الاتحـــاد الـدولـــي للاتصـــالات

ITU-T M.3016.1

(2005/04)

قطـاع تقييس الاتصـالات
في الاتحاد الدولي للاتصالات

السلسلة M: إدارة الاتصالات، بما في ذلك إدارة شبكة الاتصالات (TMN) وصيانة الشبكات

شبكة إدارة الاتصالات

أمن مستوي الإدارة: متطلبات الأمن

التوصيـة ITU-T M.3016.1

الاتحاد الدولي للاتصالات

توصيات السلسلة M الصادرة عن قطاع تقييس الاتصالات

إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات

مقدمة ومبادئ عامة بشأن الصيانة وتنظيمها	M.10 - M.299
أنظمة الإرسال الدولية	M.300 - M.559
الدارات الهاتفية الدولية	M.560 - M.759
أنظمة التشوير على قناة مشتركة	M.760 - M.799
أنظمة الإبراق الدولية وإرسال الصور برقياً	M.800 - M.899
وصلات الزمر والزمر الثانوية المؤجرة الدولية	M.900 - M.999
الدارات الدولية المؤجرة	M.1000 - M.1099
أنظمة وخدمات الاتصالات المتنقلة	M.1100 - M.1199
الشبكة الدولية للهواتف العمومية	M.1200 - M.1299
الأنظمة الدولية لإرسال المعطيات	M.1300 - M.1399
تبادل التسميات والمعلومات	M.1400 - M.1999
شبكة النقل الدولية	M.2000 - M.2999
شبكة إدارة الاتصالات	**M.3000 - M.3599**
الشبكات الرقمية متكاملة الخدمات	M.3600 - M.3999
أنظمة التشوير على قناة مشتركة	M.4000 - M.4999

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـة ITU-T M.3016.1

أمن مستوي الإدارة: متطلبات الأمن

موجز

تحدد هذه التوصية متطلبات أمن مستوي الإدارة في مجال إدارة الاتصالات. وتركز تحديداً على الجانب الأمني لمستوي إدارة عناصر الشبكة (NE) وأنظمة الإدارة التي تشكل جزءاً من البنية الأساسية للاتصالات.

المصدر

وافقت لجنة الدراسات 4 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 أبريل 2005 على التوصية M.3016.1 بموجب الإجراء الوارد في التوصية A.8.

تمهيـد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB).

جـدول المحتـويات

الصفحة

مقدمة

تمثل الاتصالات بنية أساسية بالغة الأهمية للاتصال والاقتصاد العالميين. ومن الضروري توفير الأمن اللازم لوظائف الإدارة التي تتحكم في هذه البنية. وتوجد عدة معايير لتحقيق الأمن فيما يتعلق بإدارة شبكة الاتصالات. ومع ذلك، فإن التقيد بذه المعايير متدن، وعمليات تطبيقها لا تتفق مع مختلف مكونات المعدات والبرمجيات المستخدمة في الاتصالات. وتحدد هذه التوصية متطلبات الأمن لإفساح المال أمام الجهات البائعة، والوكالات، ومقدمي الخدمات لتنفيذ بنية أساسية آمنة لإدارة الاتصالات. وعلى الرغم من أن هذه المموعة من المتطلبات تمثل الفهم الحالي لآخر ما تم التوصل إليه في هذا المال، فإن التكنولوجيات آخذة في التقدم والظروف آخذة في التغير. ومن أجل تكليل هذه التوصية بالنجاح، يجب أن تكون قابلة للتطور بحسب ما تقتضيه الظروف. والغرض من هذه التوصية هو الاستناد إليها كأساس. ويمكن أن يدرج مقدمو الخدمات متطلبات إضافية في التوصية لتلبية احتياجاتم الخاصة علاوة على تلك التي تتناولها التوصية.

وهذه التوصية هي جزء من توصيات السلسلة ITU-T M.3016.x والرامية إلى تقديم إرشادات ونصائح بشأن تأمين مستوي إدارة الشبكات المتطورة، وهي:

- التوصية ITU-T M.3016.0 – أمن مستوي الإدارة: نظرة عامة.
- التوصية ITU-T M.3016.1 – أمن مستوي الإدارة: متطلبات الأمن.
- التوصية ITU-T M.3016.2 – أمن مستوي الإدارة: خدمات الأمن.
- التوصية ITU-T M.3016.3 – أمن مستوي الإدارة: آلية الأمن.
- التوصية ITU-T M.3016.4 – أمن مستوي الإدارة: نموذج الملامح العامة.

التوصيـة ITU-T M.3016.1

أمن مستوي الإدارة: متطلبات الأمن

1 مجال التطبيق

تحدد التوصية M.3016.1-3 من توصيات السلسلة M الصادرة عن قطاع تقييس الاتصالات (ITU-T) مجموعة من المتطلبات والخدمات والآليات الرامية إلى تحقيق الأمن المطلوب للوظائف الإدارية اللازمة لدعم البنية الأساسية للاتصالات. وبالنظر إلى ما تحتاجه الإدارات والمنظمات المختلفة من مستويات دعم متباينة في ميدان الأمن، لا تحدد التوصية M.3016.1-3 ما إذا كانت هذه المتطلبات، الخدمات/أو الآليات إلزامية أم اختيارية.

وتحدد هذه التوصية متطلبات أمن مستوي الإدارة في مجال إدارة الاتصالات. وتركز تحديداً على الجانب الأمني لمستوي إدارة عناصر الشبكة (NE) وأنظمة الإدارة (MS) التي تشكل جزءاً من البنية الأساسية للاتصالات.

وتتسم هذه التوصية بطابع تنوعي ولا تحدد المتطلبات اللازمة لسطح بيني معين لشبكة إدارة الاتصالات (TMN) أو تتطرق إلى هذه المتطلبات.

ويقدم نموذج الملامح العامة المحدد في التوصية ITU-T M.3016.4 لمساعدة المنظمات والإدارات وغيرها من المنظمات الوطنية/الدولية في تحديد الطابع الإلزامي أو الاختياري لدعم المتطلبات إلى جانب تحديد مدى القيم، القيم، وغير ذلك، من أجل مساعدة هذه المنظمات والوكالات على تنفيذ سياساتا الأمنية.

1.1 الغرض من الوثيقة

تحدد التوصية ITU-T M.3016.0 عدداً من الأهداف بخصوص تأمين شبكة الإدارة وبشأن التهديدات التي تشكل مخاطر تحدق بتحقيق هذه الأهداف. وتستمد هذه التوصية المتطلبات اللازمة من الأهداف المنشودة في مواجهة التهديدات، وتحدد خدمات الأمن التي تواجه هذه المتطلبات. وتستخدم آليات قائمة على خوارزميات معينة عند تحديدها لهذه الخدمات. وتستند التوصيات الأخرى التابعة لهذه السلسلة إلى الهيكل المحدد في النظرة العامة الواردة في التوصية ITU-T M.3016.0. وتقدم هذه التوصية الدعم لمختلف الخطوات اللازمة لتأمين مستوي الإدارة.

2.1 علاقة التوصية بمعمارية الأمن المحددة في التوصية X.805

تحدد التوصية ITU-T X.805 معمارية الأمن اللازمة لتحقيق أمن الاتصال من طرف إلى طرف عبر الشبكة. واستناداً إلى المنطق، تقسم معمارية الأمن هذه مجموعة مركبة من الخصائص المتعلقة بأمن الاتصال من طرف إلى طرف عبر الشبكة إلى ثلاثة مكونات معمارية مستقلة هي أبعاد الأمن وطبقاته ومستوياته (انظر الشكل 2/التوصية X.805). ويتمثل بُعد الأمن في مجموعة من قياسات الأمن المصممة لمعالجة جانب معين من جوانب أمن الشبكة. وتحدد التوصية ITU-T X.805 ثلاث طبقات للأمن هي: طبقة أمن البنية الأساسية، وطبقة أمن الخدمات، وطبقة أمن التطبيق، التي تعتمد بعضها على بعض لتقديم حلول قائمة على الشبكة. ومستوي الأمن هو نمط معين من أنشطة الشبكة المحمية بأبعاد الأمن. وتحدد التوصية X.805 ثلاثة مستويات أمن هي: مستوي الإدارة، ومستوي التحكم، ومستوي المستعمل النهائي. ومن أجل تقديم حل شامل، ينبغي تطبيق قياسات الأمن (مثل مراقبة النفاذ واستيقانه) على كل نمط من أنشطة الشبكة (أي نشاط مستوي الإدارة، ونشاط مستوي التحكم، ونشاط مستوي المستعمل النهائي) فيما يخص البنية الأساسية للشبكة، والخدمات التي تقدمها الشبكة، والتطبيقات المتعلقة بـا. وتركز هذه التوصية تحديداً على الجانب الأمني لمستوي إدارة عناصر الشبكة (NE) وأنظمة الإدارة (MS) التي تشكل جزءاً من البنية الأساسية للاتصالات.

3.1 علاقة التوصية بمتطلبات أمن شبكات الاتصالات المحددة في التوصية E.408

تقدم التوصية ITU-T E.408 نظرة عامة على متطلبات الأمن وإطاراً يحدد التهديدات الأمنية التي تواجهها شبكات الاتصالات عموماً (الثابتة والمتنقلة؛ الهاتفية منها والمعطياتية على حد سواء) وتقدم إرشادات بشأن ما يمكن اتخاذه من تدابير مضادة في ميدان التخطيط من أجل التخفيف من وطأة المخاطر الناجمة عن التهديدات المحدقة بالأمن. وتتسم هذه التوصية بطابع عام ولا تحدد المتطلبات المتعلقة بشبكات معينة أو تتطرق إلى هذه المتطلبات. وتحدد سلسلة التوصيات M.3016.x متطلبات وخدمات وآليات الأمن اللازمة لشبكة الاتصالات، أي مستوى الإدارة عموماً في إدارة الاتصالات.

