول المسائل الأمنية بالشكل الوافي، ولكفالة امتثال ممارسات المنظمة وتدابيرها لمتطلبات النظام.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

المراجع

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[6] COUNCIL OF EUROPE, Convention on Cybercrime, ETS No. 185, COE, Strasbourg (2001).

[٧] الوكالة الدولية للطاقة الذرية، النظام الإداري للمرافق والأنشطة، سلسلة معايير الأمان الصادرة عن الوكالة، GS-R-3، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١١).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[٩] الوكالة الدولية للطاقة الذرية، ثقافة الأمن النووي، العدد ٧ من سلسلة الأمن النووي الصادرة عن الوكالة، الوكالة الدولية للطاقة الذرية، فيينا ٢٠١١.

[١٠] الوكالة الدولية للطاقة الذرية، أهداف الحماية المادية ومبادئها الأساسية، GOV/2001/41، الوكالة الدولية للطاقة الذرية، فيينا (٢٠٠١).

[١١] الحماية المادية للمواد النووية والمرافق النووية، INFCIRC/225/Rev.4، الوكالة الدولية للطاقة الذرية، فيينا (١٩٩٩).

[١٢] الوكالة الدولية للطاقة الذرية، الارشادات والاعتبارات المتعلقة بتنفيذ الوثيقة INFCIRC/225/Rev.4، المعنونة "الحماية المادية للمواد النووية والمرافق النووية"، الوكالة الدولية للطاقة الذرية،-وثيقة تقنية-٩٦٧ (التعديل ١)/ألف، IAEA-TECDOC-967 (Rev.1)/A، الوكالة الدولية للطاقة الذرية، فيينا (٢٠٠٢).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[١٥] الوكالة الدولية للطاقة الذرية، مسرد مصطلحات الأمان الصادر عن الوكالة الدولية للطاقة الذرية، المصطلحات المستخدمة في مجالي الأمان النووي والوقاية من الإشعاعات، الوكالة الدولية للطاقة الذرية، فيينا (٢٠٠٧).

[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).

[17] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Inventory of Risk Management/Risk Assessment Methods and Tools, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools.

[١٨] الوكالة الدولية للطاقة الذرية، إعداد وصف التهديدات المحتاط لها في التصميم واستخدامه وصيانته، العدد ١٠ من سلسلة الوكالة للأمن النووي، الوكالة الدولية للطاقة الذرية، فيينا (٢٠١٢).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[20] STOUFFER, K.A., FALCO, J.A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Institute of Standards and Technology, Chicago (2011).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Geneva (2008).

[22] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Cyber Security Procurement Language for Control Systems, September (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Risk Management — Vocabulary, ISO/IEC Guide 73:2009, ISO/IEC, Geneva (2009).

ببليوغرافيا

AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

FEDERAL MINISTRY OF THE INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlin (2005).

INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection Objectives and Fundamental Principles, Resolution GOV/2001/41, IAEA, Vienna (2001).

INTERNATIONAL SOCIETY FOR AUTOMATION, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

KOREA INSTITUTE OF NUCLEAR SAFETY, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seoul (2007).

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, November (2006).

NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 0809 (Rev. 5), NEI, Washington DC (2010).

NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris (2002).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security, DSTI/ICCP/REG (2003) 5/REV1, OECD, Paris (2003).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG (2005) 1/FINAL, OECD, Paris (2005).

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

المرفق الأول

سيناريوهات الهجوم على النظم في المرافق النووية

كما ورد في الفقرة ٦–٣، يمكن لطبيعة وأشكال الهجمات القائمة على أساس الحاسوب، والتي يجب الحماية ضدها كلها، أن تتفاوت بشكل كبير. وفيما قد تكون الهجمات من أنواع مختلفة، فإن عواقبها على المستوى العالي تشمل ما يلي:

- الوصول غير المأذون به إلى المعلومات أو اعتراضها (فقدان السرية)؛
- التعديل غير المأذون به للمعلومات أو البرامج الحاسوبية أو الأجهزة الحاسوبية أو غيرها (فقدان السلامة)؛
- قطع خطوط إرسال البيانات و/أو إغلاق النظم (فقدان اللياقة التشغيلية).

عند صياغة التدابير الوقائية ضد الهجمات الحاسوبية، من الأهمية بمكان فهم طبيعة الهجمات والمواقع المحتملة التي قد يستخدمها هجوم أو مهاجمون للحصول على معلومات ذات صلة وللوصل إلى النظم الحاسوبية المستهدفة. **والقصد من الأمثلة الواردة أدناه هو تشجيع القرّاء – بعد أن يكونوا قد اكتسبوا فهماً أفضل للتهديدات – على التفكير في منظمتهم الخاصة/نظامهم الخاص، وعند الاقتضاء، تصحيح الوضع الأمني وفقاً لذلك.** وفي حين أن الهجمات الوارد وصفها هنا هي خيالية، فإنها ذات صلة بسيناريوهات قابلة للتصديق قائمة على أساس هجمات مماثلة طرأت في قطاعات صناعية أخرى. والتفكير في هذا النوع من السيناريوهات يشكل وسيلة جيدة لضمان أن الخطة الأمنية تتصدّى لديناميكيات بيئة التهديدات الدائمة التغيّر.

وينطوي أي هجوم حاسوبي جيد التنسيق على مراحل متعددة. وتشمل هذه المراحل ما يلي:

- تحديد الهدف؛
- الاستطلاع؛
- الوصول إلى النظام/انتهاكه؛
- تنفيذ الهجوم؛
- إخفاء الآثار للحفاظ على إمكانية الإنكار؛

وترد في الفقرات الفرعية التالية ثلاثة سيناريوهات خيالية عن هجمات حاسوبية. ويمكن تطبيق السيناريو الأول، الذي يهدف إلى جمع المعلومات، كتمهيد للسيناريوهين التاليين.

السيناريو الأول – جمع المعلومات لدعم عمل كيدي

هدف الهجوم – تأمين الوصول المادي إلى مجالات خاضعة للرقابة (وصول محدود) من المرفق لدعم هجوم لاحق.

والهدف موضع الاهتمام هو الشخص المسؤول عن إدارة بطاقات الدخول وعن إسناد امتيازات الوصول. ويشمل تأمين الوصول المادي إلى المجالات المحظورة انتهاك الحاسوب الخاص بمدير البطاقات وانتهاك نظام إصدار شفرات الوصول. ويختار المهاجم أن يتظاهر بأنه مقاول من الباطن يعمل على تسليم مكوّنات من المعدات.

والأهداف الممكنة لجمع المعلومات بغية دعم الهجوم تشمل ما يلي:

— المعلومات الخاصة بالموظفين لإمكانية ابتزازهم أو لتنفيذ 'الهندسة الاجتماعية'؛
— الوثائق المتعلقة بتصميم نظام التحكم بالوصول؛
— سياسات النظم الأمنية ومخططاتها الهندسية أو ما سوى ذلك من مناطق المحطة ذات الصلة؛
— الجداول التشغيلية – جدول المحطة، والروتين اليومي، وأسماء العاملين، وأوقات عمل كل منهم، وأسماء الموظفين الغائبين في إجازة، عندما تطرأ تغييرات معيّنة؛
— قائمة بالمورّدين ومواعيد عملهم على المعدات؛
— الجرد بالمعدات والمكوّنات؛
— التدابير الخاصة بكلمات المرور وتدابير التحكم بالوصول؛
— التدابير الإدارية والتقنية للتحكم بالوصول؛
— المعلومات الخاصة بمطوّري البرامج الحاسوبية وتلك الخاصة بالمشاريع الجارية؛
— هندسة الشبكات؛
— هندسة الاتصالات.

وتشمل الطرق المحتملة لجمع هذه المعلومات ما يلي:

- ’هندسة اجتماعية‘؛
- عمليات البحث الإلكتروني عن المعلومات العامة؛
- الغوص في براميل القمامة؛
- الاتصال الكيدي بحثاً عن الحواسيب؛ البحث الكيدي عن الشبكات الحاسوبية اللاسلكية؛
- الهجمات التي تستهدف عناوين البريد الإلكتروني – ’التصيّد‘[1] للتمكن من الدخول على الشبكة، رواصد لوحات المفاتيح؛
- تنصيب البرامج الحاسوبية أو تركيب الأجهزة على الآلات المضيفة – باستخدام أسطوانة أو ذاكرة محمولة أو قرص مدمج؛
- التنصّت على رقن كلمات المرور أو رقن شفرات الوصول (المراقبة اليدوية أو الصوتية أو بالفيديو).

وقد تشمل مكوّنات الهجوم ما يلي:

- الحصول على بطاقة الدخول (البطاقة الإلكترونية) والشفرة؛
- سرقة/استنساخ بطاقة دخول قائمة؛
- إمكانية الوصول إلى آلة طبع البطاقة لصنع بطاقة جديدة؛
- استحداث بيانات موظف جديد؛
- انتحال شخصية موظف انتهى عقد عمله مؤخراً؛
- منح مستوى الوصول المرجو.

عند الحصول على البطاقة والشفرات، يقوم المهاجم باستخدام المعلومات المكتسبة لنشاط تنظيمي بغية الدخول إلى المرفق من دون إثارة الشبهات منتحلاً صفة شخص يقوم بتوصيل مكوّنات المعدات.

[1] يشير ’التصيّد‘ إلى محاولات الاحتيال للحصول على معلومات حساسة، من قبيل أسماء المستخدمين وكلمات المرور وتفاصيل البطاقات الائتمانية، عن طريق تظاهر المهاجم بأنه كيان موثوق في الاتصالات الإلكترونية.

السيناريو الثاني – هجوم يهدف إلى إضعاف أو انتهاك نظام حاسوبي واحد أو أكثر

هدف الهجوم – تخريب محطة قوى نووية والحؤول دون إعادة التشغيل الفوري للمحطة.