2 المراجع

تضم التوصيات التالية وسائر المراجع الصادرة عن قطاع تقييس الاتصالات (ITU-T) أحكاماً تشكل، من خلال الإشارة إليها في هذا النص، أحكاماً تتعلق بذه التوصية. وكانت الطبعات المشار إليها سارية المفعول في وقت نشرها. غير أنه يجري تنقيح جميع التوصيات والمراجع الأخرى؛ ولذلك، يُشجع مستعملو هذه التوصية على تقصي إمكانية تطبيق أحدث طبعة من التوصيات وسائر المراجع المدرجة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات (ITU-T) السارية المفعول في وقت صدور القائمة. وورود إشارة إلى وثيقة معينة في هذه التوصية لا يمنحها، كوثيقة قائمة بذاتها، صفة التوصية

- التوصية ITU-T E.408 (2004)، *متطلبات أمن شبكات الاتصالات*.
- التوصية ITU-T G.8080/Y.1304 (2001)، *معمارية الشبكة البصرية المبدلة أوتوماتياً (ASON)*، بالإضافة إلى التعديل 2 (2005).
- التوصية ITU-T M.3010 (2000)، *مبادئ شبكة إدارة الاتصالات*.
- التوصية ITU-T M.3013 (2000)، *اعتبارات خاصة بشبكة إدارة الاتصالات*.
- التوصية ITU-T M.3016.0 (2005)، *أمن مستوي الإدارة: نظرة عامة*.
- التوصية ITU-T M.3016.2 (2005)، *أمن مستوي الإدارة: خدمات الأمن*.
- التوصية ITU-T M.3016.3 (2005)، *أمن مستوي الإدارة: آلية الأمن*.
- التوصية ITU-T M.3016.4 (2005)، *أمن مستوي الإدارة: نموذج الملامح العامة*.
- التوصية ITU-T X.509 (2000)، *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - الدليل: أطر التصديق العمومية الرئيسية وتصديق النعوت*، بالإضافة إلى التصويب التقني 1، والتصويب التقني 2 (2002)، والتصويب التقني 3 (2003).
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف*.
- التوصية ITU-T X.805 (2003)، *معمارية أمن الأنظمة التي تكفل الاتصالات من طرف إلى طرف*.
- الوثيقة IETF RFC 1750 (1994)، *التوصيات المتعلقة بالعشوائية في مجال الأمن*.

3 المصطلحات والتعاريف

تستخدم هذه التوصية المصطلحات التالية المستمدة من التوصيتين G.8080/Y.1304 الصادرتين عن قطاع تقييس الاتصالات (ITU-T)، وهي:

- مستوي التحكم؛
- مستوي الإدارة؛
- مستوي النقل.

وتستعمل هذه التوصية المصطلحين التاليين المأخوذين عن التوصية ITU-T M.3010، وهما:

- نظام الإدارة؛

- عنصر الشبكة.

وتستخدم هذه التوصية المصطلح التالي المستمد من التوصية ITU-T M.3013، وهو:

- نظام إدارة العناصر.

وتستعمل هذه التوصية المصطلح التالي المأخوذ عن التوصية ITU-T X.509، وهو:

- الاستيقان الشديد.

وتستخدم هذه التوصية المصطلحين التاليين المستمدين من التوصية ITU-T X.800، وهما:

- مراقبة النفاذ؛
- الاستيقان.

وتحدد هذه التوصية المصطلح التالي:

1.3 **أهم إجراءات إدارة الأمن**؛ والتي تشتمل على ما يلي، ولكنها ليست مقصورة عليه:

أ) تحديد امتيازات المستعمل وتخصيصها؛

ب) إضافة معرفات هوية (IDs) المستعملين وحذفها؛

ج) تعطيل استخدام معرفات هوية (IDs) مستعمل معين بوصفها معرفات هوية (IDs) تسجيل الدخول؛

د) تشكيل كلمات السر المستخدمة في تسجيل الدخول وإعادة تحديدها؛

هـ) تشكيل مفاتيح حاملة لرموز سرية وتغييرها؛

و) تحديد عتبة تقادم النظام بالنسبة لكلمات السر المستخدمة في تسجيل الدخول إليه؛

ز) تحديد حد الدخول إلى النظام على أساس عدد محاولات الدخول الفاشلة لكل معرف هوية تسجيل دخول؛

ح) إلغاء إغلاق النظام، أو تغيير قيمة مؤقت إغلاقه؛

ط) تحديد قيمة مؤقت خمول النظام؛

ي) تحديد تشكيلة التسجيل والتشكيل الخاصين بالإنذار المتعلق بأمن النظام؛

ك) إدارة عمليات التسجيل المتعلقة بالأمن؛

ل) تحسين برمجيات الأمن؛

م) إناء أية دورة للمستعمل أو للنظام.

4 المختصرات والصيغ المقتضبة

تستخدم هذه التوصية المختصرات التالية:

AAA الاستيقان والتخويل والمحاسبة *(Authentication, Authorization and Accounting)*

ACS وحدة خدمة مراقبة النفاذ *(Access Control Server)*

ALE الخسارة المتوقعة سنوياً *(Annualized Loss Expectancy)*

ANSI المعهد الأمريكي المعني بالمعايير الوطنية *(American National Standards Institute)*

CO مكتب رئيسي *(Central Office)*

CORBA المعمارية الشائعة لبرمجيات نقل الطلبات إلى الهدف *(Common Object Request Broker Architecture)*

CSI القدرة الشائعة على التشغيل البيني الآمن *(Common Secure Interoperability)*

DoS رفض الخدمة *(Denial of Service)*

EMS نظام إدارة العناصر *(Element Management System)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HAZMAT مواد خطرة *(Hazardous Materials)*

HTTP بروتوكول نقل النصوص الإلكترونية *(HyperText Transfer Protocol)*

IETF فريق مهام هندسة الإنترنت *(Internet Engineering Task Force)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPsec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

IEC/ISO المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية
(International Organization for Standardization/International Electrotechnical Commission)

ITU-T الاتحاد الدولي للاتصالات – قطاع تقييس الاتصالات
(International Telecommunication Union – Telecommunication Standardization Sector)

LAES مراقبة إلكترونية مصرح بها قانونياً *(Lawfully Authorized Electronic Surveillance)*

MS نظام الإدارة؛ سواء كان نظام إدارة العناصر، أم نظام إدارة الشبكة، أم نظام دعم التشغيل[1]
(Management System; any EMS, NMS, or OSS)

NE عنصر الشبكة *(Network Element)*

MS/NE عنصر الشبكة أو نظام الإدارة *(NE or MS)*

NMS نظام إدارة الشبكة *(Network Management System)*

NTP بروتوكول التحديد الدقيق للوقت الفعلي في شبكة الحواسيب *(Network Time Protocol)*

P & OAM العمليات والإدارة والصيانة والتزويد *(Operations, Administration, Maintenance and Provisioning)*

OASIS منظمة تطوير معايير المعلومات المنسقة
(Organization for the Advancement of Structured Information Standards)

OEM جهة أصلية مصنعة للمعدات *(Original Equipment Manufacturer)*

ORB برمجيات نقل الطلبات إلى الهدف *(Object Request Broker)*

OS نظام تشغيل *(Operating System)*

OSS نظام دعم التشغيل *(Operations Support System)*

RFC طلب إبداء تعليقات *(Request for Comments)*

SAML لغة تشفير توكيد الأمن *(Security Assertion Markup Language)*

SNMP البروتوكول البسيط لإدارة الشبكة *(Simple Network Management Protocol)*

SOAP البروتوكول البسيط للنفاذ إلى الهدف *(Simple Object Access Protocol)*

SSH برنامج شل للدخول الآمن *(Secure Shell)*

SSL طبقة مقابس الأمن *(Secure Socket Layer)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TMN شبكة إدارة الاتصالات *(Telecommunications Management Network)*

XML لغة تشفير قابلة للتوسيع *(Extensible Markup Language)*

---

[1] يمكن عموماً استخدام تعبير أنظمة دعم التشغيل (OSS) في نفس سياق استخدامه على أنه أنظمة إدارة (MS) على أي طبقة من تراتب شبكة إدارة الاتصالات.

5 الاصطلاحات

يستعمل في التوصيات ITU-T M.3016.1-3 واصف يحدد مختلف المتطلبات والخدمات والآليات. ويتألف هذا الواصف من وسم واحد من الوسوم التالية المكونة من ثلاثة أحرف متبوعاً برقم، وهي:

- REQ ويستعمل لوصف المتطلب؛
- SER ويستخدم لوصف الخدمة؛
- MEC ويستعمل لوصف الآلية.

6 متطلبات الأمن

يتضمن هذا البند متطلبات الأمن اللازمة للتشغيل والإدارة والصيانة والتزويد (OAM&P) ونظام دعم تشغيل (OSS) مستوي الإدارة.

ويصف الشكل M.3016.0/1 العلاقات بين أهداف الأمن، والتهديدات، والمخاطر، ومتطلبات الأمن وخدماته. كما يصف كيفية استنباط "متطلبات الأمن" من "التهديدات" و"أهداف الأمن" التي سيتم تحقيقها بعد ذلك من خلال مجموعة من خدمات الأمن. وتستفيد هذه "الخدمات"، التي تتصدى للتهديدات، من "آليات" تستفيد بحد ذاتا من "خوارزميات أمنية". ويبين الجدول 1 (الذي هو الجدول M.3016.0/4) العلاقة بين متطلبات الأمن وخدمات الأمن. ومتطلبات الأمن التي يرد وصفها في هذا البند منسقة وفقاً للجدول 1 كالآتي:

- التحقق من الهويات؛
- النفاذ والتخويل المراقبان؛
- حماية السرية؛
- حماية تكاملية المعطيات؛
- المساءلة؛
- التسجيل والتدقيق في مجال الأمن؛
- الإبلاغ عن إنذارات الأمن.

ملاحظة – العودة إلى ما كان عليه الحال بعد انتهاك الأمن هو مجال يخضع للمزيد من البحث.

الجدول M.3016.1/1 - تقابل متطلبات الأمن وخدمات الأمن (الجدول M.3016.0/4)

المتطلب الوظيفي	الخدمة الأمنية
التحقق من الهوية	استيقان المستعمل استيقان الكيان الند استيقان مصدر المعطيات
النفاذ والتخويل المراقبان	طرق النفاذ
حماية سرية المعطيات المخزونة	سرية مراقبة النفاذ
حماية سرية المعطيات المنقولة	السرية
حماية سلامة المعطيات - المعطيات المخزونة	التحكم في النفاذ
حماية سلامة المعطيات - المعطيات المنقولة	السلامة
المساءلة	عدم الانكار
تسجيل الأنشطة	تسجيل تدقيقي
الإبلاغ عن إنذارات الأمن	إنذار الأمن
تدقيق الأمن	تسجيل التدقيق

1.6 التحقق من الهويات

يحقق **الاستيقان** غرضين في مجال تأمين **مستوي الإدارة**، يتمثلان في أنه:

1) يكفل التحقق من هوية الأطراف المتصلة ببعضها، مما يوفر أساساً لإجراء اتصالات خاصة مع الحفاظ الكامل على تكاملية المعطيات وسريتها النظامين؛

2) يوفر آلية أساسية للدخول إلى نظام الإدارة و/أو تدقيق أنشطة الإدارة المضطلع با عبر أي نظام.