في هذا المثال، خلال فترة إغلاق، يجري مقاول من الباطن اختبارات على نظام التحكم بمياه التغذية. ويركّب المقاول نقطة وصول عن بعد لمراقبة النظام واختباره من مكتبه. وبعد استكمال المقاول لعمله، تبقى نقطة الوصول في مكانها سهواً.

وقام المهاجم بجمع معلومات عن المحطة كشفت له عن أن المقاول من الباطن كان في السابق يعمل في المحطة وعن أنه هدف أساسي لاكتساب معلومات بشأن المحطة. وينفّذ المهاجم هجوماً للتصيّد بواسطة البريد الإلكتروني ضد مكتب المقاول من الباطن، ويدسّ في النظام حزمة جذرية "روت كيت" توفّر له ضوابط تحكم إداري. وهكذا يكتسب المهاجم إمكانية الوصول إلى شبكة المقاول الحاسوبية ويكتشف المخططات الاختبارية من المحطة، فضلاً عن إمكانية الاستفادة من نقطة الوصول عن بعد التي لم تقم المحطة بتفكيكها.

وبفضل هذه المعلومات، يصبح بإمكان المهاجم أن ينفذ هجوم رفض خدمة[٢] على نظام التحكم بمياه التغذية عن طريق إغراق الشبكة بكمٍّ هائل من البيانات ليتسبب بتعطيل النظام. وكان النظام مصمماً لمعالجة حركة بيانات دنيا فقط.

بعد أن يكتسب المهاجم إمكانية الوصول إلى الشبكة، ويحدّد مكوّناتها ويعيّن بروتوكولات الاتصالات المستخدمة فيها، يقوم بتنفيذ الهجوم. ويؤدي الهجوم إلى فقدان قدرة الاستجابة في نظام التحكم بمياه التغذية، ممّا يسبّب الإغلاق اليدوي للمحطة. ولا يمكن القيام فوراً بتحديد السبب الكامن وراء عطل نظام التحكم بمياه التغذية، فتبقى المحطة مغلقة بانتظار نتيجة التحقيقات.

السيناريو الثالث – انتهاك نظام حاسوبي كأداة لهجوم منسّق

الهدف من الهجوم – سرقة مواد نووية خلال انتقالها بين مرافق الخزن. يتوقع استخدام هجوم حاسوبي لتعديل نظام الجرد والاقتفاء بغية إخفاء فقدان المواد المسروقة.

الاستطلاع وجمع المعلومات يحددان عملية وسم واقتفاء شحنات المواد المشعة عند نقلها فيما بين مرافق الخزن. ويشمل ذلك وسمات تحديد الهوية باستخدام موجات الراديو[٣] على فرادى البنود التي تصف المكوّنات وتتضمن قائمة بالمحتويات.

---

٢ رفض الخدمة يتمثل في منع الوصول المأذون به إلى أحد موارد النظام أو في تأخير عمليات النظام ووظائفه.

٣ تحديد الهوية باستخدام موجات الراديو: تكنولوجيا مستخدمة لتحديد الهوية والاقتفاء باستخدام موجات الراديو.

وتشمل خطة الهجوم مساعدة عملاء من الداخل لسحب المواد خلال نقلها. وتشمل مراحل الهجوم ما يلي:

- اعتراض عملية النقل؛
- سحب كمية صغيرة من المواد المشعة المشحونة؛
- إعادة برمجة شريحة تحديد الهوية باستخدام موجات الراديو لتعرض الكمية الفعلية الباقية؛
- تعديل نظام متابعة الرصيد ليعرض الكمية الجديدة على أنها قيد الشحن باعتبار أن الكمية المسروقة ما زالت قابعة في المخزن الأصلي.

ويركّز الهجوم الحاسوبي على تأمين الوصول الشبكي إلى قاعدة البيانات الخاصة بالأرصدة وعلى تعديل سجلات الرصيد والانتقال.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

المرفق الثاني
منهجية لتعيين المتطلبات الخاصة بالأمن الحاسوبي

عملية تعيين التهديدات التي قد تضرّ بالأمن الحاسوبي في مرفق نووي أو التحكم بهذه التهديدات أو إزالتها أو تدنيتها ينبغي أن تُنفَّذ بشكل منهجي ومتساوق وفقاً للمعايير القائمة. ويقدّم هذا المرفق رؤيا أكثر عمقاً عن إحدى المنهجيات المعيّنة. واختيار هذه المنهجية بدلاً من المنهجيات العديدة المتاحة لا يعني ضمناً أن الوكالة تؤيدها، وينبغي اعتبارها على أنها مثال مفصّل ليس إلاّ. وللحصول على تعريف عام بمبادئ تقييم المخاطر، يرجى الرجوع إلى الفقرة ٦–١.

وعلى وجه العموم، للتمكن من فهم التهديدات ومواطن الضعف التي تشوب نظاماً محوسباً معيّناً، يلزم أولاً تحليل النظام، من الناحيتين الوظيفية والتقنية، وتحديد عوامل الموثوقية ذات الصلة التي يجب الحفاظ عليها. وبعد ذلك، يلزم تحديد المخاطر المرتبطة بهذه العوامل وتحليلها.

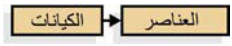
وتتضمن الفقرات التالية لمحة عامة عن وسيلة EBIOS. و'EBIOS' هو مختصر فرنسي يعني *تعبير عن الاحتياجات وتحديد الأهداف الأمنية* (expression des besoins et identification des objectifs de sécurité). وهذه الوسيلة هي من تصميم الإدارة المركزية الفرنسية لأمن نظم المعلومات (DCSSI – Direction Centrale de la Sécurité des Systèmes d'Information).[1]

وتتيح وسيلة EBIOS نهجاً ذا طابع رسمي لتقييم المخاطر ومعالجتها ضمن ميدان أمن نظم المعلومات، وهي تشمل أدوات دعم التعاقد مع السلطات، وصياغة الوثائق، ورفع مستوى الوعي.

ولا نستعرض هنا سوى المبادئ الأساسية لهذا النهج التي اقتبسناها عن الوثائق المتاحة على موقع الدعم الإلكتروني للإدارة المركزية لأمن نظم المعلومات.

مبادئ وسيلة EBIOS

دراسة السياق وتحديد الإطار



[1] وسائل لتحقيق أمن نظم المعلومات:
http://www.ssi.gouv.fr/site_rubrique113.html

وتتمثل الخطوة الأولى في رسم إطار السياق التقني والتجاري والرقابي للدراسة. وعلى وجه الخصوص، تقوم نظم المعلومات على أساس عناصر ووظائف ومعلومات جوهرية تشكّل القيمة المضافة التي تحققها نظم المعلومات بالنسبة للمنظمة.

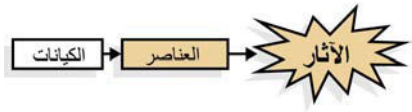
وعلى سبيل المثال، يعتمد نظام لرصد نظام تبريد محطة قوى على مفردات معلومات متنوّعة من قبيل التدابير والبارامترات ونتائج الحوسبة، كما يعتمد على وظائف متنوّعة تتيح الاضطلاع بهذه الحوسبة.

ويتم ربط العناصر الجوهرية بمجموعة من **الكيانات** المختلفة الأنواع: الأجهزة الحاسوبية والبرامج الحاسوبية والشبكات والمنظمات والموارد البشرية والمواقع.

لنأخذ مثال بارامتر مستخدم لاستهلال تشغيل إحدى المضخات المعيّنة ضمن نظام التبريد. ويتم ربط هذا البارامتر بحواسيب المراقبة، والبرامج الحاسوبية المعالِجة، والمشغلين، وحالة المصادر الباردة، وحالة المحطة، والقواعد التنظيمية السارية، وغيرها من الأمور.

الحصيلة: هدف الدراسة (السياق + العناصر + الكيانات).

التعبير عن مستويات الحساسية



لضمان التشغيل السليم للمحطة، يجب التعبير عن مستوى **حساسية** كلٍّ من العناصر الجوهرية.

ويقوم التعبير على أساس مجموعة متنوّعة من **المعايير الأمنية** من قبيل اللياقة التشغيلية والسلامة والسرية. وفي حال عدم تغطية هذه الحساسية، تتعرّض المنظمة **لآثار** قد تأخذ أشكالاً متنوّعة، من قبيل انتهاكات الأمن النووي، أو إضعاف مستوى الأمان، أو الإخلال بعمل الأنشطة، أو فقدان ثقة العملاء، أو الخسائر المالية.

وبالعودة إلى مثال بارامتر استهلال عمل المضخة لنظام تبريد محطة القوى، ينبغي لمتطلب اللياقة التشغيلية والسلامة بالنسبة لهذه المعلومات أن يكون عالي المستوى بغية تفادي أي أثر ضار على المواد أو البيئة أو الموظفين وكذلك على اللياقة التشغيلية للمحطة.

الحصيلة: مستويات الحساسية.

دراسة التهديدات

تتعرض كل منظمة لمجموعة متنوّعة من عوامل التهديد المرتبطة ببيئتها الطبيعية وثقافتها وصورتها ومجال نشاطها وما إلى ذلك. ويمكن تصنيف عامل التهديد بناءً على نوعه (طبيعي أو بشري أو بيئي) وبناء على سببه (عرضي أو مقصود).

ويمكن لعامل التهديد أن يستخدم مجموعة متنوعة من **وسائل الهجوم** التي يلزم بالتالي تحديدها. ويتم تصنيف وسيلة الهجوم بناءً على الخصائص الأمنية (اللياقة التشغيلية أو السلامة أو السرية، على سبيل المثال) التي يمكنها أن تنتهكها وبناءً على عوامل التهديد المرجّحة.