1.1.6 استيقان المستعمل، وكلمات السر، ومعرفات هوية (IDs) المستعملين

يتعلق **استيقان** المستعمل **باستيقان** الزبائن المشاركين في إدارة الشبكة. ويتيح **الاستيقان** في هذه الحالة إثبات هوية المستعمل الشرعي ويمنع المستعملين غير الشرعيين من شن هجمات تنكرية. ويتسنى من خلال **الاستيقان** الصحيح تتبع الأنشطة وفرض قيود على المستعملين بشأن الأنشطة أو الأدوار المصرح با مسبقاً مثلما يناقش ذلك البند 3.6.

والحد الأدنى لمتطلبات **الاستيقان** هو استخدام معرف هوية المستعمل **وكلمة سر معقدة** وثابتة. ويمكن استخدام آليات أخرى ما دام القائمون على إدارة عنصر الشبكة (NE)/نظام الإدارة (MS) واثقين من أن قوة مستوى الأمن مكافئة على الأقل للقوة التي يوفرها معرف هوية مستعمل **وكلمة سر معقدة** وسكونية وثابتة. وتشمل الآليات الأخرى التي يمكن أن يُنظر فيها ما يلي:

- معرف هوية مستعمل، **واستيقان عاملين** يستخدمان مولد كلمة سر تستعمل لمرة واحدة؛[2]
- **واستيقان مؤلف من عاملين** يستخدم بطاقة ذكية تُخزن فيها أوراق اعتماد بطريقة محمية.

REQ 1: فيما يتعلق لتسجيل الدخول إلى عنصر الشبكة/نظام الإدارة، ينبغي تقديم الدعم للتسجيل والتدقيق والاستيقان المكثف.

ويمثل REQ 1 متطلب الأمن. ويرد وصف آلية الاستيقان العام في التوصية ITU-T M.3016.3. ومن المتوقع أن يستمر تحسين تقنيات **الاستيقان** وتكنولوجيات الدخول الأحادي.

وفيما يخص الدخول الأحادي المأمون، يواصل البروتوكول تحديه للكيان (الكيانات) من أجل الحصول على أوراق الاعتماد؛ ومع ذلك، قد لا يضطر المستعمل إلى إدخال هذه الأوراق لأنا مخزونة بطريقة ما خزناً مأموناً (مثل خزنا بأسلوب Kerberos).

وتساعد المتطلبات التالية في الحفاظ على تعقد كلمة السر وهي مفيدة في التدقيق والتسجيل.

REQ 2: ينبغي أن يعمل كل عنصر من عناصر الشبكة/نظام الإدارة على تعزيز **الاستيقان** وفقاً لسياسة تنظيمية معينة.

REQ 3: لا بد أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم للحد الأدنى من قواعد التعقيد اللازمة **للاستيقان** وفقاً لسياسة تنظيمية معينة.

REQ 4: من الضروري أن يمنع عنصر الشبكة/نظام الإدارة مستعملاً آخر من تغيير كلمة سر يستخدمها غيره في تسجيل الدخول من دون علم الأخير.

REQ 5: ينبغي لعنصر الشبكة/نظام الإدارة أن يكفل تلقائياً اختلاف كل كلمة سر جديدة تستعمل في تسجيل الدخول عن سابقتها. ولا بد أن تكون درجة الاختلاف قابلة للتعديل وفقاً لسياسة تنظيمية معينة.

ونظراً إلى أن كلمات السر عادة ما تُخزن بواسطة التجفير باتجاه واحد، فإن إدخال كلمة السر القديمة ضروري أيضاً لإفساح المال أمام عنصر الشبكة (NE)/نظام الإدارة (MS) لتحديد درجة الاختلاف بين كلمتي السر القديمة والجديدة.

---

[2] لا يناقش هذا البند كلمات السر الدينامية لأنا تعتبر خارج نطاق هذه التوصية.

REQ 6: لا بد أن يقدم عنصر الشبكة/نظام الإدارة الدعم لمنع استعمال كلمة السر مجدداً. وينبغي أن تكون معلمات منع استعمال كلمة السر قابلة للتعديل وفقاً لسياسة تنظيمية معينة.

REQ 7: من الضروري أن يكون لدى كل معرف الهوية المستعمل كلمة سر قابلة للتحديد يستخدمها في تسجيل الدخول وتخصه تحديداً.

REQ 8: ينبغي أن يكون بوسع المستعمل تغيير كلمة السر حسب تقديره، عقب تطبيق حد أدنى للمهلة الزمنية المنقضية منذ إجراء آخر تغيير. ولا بد أن يكون هذا الحد الأدنى قابلاً للتعديل وفقاً للسياسة التنظيمية المتبعة وأن تحدده **الجهة القائمة على إدارة أمن النظام**.

REQ 9: لا بد أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم للتحكم في كلمة السر على مستويات عدة. ويمكن أن تُغلق دورة بعض المستعملين (نتيجة لتقادم كلمة السر أو تعذر الدخول على سبيل المثال) بينما لا يمكن إغلاق دورة غيرهم من المستعملين.

2.1.6 استيفان كلمات السر المحددة بالتغيب

تناقش الدراسات المتعلقة بالأمن الاستخدام الصحيح لكلمات السر المحددة بالتغيب مناقشة مستفيضة. ووفقاً لتسلسل الأحداث الزمنية، فإن كلمات السر المحددة بالتغيب تتراوح بين كلمات مشفرة بشفرة البرمجة داخل البرنامج إلى كلمة محددة بالتغيب ومقترنة بكل عملية طرح للبرمجيات أو تحسين لها. وفيما يلي متطلبات **استيفان** حالات التغيب:

REQ 10: ينبغي أن تنطبق واحدة من الحالات التالية:

- من الضروري أن توجد برمجية التشكيل كلمة سر وحيدة للتمهيد لكل تطبيق يتعلق بطرح أو تحسين[3] جديد للبرمجيات.
- إذا استخدمت كلمة سر محددة بالتغيب، ينبغي أن يتطلب النظام استبدالها بكلمة سر وحيدة قبل أن يبدأ الجهاز بالعمل.
- في حال تسليم جهاز من دون كلمة سر أو كلمة سر ملغية، لا بد من تخصيص كلمة سر وحيدة أثناء عملية التركيب قبل أن يبدأ الجهاز بالعمل.

REQ 11: ينبغي أن تكون عتبة تقادم النظام المحددة لكلمات السر المستعملة في الدخول قابلة للتعديل إذا كانت العناصر الوظيفية متأصلة أيضاً في التطبيق. وبانقضاء مهلة عتبة التقادم هذه، لا بد من إعادة تحديد كلمة السر المستعملة في الدخول إلى التطبيق المتأثر، وذلك وفقاً لحالة التغيب الأصلية المحددة في المتطلب 10 (REQ 10). وينبغي إلغاء جميع امتيازات تغيير كلمة السر التي يتمتع با المستعملون فيما عدا دور المستعمل الذي يتسم بأعلى مستوي من السلطة الأمنية لنظام أو لحالة تطبيق.

REQ 12: من الضروري أن تكون قيمة مؤقت خمول النظام قابلة للتعديل إذا كان العنصر الوظيفي متأصلاً أيضاً في التطبيق. وعند تمكين مؤقت خمول النظام، ينبغي منع الدخول إلى النظام بواسطة معرف هوية مستعمل معين ولا بد من تعطيل عملية دخول هذا المستعمل.

REQ 13: ينبغي أن يكون حد تقبل النظام لتتابع حالات الدخول الفاشلة بواسطة معرف هوية مستعمل معين قابلاً للتعديل إذا كان العنصر الوظيفي متأصلاً أيضاً في التطبيق. وعند بلوغ هذا الحد، يتعين الاحتكام إلى مؤقت خمول النظام المحدد في المتطلب 12 (REQ 12).

---

[3] يماثل هذا الأمر الممارسة التي يحمل فيها كل قرص مدمج يتم شراؤه من الأسواق كلمة سر وحيدة تُمكن من الدخول.

2.6 النفاذ والتخويل المرافبان

يجب أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم لمفهوم "الحصول على أقل الامتيازات" (أي ينبغي أن يكون لدى كل شخص دوراً وتصريحاً يطلع بموجبه على المعطيات، أو يدخل تعديلات عليها، أو يشرع في اتخاذ **إجراءات إدارية** فيما يتعلق حصراً بالوظائف التي يسمح هذا الدور بأدائها). ويحدد هذا البند المتطلبات الأساسية اللازمة لتنفيذ مفهوم "الحصول على أقل الامتيازات" من خلال الإدارة الجيدة لأمن النظام.

1.2.6 إدارة الأمن

ينبغي لكل عنصر من عناصر الشبكة/نظام الإدارة ألا يكفل السماح بإدارة موارد أمن النظام سوى للمستعملين المصرح لهم بذلك. وترتبط جميع الإجراءات الإدارية بأدوار المستعملين، وتخصص هذه الأدوار لأفراد معينين. وعلى الرغم من اقتصار المناقشة على القليل من أنماط أدوار المستعملين هذه، إلا أنه يحتمل وجود أنماط أخرى كثيرة لهذه الأدوار المتباينة الدرجات من حيث الامتيازات التي تمنحها، ولا سيما فيما يتعلق بأهم **إجراءات إدارة** الأمن. والهدف من ذلك هو ضمان عدم السماح بإدارة أهم موارد الأمن المهمة سوى للمستعملين المصرح لهم بذلك والحاصلين على الامتيازات المذكورة.

REQ 14: من الضروري أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم لأنماط أدوار المستعملين التي يحددها مستعملون متعددون، وبالإمكان تخصيص **إجراءات إدارة** لكل دور من أدوار المستعملين.

وقد تفضي أدوار المستعملين إلى إيجاد تراتب للأدوار بحيث يُخصص لكل دور منها مهام مختلفة أو أقل كأن تتمتع بسلطة أقل من سلطة دور المستعمل الحاصل على امتيازات أكثر. وثمة مثال على هذا التراتب يكون فيه لدى دور المستعمل القدرة على تنفيذ جميع **إجراءات الإدارة**، مثل 'المستعمل الثانوي' للحاسوب. ويوجد دور آخر للمستعمل لا يدعم سوى النفاذ إلى الملفات المخصصة للقراءة من أجل دعم مراقبة الأجهزة، مثل المشغل.