وبالعودة إلى المثال، يجب على محطة للقوى النووية أن تراعي عدداً كبيراً من عوامل التهديد، وفقاً لما تمت مناقشته في الفقرة ٦–٣:

- سارقو تجسس/تكنولوجيا؛
- موظف/مستخدم ساخط (داخلي أو خارجي)؛
- قرصان يسعى إلى التسلية؛
- ناشط إلكتروني؛
- جريمة منظمة؛
- دولة قومية؛
- إرهابي.

وأيضاً وسائل هجوم:

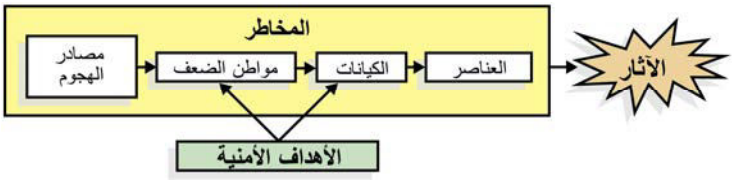
- تنصت؛
- إغراق/رفض خدمة؛
- أحبولة برنامجية/باب خلفي برنامجي؛
- هجمات على تسجيل الدخول/كلمات المرور (قوة غاشمة، قاموس، إلخ).

لكل كيان **مواطن ضعف** يمكن لعوامل التهديد استغلالها باستخدام وسائل الهجوم ذات الصلة. ويمكننا بالتالي أن نسلط الضوء على عدة مواطن ضعف مرتبطة بنظام تبريد محطة القوى النووية:

- إمكان وجود وظائف مخفية تم إدخالها خلال مرحلة التصميم والتطوير (برامج حاسوبية)؛
- استخدام معدات غير مقيّمة (أجهزة حاسوبية)؛
- إمكانية استحداث أو تعديل أوامر تحكم بالنظام عبر الإنترنت (شبكات)؛
- الشبكة، التي يمكن استخدامها للتلاعب بالبرامج الحاسوبية الخاصة بموارد النظام (شبكات)؛
- سهولة اختراق الموقع باستخدام طرقات وصول غير مباشرة (مبانٍ)؛
- تخلف المشغل عن الامتثال للتعليمات (موظفون)؛
- عدم وجود تدابير أمنية خلال مراحل التصميم والتركيب والتشغيل (منظمة)؛

الحصيلة: تشكيل التهديد (بما يشمل السيناريوهات).

التعبير عن الأهداف الأمنية



حدِّدوا الآن كيف يمكن للعناصر الجوهرية أن تتأثر بعوامل التهديد وبوسائل الهجوم الخاصة بها: هذا هو **الخطر**.

ويمثّل الخطرُ الآثارَ الممكنة. وهو ينشأ عن أنه يمكن لعامل تهديد أن يضرّ بالعوامل الجوهرية عن طريق استخدام وسيلة معيّنة من وسائل الهجوم لاستغلال مواطن ضعف الكيانات التي تعتمد عليها هذه العناصر.

ويتضمن المثال خطرَ انتهاك معلومات حساسة نتيجة أحبولة برنامجية ناشئة عن إمكانية استحداث أو تعديل أوامر تحكم بالنظام مربوطة بالشبكة، ممّا قد يخلف أثراً على المواد والبيئة وأمان الموظفين واللياقة التشغيلية للمحطة وثقة الجمهور.

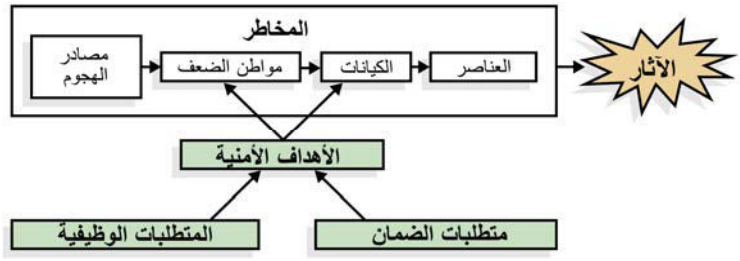
وتتمثل الأهداف الأمنية، بشكل رئيسي، في تغطية مواطن ضعف الكيانات التي تمثّل جميع المخاطر التي تمت مراعاتها. ومن الواضح أن لا داعي لحماية ما هو غير معرّض.

ولكن، مع تزايد المخاطر المحتملة، يجب أيضاً زيادة شدة الأهداف الأمنية. وبالتالي، تشكل هذه الأهداف مجموعةً فائقة التكييف من المواصفات.

ويتمثل أحد الأهداف الأمنية الخاصة بمحطة القوى النووية المعنية بالمثال في حماية عملية استحداث وتعديل أوامر التحكم بالنظام المرتبطة بالشبكة الخاصة بنظام التبريد.

الحصيلة: الأهداف الأمنية.