REQ 15: وينبغي أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم لنمط المستعمل المحدد بالتغيب، الذي يكون لديه حد أدنى أو مقيد من **إجراءات الإدارة**.

REQ 16: يجب أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم **لأهم إجراءات إدارة الأمن** التالية، على ألا يقتصر على ما يلي:

- تحديد وتخصيص امتيازات المستعملين والمجموعات.
- حفظ سجل بجميع طلبات الحصول على معرفات هوية الدخول إلى النظام.
- إضافة معرفات هوية المستعملين وحذفها.
- تعطيل استخدام معرفات هوية مستعملين معينين بوصفها معرفات هوية دخول، والتمكين من استعمال هذه المعرفات؛
- تشكيل كلمات السر المستخدمة في الدخول وإعادة تحديدها؛
- تشكيل مفاتيح تجفير وتغييرها؛
- تحديد عتبة تقادم النظام بالنسبة لكلمات سر تسجيل الدخول؛
- وضع الحد الخاص بالنظام فيما يتعلق بعدد محاولات الدخول الفاشلة لكل معرف هوية تسجيل دخول؛
- إلغاء إغلاق النظام، أو تغيير قيمة مؤقت إغلاقه.
- تحديد قيمة مؤقت خمول النظام.
- تحديد تشكيلة التسجيل والإنذار بشأن أمن النظام.
- مراقبة جميع سجلات أمن النظام.
- إدارة عمليات التسجيل المتعلقة بأمن النظام.
- تحسين برمجيات الأمن.

- إناء أية دورة من دورات المستعمل أو دورات النظام.
- تخويل أشخاص معينين بتراخيص أمن فيما يتعلق بأدوار أخرى.
- تحديد قواعد تعقيد كلمات السر.

REQ 17: ينبغي أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم **لإجراءات إدارة أمن التطبيق** الآتية، والتي لا تقتصر على ما يلي:

- تحديد وتخصيص امتيازات جديدة للمستعملين والمجموعات على مستوى التطبيق.
- حفظ سجل بجميع طلبات الحصول على معرفات هوية الدخول إلى التطبيق.
- إضافة مستعملين وحذفهم على مستوى التطبيق.
- مراقبة جميع سجلات أمن التطبيق.
- تحديد تشكيلة التسجيل والإنذارات بشأن أمن التطبيق.
- إدارة عمليات تسجيل أمن التطبيق.
- إناء دورة مستعمل التطبيق.

2.2.6 استخدام وتشغيل عنصر الشبكة/نظام الإدارة

تنطبق المتطلبات الواردة في هذا البند على النفاذ عن بعد والنفاذ عبر وحدة التحكم على حد سواء إلى عنصر الشبكة/نظام الإدارة. وتمثل هذه المتطلبات الإلزامية خط أساسي يستند إليه عنصر الشبكة/نظام الإدارة الذي يخزن فعلاً معرفات هوية المستعملين وكلمات السر التي يستخدمونا. ويلجأ الكثير من عناصر الشبكة/نظام الإدارة إلى وحدة خدمة مركزية لمراقبة النفاذ من أجل خزن معرفات هوية المستعملين وكلمات السر. وتنطبق المتطلبات الإلزامية المبينة في هذه التوصية إجمالاً على عنصر الشبكة/نظام الإدارة إذا كان هذا العنصر/النظام يحتفظ بمعرفات هوية مستعملين وكلمات سر وكانت هذه المعرفات والكلمات مخزونة في وحدة خدمة مراقبة النفاذ.

REQ 18: لا بد أن يعمل عنصر الشبكة/نظام الإدارة على تزامن الوقت بأسلوب مستيقن (باستخدام الصيغة 3 مثلاً من بروتوكول التحديد الدقيق للوقت الفعلي في شبكة الحواسيب (NTP)).

REQ 19: ينبغي أن يقترن كل **إجراء إداري** في عنصر الشبكة/نظام الإدارة بفترة واحدة يصرح له بـا.

REQ 20: من الضروري تحديد كل فترة من خلال إجراء **استيفان** صحيح على غرار ما هو مبين بالتفصيل في المتطلب 1 (REQ 1).

REQ 21: ينبغي عبر **مسير موثوق** أن تتم الاتصالات بين عنصر الشبكة/نظام الإدارة وإحدى وحدات خدمة مراقبة النفاذ، لأغراض نقل أوراق اعتماد الاستيقان،.

REQ 22: لا بد أن يستخدم عنصر الشبكة/نظام الإدارة التحكم في النفاذ والفواصل من أجل السماح بدخول مستعمل ما، أو مجموعة مستعملين، أو حالة دخول عن بعد عبر النظام إلى عنصر الشبكة/نظام الإدارة، أو رفض هذا الدخول، أو التحكم فيه بذا الشكل أو ذاك، وينبغي أن يوفر هذا العنصر/النظام وظائفية تفرض قيوداً على المستعملين بشأن الاطلاع على المعطيات، وإجراء المعاملات، واستخدام المعدات اللازمة لتأدية أدوارهم. ويجب أن تشمل رخص الدخول الملفات المخصصة للقراءة حصراً والملفات المخصصة للقراءة والكتابة، ولكن من دون أن تقتصر على ذلك.

3.2.6 عملية الدخول

REQ 23: من الضروري أن يقدم عنصر الشبكة/نظام الإدارة الدعم للقدرة على تخصيص معرف هوية وحيد لكل فرد من المستعملين للدخول إلى تطبيق ما أو إلى نظام حاسوب مضيف.

REQ 24: ينبغي أن يكون لدى عنصر الشبكة/نظام الإدارة، حيثما اقتضت الضرورة، القدرة على إلزام المستعمل تلقائياً بتغيير كلمة السر المستخدمة في أول دخول بعد التثبت من حساب المستعمل وفي أول دخول له بعد إعادة تحديد كلمة السر.

ملاحظة - يستوجب المتطلب التالي (REQ 25) إجراء تمييز فيما يتعلق بإدارة عنصر الشبكة مقابل نظام الإدارة. وتتطلب إدارة عناصر الشبكة مراقبة جهاز معين باستخدام العديد من الآليات، ولربما تم ذلك آنياً، مع العمل في نفس الوقت على إدخال تعديلات على التشكيلة. أما في حالة نظام الإدارة، فإن ذلك ليس ضرورياً.

والمراد بذا المتطلب هو إدارة مقدرة المستعملين على استهلاك جميع الموارد المتيسرة لعنصر الشبكة/نظام الإدارة. وينبغي أن يقوم موظفو التشغيل بتعديل قيمة تغيب عنصر الشبكة المحددة بالتغيب حسب الحاجة في الحالات الفردية، ومن الضروري أن يراقبوا ويتحققوا من المحاولات الرامية إلى تجاوز هذه الحدود، بالنظر إلى أنا قد تدل على وجود خلل في التشغيل أو محاولة للقيام بأنشطة تخريبية.

REQ 25: لا بد أن يحول عنصر الشبكة/نظام الإدارة دون استخدام نفس معرف هوية المستعمل للدخول في آن معاً إلى دورة فعالة، أو يتحكم في هذا الاستخدام، أو يضع حداً له، وذلك حسب الاقتضاء. ومن الضروري أن يكون عدد الدورات الفعالة المتزامنة قابلاً للتعديل على أساس معرف هوية المستعمل.

REQ 26: ينبغي أن ينوه تطبيق عنصر الشبكة/نظام الإدارة بضرورة تمتع **المستعمل الثانوي** لكي يعمل بصورة صحيحة.

REQ 27: يجب أن يكون لدى عنصر الشبكة/نظام الإدارة القدرة على عرض وقت وتاريخ آخر **استيفان** تم بنجاح لهوية المستعمل على هذا المستعمل أثناء عملية الدخول، وحسب الاقتضاء.

REQ 28: ينبغي عرض بيان بمعلومات خاصة قابلة للمواءمة مع احتياجات الزبون، وينبغي ألا يعرض تحذير من التعدي على شاشة الدخول الأولي قبل السماح بأي نفاذ منطقي. وينبغي أن تدعم المعدات طولاً بحد أدنى قدره 1600 رمز. ومن الضروري تقديم رسالة بالتغيب.

وفيما يلي مثال على نص تحذيري.

> تحذير! نظام الحاسوب والشبكة هذان خاصان ومملوكان لجهة خاصة ولا يمكن السماح بالدخول إليهما إلا للمستعملين المصرح لهم بذلك. والاستخدام غير المصرح به لهذا النظام أو هذه الشبكة ممنوع منعاً باتاً ويمكن أن يعرِّض فاعله للملاحقة الجنائية، أو اتخاذ إجراءات تأديبية بحق الموظف المسؤول قد تصل إلى الفصل من الخدمة، أو فسخ عقود الجهة البائعة/الخدمة. ويجوز للجهة المالكة أو وكلائها مراقبة أي نشاط أو اتصال يُجرى عبر نظام الحاسوب أو الشبكة. ويجوز لها أو لوكلائها استعادة أية معلومات مخزونة داخل هذا النظام أو هذه الشبكة. ودخولكم إلى هذا النظام أو هذه الشبكة واستخدامكم لأي منهما يعني موافقتكم على المراقبة واستعادة المعلومات من أجل إنفاذ القانون وتحقيق أغراض أخرى. ولا ينبغي أن يتوقع المستعملون التمتع بالخصوصية فيما يتعلق بأي اتصال يُجرى عبر هذا النظام أو هذه الشبكة أو أية معلومات مخزونة داخل أي منهما، بما في ذلك المعلومات المخزونة محلياً أو عن بعد على الأقراص الصلبة أو غيرها من الوسائط المستخدمة بمعية هذا النظام أو هذه الشبكة.

ويُوصى بأن يصدر كل كيان نصاً تحذيرياً مناسباً.

REQ 29: ينبغي عدم إبلاغ المستعمل بأي محاولة دخول فاشلة إلا عندما تفشل عملية الدخول أو تكون غير صحيحة. وينبغي عدم الإبلاغ عن معلومات من قبيل " معرف غير صحيح لهوية المستعمل" أو "كلمة سر غير صحيحة".

REQ 30: لا بد أن يقوم عنصر الشبكة/نظام الإدارة **بإغلاق** حساب المستعمل ومنعه من الدخول بعد بلوغ عدد محاولات الدخول الفاشلة عتبة معينة قابلة للتعديل. ويجب أن يشمل **الإغلاق** السطح البيني لوحدة التحكم، ولا ينبغي أن يشمل **الإغلاق** الحساب الأصلي المحدد بالتغيب والذي يدعم جميع إجراءات الإدارة.

REQ 31: ينبغي ألا يكون لدى عنصر الشبكة/نظام الإدارة آلية للتغاضي عن **استيفان** تسجيل الدخول وعمليات تسجيل الدخول.

REQ 32: ينبغي ألا يعرض أي عنصر من عناصر الشبكة/نظام الإدارة على وجه الإطلاق الشرط التأهيلي لنص واضح، مثل كلمة السر، في أي واسطة من الوسائط، بما في ذلك عرضه على الشاشات المطرافية، والنسخ المطبوعة، أو خزنه في قيود السجلات.

REQ 33: من الضروري أن يدعم عنصر الشبكة/نظام الإدارة تقادم كلمة السر عن طريق تحديد عتبة قابلة للتعديل.

وتنفيذ المتطلب 33 (REQ 33) تنفيذاً مشتركاً ومقبولاً هو أمر متروك للنظام لكي يتطلب فوراً من المستعمل أن يحدد كلمة سر جديدة بعد استيقان المستعمل بواسطة كلمة السر القديمة. وبدلاً من ذلك، يمكن أن يتطلب النظام أحد القائمين على الإدارة ليغير كلمة السر على نحو سليم. وفي حال عدم استعمال حساب ما لفترة من الزمن، يعتبر هذا الحساب ساكناً.

REQ 34: إذا تجاوت كلمة سر لتسجيل الدخول حد التقادم المعين لذلك النظام، ينبغي أن **يغلق** عنصر الشبكة/نظام الإدارة باب الدخول أمام معرف هوية هذا المستعمل لحين تغيير كلمة السر كما يجب.

REQ 35: إذا استمر سكون حساب ما لفترة زمنية تتجاوز فترة العتبة القابلة للتعديل، ينبغي أن يوجه كل عنصر من عناصر الشبكة/نظام الإدارة إنذاراً.

REQ 36: إذا استمر سكون حساب ما للفترة الزمنية القابلة للتعديل، يجب أن يقوم عنصر الشبكة/نظام الإدارة بتعطيل هذا الحساب بعد توجيه إنذار. وينبغي ألا تتضمن عملية التعطيل حساب كل من **الجهة القائمة على إدارة النظام**، **والجهة القائمة على إدارة أمن النظام**، **والمستعمل الثانوي**.

REQ 37: من أجل التمكين مجدداً من استخدام معرف هوية مستعمل **معطّل**، تلزم جهة تضطلع بإدارة الدخول بصورة صحيحة، وتسند إليها أهم إجراءات إدارة الأمن التي تتيح تشكيل وإعادة تحديد كلمات السر المستخدمة في تسجيل الدخول.

ويمكن تشكيل الخيارات المتاحة لإعادة تمكن معرفات هوية المستعمل بوصفها معلمة تشمل النظام ككل على مستوى الدور المؤدى.

REQ 38: من أجل إعادة تحديد معرف هوية مستعمل مغلـق يستخدم في الدخول وإلغاء حالة **الإغلاق**، فمن الضروري وجود جهة قائمة على إدارة الدخول بصورة صحيحة، تكون مكلفة باتخاذ إجراء حاسم لإدارة الأمن فيما يتعلق بإلغاء الإغلاق أو تغيير قيمة مؤقت إغلاق النظام.

ويمكن تشكيل الخيارات المتعلقة بإلغاء **إغلاق** معرفات هوية المستعمل على هيئة معلمة تشمل النظام ككل على مستوى الأدوار المؤداة.

4.2.6 عملية الإناء

REQ 39: ينبغي أن يقوم المستعمل أو النظام بإناء كل دورة يتم الدخول إليها بشكل صحيح بعد فترة معينة من خمول النظام.

REQ 40: ينبغي أن ينهي عنصر الشبكة/نظام الإدارة أي **دورة** يتم توصيلها بشكل سليم عندما يتجاوز آخر نشاط لها، قيمة مؤقت خمول النظام القابلة للتعديل.

5.2.6 التطبيقات

REQ 41: يجب أن يبقى نمط دور المستعمل دون تغيير أثناء تنفيذ أي تطبيق لعنصر الشبكة/نظام الإدارة وحتى إتمام إناء هذا التطبيق.

وينبغي ألا يكون بوسع المستعمل استخدام آلية للتحكم في التتابع، مثل الانفلات من طبقة البرنامج الخارجية إلى أسلوب **المستعمل الثانوي**. وفي حال فشل التطبيق، يجب ألا يترك المستعمل في دور مختلف يتمتع بالمزيد من الامتيازات. ولا بد أن يتم استيقان المستعمل مجدداً (توصيله مجدداً) من أجل تكليفه بدور مختلف.

3.6 حماية السرية

يحدد هذا البند المتطلبات اللازمة لخوارزميات تحمل رموز سرية ولإدارة المفاتيح بغية المساعدة على ضمان أمن النظام والشبكة. وعادة ما تستخدم خوارزميات متناظرة في تقديم خدمات السرية والسلامة على حد سواء. وبطبيعة الحال، ينبغي تبادل مفاتيح الخوارزميات المتناظرة في عملية ترتبط ارتباطاً وثيقاً بالاستيقان. كما يمكن استخدام خوارزميات غير متناظرة في تقديم خدمات الاستيقان وتبادل المفاتيح. وتكتسي الطرائق المستخدمة في توليد هذه المفاتيح وخزنا وتوزيعها وإتلافها وإلغائها أهمية قصوى. وبالإضافة إلى ذلك، ترتبط عوامل من قبيل طول المفتاح، واختياره، وانتفاء الخوارزمية بصلة مباشرة بمدى قوة الأمن التي يتمتع با نظام سري معين.

وتستند حماية **الاستيقان** وسرية المعطيات إلى أساس يحمل رموزاً سرية. ويستخدم الترميز السري خوارزميات خاصة تستند إلى معايير معينة ومتيسرة عموماً، مما يفسح المال بالتالي أمام دقة التنفيذ وسهولته على نطاق واسع. وتستند "قوة" الترميز السري إلى ما يستخدم من خوارزميات مرمزة سراً، فضلاً عن حجم المفتاح المستخدم (أي، يشير تعبير قوة إلى الفترة الزمنية التي يحتاجها المهندس المسؤول عن عملية القلب (يعني إيجاد أو تخمين) قيمة (قيم) المفتاح المستخدم بمعية خوارزمية معينة).

وفي العادة، تؤمن بروتوكولات الأمن (مثل أمن بروتوكول الإنترنت (IP sec) وطبقة مقابس الأمن (SSL)، وبرنامج شل للدخول الآمن (SSH)) **الاستيقان**، والتكاملية، والسرية. وحالات توسيع نطاق الأمن ليضم بروتوكولات أخرى من قبيل الصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3)[4]، والمعمارية الشائعة لبرمجيات نقل الطلبات إلى الهدف (CORBA)، وبروتوكول بوابة الحدود، وأقصر مسير يفتح أولاً، هي حالات يراد با تأمين **الاستيقان** والتكاملية. وحماية **الاستيقان** والسلامة ضرورية بين عنصر الشبكة/نظام الإدارة، كما أن من الضروري تأمين السرية حيثما تقتضي الحاجة.

1.3.6 خوارزميات التجفير المتناظر

يشير تعبير التجفير المتناظر أو التجفير بمفاتيح سرية إلى نظام يحمل رموزاً سرية تكون فيه مفاتيح التجفير ومفاتيح إزالته متماثلة. وتستوجب الأنظمة المتناظرة التي تحمل رموزاً سرية إجراء ترتيبات أولية بخصوص تشارك الأفراد في مفتاح سري وحيد (مثل مفتاح التجفير). ويجب توزيع المفتاح على الأفراد باستخدام وسيلة سرية، أو بوسيلة تُستنبط من الداخل (كأن تكون مستندة مثلاً إلى التشارك في مفتاح جذر سري) لأن معرفة مفتاح التجفير تدل ضمناً على معرفة مفتاح إزالته والعكس بالعكس.

REQ 42: ينبغي أن يكون مستوي قوة الخوارزميات المستخدمة في جميع تطبيقات التجفير المتناظر متفقاً والسياسة الوطنية، أو الصناعية، أو التنظيمية المتبعة.

2.3.6 خوارزميات التجفير غير المتناظر

نظام التجفير غير المتناظر هو نظام يرتبط فيه مفتاح التجفير بمفتاح إزالته ولكنهما يختلفان عن بعضهما. ويكون أحد هذين المفتاحين عاماً، بينما يبقى الآخر سرياً. ويختلف المفتاح العام عن المفتاح الخاص، وليس هناك طريقة عملية معروفة لاستنباط المفتاح الخاص من العام. وتُوزع المفاتيح العامة على نطاق واسع؛ غير أن المفتاح الخاص يبقى سرياً دوماً. وعادة ما يقتصر استخدام التجفير غير المتناظر على تجفير مفاتيح متناظرة من أجل تبادل المفاتيح وتسجيل سلاسل الرسائل المحررة في نصوص من أجل الحصول على إشارات رقمية. ويستخدم المفتاح العام للمتلقي في تبادل المفاتيح، بينما يستعمل المفتاح الخاص للمسجل في تسجيل سلاسل الرسائل المحررة في نصوص.

REQ 43: لا بد أن يكون مستوى قوة الخوارزميات المستخدمة في جميع تطبيقات التجفير غير المتناظر متفقاً مع السياسة الوطنية، أو الصناعية، أو التنظيمية المتبعة.

REQ 44: يجب أن يكون مستوى قوة الخوارزميات المستخدمة في جميع تطبيقات تبادل المفاتيح متفقاً والسياسة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا الصدد.

---

[4] قد تؤمن أيضاً هذه الصيغة (SNMPv3) السرية.

3.3.6 إدارة المفاتيح التي تحمل رموزاً سرية

إدارة مواد المفاتيح التي تحمل رموزاً سرية إدارة صحيحة أمر صعب وغالباً ما يكون معقداً لأن إدارتا تنطوي على انقضاء مدتا، وتبادلها بشكل آمن، ونشرها بأمن، إضافة إلى توليد المفاتيح. وتقدم الوثيقة IETF RFC 1750، *التوصيات المتعلقة بالعشوائية في مجال الأمن*، إرشادات إضافية في هذا الخصوص.

4.3.6 الاتصالات

الاتصالات المؤمنة أساس تأمين **مستوي الإدارة** في أي شبكة حديثة. ويناقش الملحق A معماريات وبروتوكولات تنفيذ **اتصالات إدارية مؤمّنة**. وتنطبق المتطلبات الإلزامية المحددة في هذا البند على جميع السطوح البينية لأي شبكة من شبكات إدارة الاتصالات (TMN) على غرار الوصف الوارد في التوصية ITU-T M.3010، المبادئ المتعلقة بشبكة إدارة الاتصالات.