تحديد المتطلبات الأمنية



يجب عندئذ على الفريق المسؤول عن تنفيذ النهج أن يقدّم مواصفات دقيقة للوظائف الأمنية المطلوبة. وبعد ذلك، يجب عليه أن يبرهن أن الأهداف الأمنية مشمولة تماماً في هذه **المتطلبات الوظيفية**.

في المثال، يمكن للمتطلبات الوظيفية لحماية استحداث وتعديل أوامر التحكم بالنظام المرتبطة بالشبكة أن تشمل ما يلي:

- سلسلة من الاختبارات الذاتية يجريها النظام دورياً خلال التشغيل العادي للبرهنة عن أن النظام يعمل بشكل صحيح؛
- التحكم المادي والمنطقي بالوصول.

وبالنهاية، يجب على الفريق المسؤول أن يحدّد **متطلبات الضمان** التي تتيح بلوغ المستوى المطلوب من الثقة ومن ثم البرهنة عن بلوغ المستوى المطلوب.

ويمكن لأحد متطلبات الأمان أن يتمثل في أن على مطوّر البرامج أن يضطلع بتحليل مقاومة لوظائف أمن النظام على المستوى المطلوب من المقاومة.

الحصيلة: المتطلبات الوظيفية ومتطلبات الضمان.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

المرفق الثالث

دور الأخطاء البشرية في الأمن الحاسوبي

يتطرق هذا المرفق إلى مسائل الأداء البشري المرتبطة بالأمن الحاسوبي؛ وهو يتناول بشكل خاص كيف يمكن للأداء البشري أن يؤثر على قدرة المنظمة على مقاومة الهجمات، والتعرف إلى الهجمات، واستعادة البيانات/الخدمات الجوهرية، والتكيّف ضد التهديدات الناشئة. تتواصل البحوث سعياً إلى وضع الحلول التقنية من قبيل البرامج الحاسوبية لمراقبة الأمن، وبرامج كشف/منع الاختراقات، ونظم أكثر تشدداً للتحقق من الهوية، ووسائل تشفير أكثر مقاومةً، ولكن في الغالب جداً ما يتم تجاهل العنصر البشري باعتباره، على حد سواء، سبباً وتدبيراً وقائياً في ميدان الأمن الحاسوبي.

وقد اعتبرت تقارير عديدة أن الخطأ البشري هو السبب الرئيسي لانتهاكات الأمن الحاسوبي. ووفقا للتقديرات الأخيرة، فإن معدل الانتهاكات ذات الصلة بالخطأ البشري يتراوح بين ٦٠ و٨٠%. ولكان من الممكن تفادي غالبية هذه الأخطاء بفضل العمل بشكل أكبر على زيادة الوعي واعتماد مستوى أعلى من الحرص في مجالي التشغيل والإشراف.

ويتمثل أحد أهداف برامج الأمن الحاسوبي في ضمان قدرة النظام/التشغيل على البقاء. وعناصر قدرة النظام على البقاء هي التالية:

- قدرة النظام على مقاومة الهجمات؛
- الإقرار بحصول الهجوم وتقييم الأضرار؛
- استعادة القدرة على توفير الخدمات الأساسية والخدمات الكاملة؛
- تكيّف النظام وتطوّره كوسيلة للدفاع ضد الهجمات المستقبلية.

يبرز الجدول ثالثاً–١ مجالات التركيز هذه مع محاولةٍ لتصنيف الأنواع الشائعة من الأخطاء البشرية وفقاً للعمليات والتطبيقات. ويتم تسجيل ارتكاب الأخطاء البشرية بواسطة المسؤولين عن إدارة النظام ومستخدميه على حد سواء. وليس المقصود من هذه القائمة أن تكون شاملة كاملة، بل القصد منها هو إبراز مستوى التفاعل البشري المرتبط بتنفيذ هذه النظم والعمليات.

وفيما يركّز الجدول على الجوانب السلبية للأداء البشري، يجب أيضاً ملاحظة الأثر الإيجابي الناتج عن الأداء البشري. فحتى لو كان المشغّل البشري أو الموظف، في بعض الأحيان، أضعف حلقة في السلسلة، يمكنه أن يشكل حاجزاً يتيح تفادي تعطل النظام أو انتهاكه. ولن تكون التكنولوجيا أبداً الحل الكامل. والموظفون هم إحدى طبقات استراتيجيةٍ للدفاع في العمق لكفالة أمن النظام/قدرة النظام على البقاء. وتبرهن الاستبيانات المنتظمة أن أعظم المسائل المضرة بالأمن هو عدم كفاية الوعي والتدريب في ميدان الأمن الحاسوبي.