REQ 45: من الضروري أن يكون عنصر الشبكة/نظام الإدارة في أي سطح بيني مادي أو منطقي يحمل حركة إدارة معينة داخل عنصر شبكة/نظام إدارة ما، قابلاً للتعديل بغية تأمين حركة الإدارة بالتلازم مع **الاستيفان الشديد** وحماية سرية الرموز المستعملة من أجل توفير الحماية للسرية والسلامة والتكرار.

REQ 46: ينبغي عدم إرسال أي كلمة سر منقولة بنص واضح غير مشفر إلا عبر **مسير موثوق** ما لم تستخدم في ذلك آلية لإرسال كلمات السر التي تستعمل لمرة واحدة. وفي حال استخدام كلمات سر من هذا القبيل، يمكن حينئذ إرسالها بنص واضح غير مشفر طالما لا يوجد مضيف وسيط.

4.6 حماية سلامة المعطيات

1.4.6 خوارزميات سلامة المعطيات

بالإمكان استخدام خوارزميات تحمل مفاتيح لسلسلة الرسائل المحررة في نصوص بالاقتران مع وظائف التظليل من أجل ضمان تكاملية المعطيات المنقولة برسائل ذات أطوال عشوائية.

REQ 47: ينبغي أن يكون مستوي قوة الخوارزميات المستخدمة في جميع التطبيقات المتناظرة لتأمين تكاملية المعطيات متفقاً والسياسة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا المال.

REQ 48: لا بد أن يكون مستوي قوة الخوارزميات المستخدمة في جميع التطبيقات غير المتناظرة لتأمين تكاملية المعطيات متفقاً مع السياسة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا الخصوص.

2.4.6 تطوير وتسليم عنصر الشبكة (NE)/نظام الإدارة (MS)

يعتمد أمن عنصر الشبكة/ نظام الإدارة على كامل عملية دورة الحياة. والأمن مسألة مطروحة أثناء التصميم المفاهيمي ويبقى كذلك خلال التصميم التفعيلي، والتطوير والنشر والإخراج من الخدمة لناتج ما. والتحكمات والاختبارات المناسبة أثناء كامل عملية دورة الحياة بالغة الأهمية من أجل توفير مستويات أمن مقبولة. ويناقش البندان 2.5.I و3.5.I اعتبارات إضافية بشأن دورة الحياة.

REQ 49: يجب أن تشمل جميع البرمجيات التي يتسلمها أحد مقدمي الخدمات أو غيره من الزبائن، حسب الاقتضاء، **استيفاناً** تجفيرياً وآليات لحماية السلامة مثل **الاستيقان** من الإشارات الرقمية أو **استيقان** الرسائل المتناظرة مثلما هو محدد في التوصية ITU-T M.3016.3.

REQ 50: يجب أن تكون لجميع عناصر الشبكة/أنظمة الإدارة المتلقية لبرمجيات معينة قدرة على تفسير **استيقان** التجفير وآليات حماية التكاملية والتحقق من مصدر البرمجيات وتكامليتها حسب الاقتضاء.

REQ 51: ينبغي إرسال جميع تحسينات البرمجيات، بما فيها برامج التصحيح، إلى عنصر الشبكة/نظام الإدارة المتلقي لهذه البرامج عبر مسير موثوق.

ومن الضروري أن يكون بمقدور عنصر الشبكة/نظام الإدارة أن يحدد إلكترونياً المستويات الحالية للمراجعة التي يجريها للبرمجيات والعتاديات وأن يتحقق من التشكيلات الملائمة للبرمجيات/البرمجيات الثابتة.

5.6 المساءلة

يتمثل هدف المساءلة في ضمان إلزام أي كيان بالمسؤولية عن أية إجراءات يشرع في اتخاذها.

REQ 52: يجب أن توفر جميع عناصر الشبكة (NE)/أنظمة الإدارة (MS) القدرة المتمثلة في عدم تمكن أي كيان من رفض مسؤولية أية إجراءات ينفذها فضلاً عن الآثار المترتبة على هذه الإجراءات.

انظر أيضاً المتطلب 49 والمتطلب 50 (REQ 49 & REQ 50) بشأن متطلبات المساءلة المتعلقة بتطوير وتسليم عنصر الشبكة/نظام الإدارة.

6.6 تسجيل الأمن وتدقيقه

من المهم أن يوفر كل عنصر من عناصر الشبكة/نظام الإدارة المقدرة الكافية التي تفسح المال أمام الاضطلاع بأنشطة التحقق، والتدقيق، والكشف في الوقت الفعلي، والتحليل، والحماية، كيما يتسنى اتخاذ الإجراءات التصحيحية المناسبة. ويدرس هذا البند سجلات تدقيق الأمن؛ غير أن التفاصيل الدقيقة لمضمون ونسق سجلات تدقيق الأمن لا تندرج ضمن نطاق هذه التوصية.

وتجدر الإشارة إلى أن أنشطة التحقق والتحليل البياني قد تشمل التحقق من رسائل التشغيل والإدارة والصيانة والتزويد (OAM&P) التي ليس لها صلة بالأمن إلى جانب المعلومات المخزونة في سجلات تدقيق الأمن التي يرد وصف لها في هذا البند. وتسجيل هذه الرسائل (OAM&P) غير المتصلة بالأمن، التي يُشار إليها أحياناً بوصفها رسائل تعبر عن "آخر ما استجد من تغييرات"، هو أمر ضروري بالنسبة إلى أية إجراءات قابلة للتدقيق.

REQ 53: لا بد أن يكون بمقدور عنصر الشبكة/نظام الإدارة تسجيل أي إجراء يغير نعوت الأمن وخدماته، ومراقبة النفاذ، ومعلمات تشكيل الأجهزة.

REQ 54: ينبغي أن يوفر عنصر الشبكة/نظام الإدارة المقدرة على تشكيل أهم **إجراءات إدارة** الأمن التي يتعين إدراجها في **سجل الأمن**.

REQ 55: من الضروري أن يكون بوسع عنصر الشبكة/نظام الإدارة تسجيل كل محاولة دخول ونتيجتها؛ وكل محاولة خروج أو إنهاء للفترة (سواء تمت عن بعد أم عبر وحدة التحكم) وكل محاولة دخول ونتيجتها تؤدي إلى تنفيذ مؤقت خمول النظام المحدد في المتطلب 12 (REQ 12).

ويُوصى بإرسال قيود سجل التدقيق إلى وحدة خدمة حاسوب غير قابلة للتغيير لتدقيقها بعد وسمها بحسب التتابع واستيقانها (توقيعها) تجفيرياً من جانب عنصر الشبكة/نظام الإدارة.

REQ 56: يجب أن يكون بمستطاع عنصر الشبكة/نظام الإدارة التسجيل عن بعد عبر **مسير موثوق**.

REQ 57: ينبغي أن يضم كل قيد من قيود السجل المعلومات التالية:

- وصف للإجراء أو الإجراء الفعلي المسجل؛
- هوية ومستوى أمن المستعمل أو العملية التي استهلت الإجراء؛
- تاريخ ووقت حصول الإجراء؛
- معلومات عن مصدر الشبكة ومقصدها، في حال انطباق ذلك (عند الدخول مثلاً)؛
- إشارة إلى نجاح النشاط أو فشله.

7.6 الإخبار عن إنذارات الأمن

من الضروري الإبلاغ عن حالات معينة بوصفها إنذارات تتعلق بالأمن، انظر المتطلب 35 (REQ 35) على سبيل المثال. ومع ذلك، فإن تحديد هذه الحالات لا يندرج ضمن نطاق هذه التوصية.

REQ 58: يجب أن توفر جميع عناصر الشبكة/نظام الإدارة المقدرة اللازمة لتوجيه تبليغات عن الإنذارات بشأن أحداث مختارة.

REQ 59: يجب أن توفر جميع عناصر الشبكة/نظام الإدارة المقدرة اللازمة لإفساح المال أمام المستعمل ليحدد معايير اختيار الأحداث التي تُوجه بشأنها تبليغات عن الإنذارات.

8.6 حماية **شبكة التحكم** في **المعطيات** (DCN)

من أجل حماية البنية الأساسية للإدارة، وحماية شبكة التحكم في المعطيات عموماً، من المفيد أن يقوم مشغل الشبكة بتفحص الحركة من أو إلى الشبكات الخارجية من شبكة التحكم في المعطيات (مثل الحركة المتأتية من شبكات أو زبائن متماثلة). واتخاذ الإجراءات اللازمة. وعلى سبيل المثال، ينبغي عدم السماح للرزم التي تحمل عناوين بروتوكول إنترنت المصدر المطابقة لحيز عناوين شبكة التحكم في المعطيات بالدخول إلى هذه الشبكة من شبكات خارجية.

REQ 60: يجب أن تحول جميع عناصر الشبكة/نظام الإدارة التي لديها توصيلية قائمة على الرزم دون الحركة التي لا تلبي سياسة الأمن التي تتبعها شبكة التحكم في المعطيات.

الملحق A

تقابل متطلبات وخدمات وآليات الأمن

يوفر هذا الملحق التقابل المستمد من متطلبات الأمن إلى خدمات الأمن المحددة في التوصية ITU-T M.3016.2 وآليات الأمن المحددة في التوصية ITU-T M.3016.3.

	متطلبات الأمن المحددة في التوصية M.3016.1	**خدمات الأمن المحددة في التوصية M.3016.2**	**آليات الأمن المحددة في التوصية M.3016.3**
REQ 1:	فيما يتعلق بتسجيل الدخول إلى عنصر الشبكة/نظام الإدارة، ينبغي دعم التسجيل والتدقيق والاستيقان الشديد.	**SER 1, SER 2, SER 3, SER 8**	**MEC 1-MEC 13**
REQ 2:	ينبغي أن يعمل كل عنصر من عناصر الشبكة/نظام الإدارة على تنفيذ **الاستيقان** وفقاً للسياسة العامة التنظيمية.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 3:	ينبغي أن يدعم كل عنصر من عناصر الشبكة/نظام الإدارة الحد الأدنى من قواعد التعقيد اللازمة **للاستيقان** وفقاً للسياسة العامة التنظيمية.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 4:	ينبغي أن تمنع عناصر الشبكة/نظام الإدارة مستعملاً آخر من تغيير كلمة سر يستخدمها غيره في الدخول من دون علم المستعمل الأول.	**SER 8**	**MEC 7-MEC 11**
REQ 5:	ينبغي لعنصر الشبكة/نظام الإدارة أن يكفل تلقائياً اختلاف كل كلمة سر جديدة للدخول عن سابقتها. ولا بد أن تكون درجة الاختلاف قابلة للتعديل وفقاً للسياسة العامة التنظيمية.	**SER 1**	**MEC 7-MEC 11**
REQ 6:	لا بد أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم لمنع استعمال كلمة السر مجدداً. وينبغي أن تكون معلمات منع استعمال كلمة السر قابلة للتعديل وفقاً للسياسة العامة التنظيمية.	**SER 1**	**MEC 7-MEC 11**

متطلبات الأمن المحددة في التوصية M.3016.1		خدمات الأمن المحددة في التوصية M.3016.2	آليات الأمن المحددة في التوصية M.3016.3
REQ 7:	من الضروري أن يكون لدى كل معرف من معرفات هوية المستعمل كلمة سر قابلة للتحديد يستخدمها في الدخول وتخصه تحديداً.	**SER 1**	**MEC 7-MEC 11**
REQ 8:	ينبغي أن يكون بوسع المستعمل تغيير كلمات السر حسب تقديره، عقب تطبيق حد أدنى للمهلة الزمنية المنقضية منذ إجراء آخر تغيير. ولا بد أن يكون هذا الحد الأدنى قابلاً للتعديل وفقاً للسياسة العامة التنظيمية وأن تحدده **الجهة القائمة على إدارة أمن النظام**.	**SER 1**	**MEC 7-MEC 11**
REQ 9:	ينبغي أن يدعم كل عنصر من عناصر الشبكة/نظام الإدارة مراقبة كلمات السر على مستويات عدة. ويمكن أن تُغلق دورة بعض المستعملين (نتيجة لتقادم كلمة السر أو فشل الدخول على سبيل المثال) بينما لا يمكن إغلاق دورة غيرهم من المستعملين.	**SER 1, SER 2, SER 3, SER 4**	**MEC 20-MEC 23**
REQ 10:	ينبغي أن تنطبق واحدة من الحالات التالية: • ينبغي أن توجد برمجيات التشكيل كلمة سر واحدة لكل تطبيق يتعلق بتحرير أو تحسين جديد للبرمجيات. • إذا استخدمت كلمة سر محددة بالتغيب، فينبغي أن يطلب النظام استبدالها بكلمة سر وحيدة قبل أن يبدأ الجهاز بالعمل. • في حال تسليم جهاز من دون كلمة سر أو كلمة سر ملغية، لا بد من تخصيص كلمة سر وحيدة أثناء عملية التركيب قبل أن يبدأ الجهاز بالعمل.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 11:	ينبغي أن تكون عتبة تقادم كلمات سر تسجيل دخول النظام قابلة للتعديل إذا كانت العناصر الوظيفية مدمجة أيضاً في التطبيق. وبانقضاء مهلة عتبة التقادم هذه، لا بد من إعادة تحديد كلمة السر المستعملة في الدخول إلى التطبيق المتأثر إلى حالة التغيب الأصلية المحددة في المتطلب 10 (REQ 10). وينبغي إلغاء جميع امتيازات تغيير كلمة السر بالنسبة لجميع المستعملين فيما عدا دور المستعمل الذي يتسم بأعلى مستوى من السلطة الأمنية في حالة أي نظام أو تطبيق معين.	**SER 4**	**MEC 7-MEC 11**
REQ 12:	ينبغي أن تكون قيمة مؤقت خمول النظام قابلة للتعديل إذا كانت العناصر الوظيفية مدمجة أيضاً في التطبيق. وعند تمكين مؤقت خمول النظام، ينبغي منع نفاذ معرف هوية مستعمل معين إلى النظام وينبغي تعطيل عملية دخول هذا المستعمل.	**SER 4**	**MEC 7-MEC 11**
REQ 13:	ينبغي أن يكون حد تقبل النظام لتتابع حالات تسجيل الدخول الفاشلة بواسطة معرف هوية مستعمل معين قابلاً للتعديل إذا كانت العناصر الوظيفية مدمجة أيضاً في التطبيق. وعند بلوغ هذا الحد، يتعين تنفيذ مؤقت خمول النظام المحدد في المتطلب 12 (REQ 12).	**SER 4**	**MEC 7-MEC 11**
REQ 14:	ينبغي أن يدعم كل عنصر من عناصر الشبكة/نظام الإدارة أنماط متعددة لأدوار المستعملين وتخصيص **إجراءات إدارية** لكل دور من هذه الأدوار.	**SER 4**	**MEC 20-MEC 23**
REQ 15:	ينبغي أن يدعم كل عنصر من عناصر الشبكة/نظام الإدارة نمط مستعمل محدد بالتغيب، ومجموعة دنيا أو تقييدية **لإجراءات الإدارة**.	**SER 4**	**MEC 20-MEC 23**

متطلبات الأمن المحددة في التوصية M.3016.1	خدمات الأمن المحددة في التوصية M.3016.2	آليات الأمن المحددة في التوصية M.3016.3
REQ 16: يجب أن يقدم كل عنصر من عناصر الشبكة/نظام الإدارة الدعم **لأهم إجراءات أدارة الأمن** التالية، وغير الشاملة: • تحديد وتخصيص امتيازات المستعملين والـموعات. • حفظ سجل بجميع طلبات الحصول على معرفات هوية الدخول إلى النظام. • إضافة معرفات هوية المستعملين وحذفها. • تعطيل استخدام معرفات هوية مستعملين معينين بوصفها معرفات هوية دخول، والتمكين من استخدام هذه المعرفات؛ • تشكيل كلمات السر المستخدمة في الدخول وإعادة تحديدها؛ • تشكيل مفاتيح تجفير وتغييرها؛ • تحديد عتبة تقادم كلمات السر الدخول إلى النظام؛ • تعيين عدد محاولات الدخول الفاشلة لكل معرف هوية للدخول إلى النظام؛ • إلغاء إغلاق النظام، أو تعديل قيمة مؤقت إغلاقه. • ضبط قيمة مؤقت خمول النظام. • تحديد تشكيلة تسجيل أمن النظام والإنذار المتعلق بأمنه. • مراقبة جميع سجلات أمن النظام. • إدارة عمليات تسجيل متعلقة بأمن النظام. • تحسين برمجيات الأمن. • إناء أية مستعمل أو نظام. • منح تصاريح أمنية لأشخاص محددين يضطلعون بأدوار أخرى. • وضع قواعد معقدة لتشكيل كلمات السر.	SER 4, SER 8	MEC 20-MEC 23
REQ 17: ينبغي أن يدعم كل عنصر من عناصر الشبكة/نظام الإدارة **إجراءات إدارة** أمن التطبيق التالية، غير الشاملة: • تحديد وتخصيص امتيازات جديدة للمستعملين والـموعات على مستوي التطبيق. • حفظ سجل بجميع طلبات الحصول على معرفات هوية تستعمل للدخول إلى التطبيق. • إضافة مستعملين وحذفهم على مستوي التطبيق. • مراقبة جميع سجلات أمن التطبيق. • تشكيلة تسجيل الأمن والإنذارات المتعلقة بأمن التطبيق. • إدارة عمليات تسجيل أمن التطبيق. • إناء دورة مستعمل للتطبيق.	SER 4, SER 8	MEC 20-MEC 23
REQ 18: يجب أن يحقق عنصر الشبكة/نظام الإدارة تزامن الوقت بطريقة مستيقنة (باستخدام الصيغة 3 مثلاً من بروتوكول التحديد الدقيق للوقت الفعلي في الشبكة (NTP)).	SER 8	**غير قابل للانطباق**
REQ 19: ينبغي أن يقترن كل **إجراء إداري** بالنسبة لعنصر الشبكة/نظام الإدارة بدورة واحدة يُصرح بـا.	SER 4	MEC 20-MEC 23
REQ 20: ينبغي تحديد كل دورة من خلال إجراء **استيفان** صحيح على غرار ما هو مبين بالتفصيل في المتطلب 1 (REQ 1).	SER 1, SER 2, SER 3	MEC 1-MEC 12
REQ 21: ينبغي أن تتم الاتصالات بين عنصر الشبكة/نظام الإدارة وإحدى وحدات خدمة مراقبة النفاذ (ACS)، لأغراض نقل الشروط التأهيلية الخاصة **بالاستيفان** عبر **مسير موثوق**.	SER 5, SER 6	MEC 19