الجدول ثالثاً–١ – الأخطاء البشرية الشائعة

العملية/التطبيق	الأخطاء البشرية الشائعة
القدرة على مقاومة الهجمات	
تقييد الوصول (إدارة النظام)	— عدم ملاءمة تصاريح الملفات. — إبقاء خدمات غير ضرورية قيد التشغيل. — إبقاء منافذ ضعيفة مفتوحة. — منح السماح بالوصول المادي. — التخلف عن حماية برامج وقاية الشاشات بواسطة كلمات سر. — التخلف عن تنصيب إصلاحات النظام. — التخلف عن فهم أهمية تنصيب إحدى الإصلاحات الحاسوبية. — تنزيل/تنصيب برامج حاسوبية كيدية/محرّفة.
استحداث/استخدام كلمات السر	— تدوين كلمات السر على أوراق. — كلمات سر ضعيفة. — استخدام كلمات سر معيارية. — إفشاء كلمة السر. — عدم استخدام كلمة سر. — استخدام كلمة السر ذاتها على نظم مأمونة وغير مأمونة على حد سواء.
الإقرار بحصول الهجوم والضرر	
نظم الكشف عن حالات الاقتحام	— اعتماد أنساق (مجموعات قواعد) غير ملائمة. — التخلف عن تنفيذ ترقيات النظام. — نقص اليقظة عند استعراض السجلات.
تدقيق السجلات	— التخلف عن الاستعراض الحريص للسجلات. — عدم ملاحظة التوجّهات على مدى فترات تسجيل متعددة.
استعادة النظام	
النسخ الاحتياطية واستعادة البيانات	— التخلف عن حفظ نسخ احتياطية. — التخلف عن حفظ نسخ احتياطية في التوقيت المناسب. — اعتماد أنساق غير ملائمة. — إلحاق أضرار مادية بوسائط حفظ النسخ الاحتياطية. — حذف البيانات عن طريق الخطأ. — خزن وسائط حفظ النسخ الاحتياطية في أماكن غير مؤمّنة/غير محمية. — استخدام وسائط معيبة. — الإخطاء في وضع ملصقات التعريف بالوسائط. — التدمير المادي للوسائط. — التخلف عن اختبار إجراءات الاستعادة. — التخلف عن حفظ نسخ متعددة عن المعلومات الحرجة الخاصة بالنظام. — التخلف عن خزن وسائط حفظ النسخ الاحتياطية في مكان خارج الموقع.

الجدول ثالثاً–١ – الأخطاء البشرية الشائعة

العملية/التطبيق	الأخطاء البشرية الشائعة
التكيّف مع التهديدات الجديدة	
إجراءات الشركات	— التخلف عن معرفة سياسة الشركة. — انتهاك سياسة الشركة. — الافتقار إلى سياسة استعادة خاصة بالشركة. — استخدام سياسة مرّ عليها الزمن. — التخلف عن التحقق من عمل السياسة/الإجراء. — التخلف عن إنفاذ السياسة.

للتمكن من الاستفادة بالشكل التام من الموظفين كأحد أصول الأمن الحاسوبي وقدرة النظام على البقاء، فإنهم يحتاجون إلى ما يلي:

— فهم راسخ لأهمية دورهم في الخطة الشاملة للأمن الحاسوبي؛
— المعارف والمهارات الخاصة بالأمن الحاسوبي الضرورية لتغطية مسؤولياتهم؛
— إدراك أن ثقافة أمن فعّالة تبدأ عندهم.

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

التعاريف

لأغراض هذا المنشور، تستخدم المصطلحات التالية وفقاً للمعاني المحددة لكل منها فيما يلي. ويجوز لهذه التعاريف أن تختلف عن تلك المستخدمة في سياقات أخرى. وعند توافرها، تقتبس التعاريف عمّا يرد في المنشورات القائمة الصادرة عن الوكالة، على الرغم من أن بعضها يستخدم هنا وفقاً للسياق الخاص بالأمن الحاسوبي. وتقتبس تعاريف أخرى من معايير دولية (على سبيل المثال، المراجع [١ و١٥ و٢٣] الواردة في هذا المنشور).

مراقبة الدخول. وسائل تضمن أن الوصول إلى الأصول مرخّص به ومقيّد وفقاً لمتطلبات الأعمال والمتطلبات الأمنية (المنظمة الدولية لتوحيد المقاييس).

هجوم. محاولة لتدمير أصل ما أو تعريضه أو تعديله أو إضعافه أو سرقته أو الوصول إليه من دون ترخيص أو استخدامه استخداماً غير مرخّص به (المنظمة الدولية لتوحيد المقاييس).

توثيق. توفير التأكيد بشأن صحة الخاصية المزعومة لكيان ما (المنظمة الدولية لتوحيد المقاييس).

لياقة تشغيلية. أن يكون الأصل متاحاً وقابلاً للاستعمال عند الطلب بواسطة كيان مرخص له (المنظمة الدولية لتوحيد المقاييس).

أمن حاسوبي. جانب معيّن من جوانب أمن المعلومات وهو معني بالنظم القائمة على أساس الحواسيب، والشبكات، والنظم الرقمية.

حادثة أمن حاسوبي. واقعة تؤدي إلى التقويض الفعلي أو المحتمل لسرية أو سلامة أو اللياقة التشغيلية الخاصة بنظام معلومات حاسوبي أو مشبّك أو رقمي أو بالمعلومات التي يعالجها هذا النظام أو يخزنها أو ينقلها، أو واقعة تشكل انتهاكاً أو خطراً وشيكاً بانتهاك السياسات الأمنية أو الإجراءات الأمنية أو السياسات الخاصة بالاستخدام المقبول.

محيط الأمن الحاسوبي. الحدود المنطقية المقامة حول شبكة تتصل بها أصول حرجة ويتم التحكم بالوصول إليها.

سياسة الأمن الحاسوبي. مجموعة الإرشادات واللوائح والقواعد والممارسات التي تنص على كيفية قيام منظمة ما بإدارة وحماية حواسيبها ونظمها الحاسوبية.

سرية. خاصية عدم إتاحة المعلومات أو الإفشاء بها لأفراد أو كيانات أو عمليات غير مرخص بها (المنظمة الدولية لتوحيد المقاييس).

تدبير مضاد. إجراء متّخذ لإبطال تهديد، أو للتخلص من مواطن ضعف أو التقليل منها.

دفاع في العمق. توليفة من طبقات متتالية من النُظم والتدابير لحماية الأهداف من التهديدات المحدقة بالأمن النووي.

أمن المعلومات. الحفاظ على سرية المعلومات وسلامتها وتوافرها.

ملحوظة: فضلاً عمّا تقدم، يمكن أيضاً أن تشمل خصائص أخرى من قبيل الأصالة، وقابلية المساءلة، وعدم التنصل، والموثوقية (المنظمة الدولية لتوحيد المقاييس).

سلامة. خاصية حماية دقة الأصول واكتمالها (المنظمة الدولية لتوحيد المقاييس).

الحاجة إلى المعرفة. مبدأ تتاح من خلاله للمستخدمين والعمليات والنظم إمكانية الوصول فقط إلى المعلومات والإمكانيات والأصول اللازمة لتنفيذ الوظائف المرخص لهم بتنفيذها.

مرفق نووي. مرفق (بما في ذلك ما يرتبط به من مبان ومعدات) يتم فيه إنتاج مواد نووية أو معالجتها أو استخدامها أو مناولتها أو خزنها أو التخلّص منها ويلزمه لذلك الحصول على إجازة أو رخصة.

مخاطرة/ خطر. احتمال قيام تهديد معيّن باستغلال نقاط ضعف أحد الأصول أو مجموعة من الأصول، وبالتالي إلحاق الضرر بالمنظمة. وتقاس المخاطر/الأخطار على أساس المزج بين احتمال حصول حدث ما وبين فداحة عواقبه.

تقييم المخاطر. عملية شاملة تشمل القيام منهجياً بتحديد خطر ما وتقديره وتحليله وتقويمه.

هندسة اجتماعية. شكل غير تقني من أشكال جمع المعلومات أو هجوم يعتمد على التفاعل البشري للتلاعب بالناس ودفعهم إلى الإخلال غير المتعمد بالإجراءات الأمنية، من قبيل إفشاء المعلومات أو تنفيذ أعمال أخرى ذات أثر أمني.

تهديد. سبب محتمل لحصول حادثة غير مرغوب بها، ممّا قد يؤدي إلى إلحاق الضرر بنظام ما أو منظمة ما (المنظمة الدولية لتوحيد المقاييس).

ملحوظة: في منشورات أخرى ضمن سلسلة الأمن النووي الصادرة عن الوكالة، تم نموذجياً تعريف 'التهديد' على أنه 'شخص أو مجموعة أشخاص لديهم الحافز والنية والقدرة على ارتكاب عمل كيدي'. ولكن هذا المنشور يستخدم المصطلح ضمن سياق الأمن الحاسوبي؛ حيث لا يكون التهديد بالضرورة ناجماً عن شخص أو أشخاص.

موطن ضعف. نقطة ضعف أحد الأصول أو أحد نظم التحكم يمكن استغلالها بواسطة تهديد ما (المنظمة الدولية لتوحيد المقاييس).

أُلغي هذا المنشور وحلَّ محلَّه العدد (No. 17-T (Rev. 1.

أُلغي هذا المنشور وحلَّ محلَّه العدد (Rev. 1) No. 17-T.

12-12796

أُلغي هذا المنشور وحلَّ محلَّه العدد (Rev. 1) No. 17-T.

ألغي هذا المنشور وحلّ محلّه العدد (No. 17-T (Rev. 1.

يهدف هذا المنشور إلى التوعية بشأن أهمية إرساء الأمن النووي كجزء لا يتجزّأ من الخطة الشاملة للأمن في المرافق النووية. وهو يهدف أيضاً إلى تزويد المرافق النووية بإرشادات خاصة بتنفيذ برنامج للأمن الحاسوبي، وإسداء المشورة بشأن تقييم البرامج القائمة وتقدير قيمة الأصول الرقمية الحرجية وتحديد التدابير الملائمة لتقليص المخاطر.

الوكالة الدولية للطاقة الذرية
فيينا

ISBN 978–92–0–642210–6
ISSN 1816–9317