متطلبات الأمن المحددة في **التوصية** M.3016.1	خدمات الأمن المحددة في **التوصية** M.3016.2	آليات الأمن المحددة في **التوصية** M.3016.3
REQ 22: ينبغي أن يستخدم عنصر الشبكة/نظام الإدارة **مراقبة النفاذ** والفواصل من أجل السماح بنفاذ مستعمل ما، أو مجموعة مستعملين، أو نفاذ إلى النظام عن بعد إلى عنصر الشبكة/نظام الإدارة، أو رفض هذا النفاذ، أو مراقبته بذا الشكل أو ذاك، وينبغي أن يوفر هذا العنصر/النظام عناصر وظيفية تحصر على المستعملين في نطاق المعطيات، والمعاملات، والمعدات اللازمة لتأدية أدوارهم. ويجب أن تشمل الأذون بالنفاذ الملفات المخصصة للقراءة حصراً والملفات المخصصة للقراءة والكتابة، لكن دون أن تقتصر على ذلك.	**SER 4**	**MEC 20-MEC 23**
REQ 23: يجب أن يدعم عنصر الشبكة/نظام الإدارة الدعم القدرة على تخصيص معرف هوية وحيد لكل فرد من المستعملين للدخول إلى تطبيق ما أو نظام حاسوب مضيف.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 24: ينبغي أن يكون لدى عنصر الشبكة/نظام الإدارة، حيثما اقتضت الضرورة، القدرة على إلزام المستعمل تلقائياً بتغيير كلمة السر المستخدمة في أول نفاذ له بعد فتح حساب المستعمل وفي أول نفاذ له بعد إعادة تحديد كلمة السر.	**SER 4**	**MEC 7-MEC 11**
REQ 25: ينبغي أن يمنع عنصر الشبكة/نظام الإدارة، حسب الاقتضاء، الاستعمال النشط المتزامن لنفس معرف هوية المستعمل وأن يتحكم فيه أو يحد منه. وينبغي أن يكون عدد مدد الاستعمال النشط المتزامن قابلاً للتعديل على أساس معرف هوية المستعمل.	**SER 1, SER 2, SER 3, SER 4**	**MEC 7-MEC 11**
REQ 26: ينبغي ألا يتطلب تطبيق عنصر الشبكة/نظام الإدارة امتيازات نفاذ **المستعمل الثانوي** لكي يعمل بصورة صحيحة.	**SER 4**	**MEC 20-MEC 23**
REQ 27: يجب أن تتوافر لعنصر الشبكة/نظام الإدارة المقدرة على عرض وقت وتاريخ آخر **استيفان** ناجح للمستعمل، على هذا المستعمل أثناء عملية الدخول، وحسب الاقتضاء.	**SER 4, SER 8**	**MEC 7-MEC 11**
REQ 28: ينبغي أن يُعرض على شاشة تسجيل الدخول الأول بيان بحصر الاستعمال في شخص معين، وتحذير بعدم التعدي على ملكيته، وذلك قبل أن يُصرح بأي نفاذ منطقي. وينبغي أن تدعم التجهيزات طولاً بحد أدنى قدره 1600 رمز. وينبغي تقديم رسالة بالتغيب.	**SER 4**	**غير قابل للانطباق**
REQ 29: بالنسبة لأي حالة تسجيل دخول فاشلة، ينبغي ألا يبلغ المستعمل سوى بأن عملية الدخول فشلت أو بأنا غير صحيحة. وينبغي عدم إبلاغه عبارات من مثل "معرف هوية المستعمل غير صحيح" أو "كلمة سر غير صحيحة".	**SER 8**	**MEC 7-MEC 11**
REQ 30: لا بد أن يقوم عنصر الشبكة/نظام الإدارة **بإغلاق** حساب المستعمل ومنعه من الدخول بعد بلوغ عدد محاولات الدخول الفاشلة عتبة معينة قابلة للتعديل. ويجب أن يشمل **الإغلاق** السطح البيني لوحدة التحكم، وينبغي ألا يشمل الحساب الأصلي المحدد بالتغيب والذي يقدم الدعم لجميع إجراءات الإدارة.	**SER 4**	**MEC 7-MEC 11**
REQ 31: ينبغي ألا يكون لدى عنصر الشبكة/نظام الإدارة آلية للتغاضي عن **استيفان** الدخول وعمليات التسجيل.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 32: ينبغي بشكل مطلق لأي عنصر من عناصر الشبكة/نظام الإدارة ألا يعرض صلاحيات واضحة، مثل كلمة السر، في أي واسطة من الوسائط، بما في ذلك عرضها على الشاشات المطرافية، والنسخ المطبوعة، والخزن في سجلات القيد.	**SER 8**	**MEC 7-MEC 11**
REQ 33: ينبغي أن تنفذ عنصر الشبكة/نظام الإدارة مدة تقادم لكلمة السر عن طريق عتبة قابلة للتعديل.	**SER 4**	**MEC 7-MEC 11**
REQ 34: إذا تجاوت كلمة سر يستخدمها مستعمل في الدخول الحد الزمني الخاص بذلك النظام، لا بد أن يقوم عنصر الشبكة/نظام الإدارة **بإغلاق** باب الدخول أمام معرف هوية هذا المستعمل لحين إتمام تغيير كلمة السر على النحو الصحيح.	**SER 4**	**MEC 7-MEC 11**
REQ 35: إذا ظل حساب ما ساكناً للفترة الزمنية للعتبة القابلة للتعديل، ينبغي أن يوجه عنصر الشبكة/نظام الإدارة إنذاراً.	**SER 4, SER 8, SER 9**	**MEC 7-MEC 11 MEC 33-MEC 37**

متطلبات الأمن المحددة في التوصية M.3016.1		خدمات الأمن المحددة في التوصية M.3016.2	آليات الأمن المحددة في التوصية M.3016.3
REQ 36:	إذا ظل حساب ما ساكناً للفترة الزمنية للعتبة القابلة للتعديل، يجب أن يقوم عنصر الشبكة/نظام الإدارة بتعطيل هذا الحساب بعد توجيه إنذار بذا التعطيل. وينبغي ألا تشمل عملية التعطيل حساب كل من الجهة القائمة على **إدارة النظام،** والجهة القائمة على **إدارة أمن النظام،** فضلاً عن حساب **المستعمل الثانوي.**	**SER 4, SER 8**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 37:	من أجل التمكين مجدداً من استخدام معرف هوية (ID) معطل عن الدخول، تلزم جهة تقوم بإدارة الدخول بصورة صحيحة، بأهم الإجراءات المخصصة لإدارة الأمن من أجل تشكيل وإعادة تحديد كلمات السر المستخدمة في الدخول.	**SER 4**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 38:	من أجل إعادة تحديد معرف هوية مغلق يستخدم في الدخول وإلغاء حالة الإغـ ـلاق، من الضروري توفير جهة تقوم بإدارة الدخول بصورة صحيحة، بأهم إجراءات إدارة الأمن المخصصة لإزالة الإغلاق أو لتغيير قيمة مؤقت إغلاق النظام.	**SER 4**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 39:	ينبغي للمستعمل الخروج من كل **دورة** يتم الدخول إليها بشكل صحيح أو عن طريق خمول النظام.	**SER 4**	**MEC 33-MEC 37**
REQ 40:	ينبغي أن ينهي عنصر الشبكة/نظام الإدارة أي **دورة** يتم الدخول إليها على نحو صحيح عندما يتجاوز المدة المنصرمة منذ آخر نشاط لهذه المدة القيمة القابلة للتعديل لمؤقت خمول النظام.	**SER 4**	**MEC 7-MEC 11**
REQ 41:	يجب أن يبقى نمط دور المستعمل دون تغيير أثناء تنفيذ أي تطبيق لعنصر الشبكة/نظام الإدارة أو الخروج منه.	**SER 4**	**MEC 20-MEC 23**
REQ 42:	ينبغي أن تكون قوة الخوارزميات المستخدمة في جميع تطبيقات التجفير المتناظر متسقة مع السياسة العامة الوطنية أو الصناعية أو التنظيمية المتبعة.	**SER 5, SER 6**	**MEC 24-MEC 26**
REQ 43:	لا بد أن يكون مستوى قوة الخوارزميات المستخدمة في جميع تطبيقات التجفير غير المتناظر متفقاً مع السياسة العامة الوطنية أو الصناعية أو التنظيمية المتبعة.	**SER 5, SER 6**	**MEC 27-MEC 28**
REQ 44:	يجب أن يكون مستوى قوة الخوارزميات المستخدمة في جميع تطبيقات تبادل المفاتيح متفقاً والسياسة العامة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا الصدد.	**SER 5, SER 6**	**MEC 38-MEC 40**
REQ 45:	من الضروري أن يكون عنصر الشبكة/نظام الإدارة في أي سطح بيني مادي أو منطقي يحمل **حركة إدارة** معينة داخل عنصر شبكة/نظام إدارة ما، قابلاً للتعديل بغية تأمين **حركة الإدارة** بالتلازم مع **الاستيفان الشديد** وحماية سرية الرموز المستعملة من أجل توفير الحماية للسرية والسلامة والتكرار.	**SER 2, SER 3, SER 5, SER 6**	**MEC 24-MEC 32**
REQ 46:	لا ينبغي إرسال أي كلمة سر منقولة بنص واضح غير مشفر إلا عبر **مسير مونوق** ما لم تستخدم في ذلك آلية لإرسال كلمات السر التي تستعمل لمرة واحدة. وفي حال استخدام كلمات سر من هذا القبيل، يمكن حينئذ إرسالها بنص واضح غير مشفر طالما أنه لا يوجد مضيف وسيط.	**SER 1, SER 2, SER 3, SER 5, SER 6**	**MEC 19**
REQ 47:	ينبغي أن يكون مستوى قوة الخوارزميات المستخدمة في جميع التطبيقات المتناظرة لتأمين سلامة المعطيات متفقاً والسياسة العامة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا المال.	**SER 5**	**MEC 29-MEC 30**
REQ 48:	لا بد أن يكون مستوى قوة الخوارزميات المستخدمة في جميع التطبيقات غير المتناظرة لتأمين سلامة المعطيات متفقاً مع السياسة العامة الوطنية، أو الصناعية، أو التنظيمية المتبعة في هذا الخصوص.	**SER 5**	**MEC 31-MEC 32**
REQ 49:	يجب أن تشمل جميع البرمجيات التي يتسلمها أحد مقدمي الخدمات أو غيره من الزبائن، حسب الاقتضاء، **استيفاناً** يحمل رموزاً سرية وآليات لحماية السلامة مثل **استيفان** من الإشارات الرقمية أو الرسائل المتناظرة مثلما هو محدد في التوصية ITU-T M.3016.3.	**SER 7**	**MEC 29-MEC 32**

متطلبات الأمن المحددة في التوصية M.3016.1		خدمات الأمن المحددة في التوصية M.3016.2	آليات الأمن المحددة في التوصية M.3016.3
REQ 50:	يجب أن يكون الجميع عناصر الشبكة/أنظمة الإدارة المتلقية لبرمجيات معينة قدرة على تفسير **الاستيقان** الذي يحمل رموزا سرية وآليات حماية التكاملية والتحقق من مصدر البرمجيات وسلامتها حسب الاقتضاء.	**SER 7**	**MEC 29-MEC 32**
REQ 51:	ينبغي إرسال جميع برامج تحديث البرمجيات، بما فيها برامج التصحيح، إلى عنصر الشبكة/نظام الإدارة المتلقي لهذه البرامج عبر **مسير مونوق**.	**SER 5, SER 6**	**MEC 19**
REQ 52:	يجب أن توفر جميع عناصر الشبكة/أنظمة الإدارة القدرة المتمثلة في عدم تمكن أي كيان من رفض مسؤولية أية إجراءات ينفذها فضلاً عن الآثار المترتبة على هذه الإجراءات.	**SER 7**	**MEC 29-MEC 32**
REQ 53:	ينبغي أن يكون بمقدور عنصر الشبكة/نظام الإدارة تسجيل أي إجراء يغير نعوت الأمن وخدماته ومراقبة النفاذ ومعلمات تشكيل الأجهزة، وكل محاولة تسجيل دخول ونتيجتها تؤدي إلى تنفيذ مؤقت خمول النظام المحدد في المتطلب 12 (REQ 12).	**SER 8**	**MEC 33-MEC 37**
REQ 54:	ينبغي أن يوفر عنصر الشبكة/نظام الإدارة المقدرة على تشكيل **أهم إجراءات إدارة الأمن** التي يتعين إدراجها في سجل الأمن.	**SER 4**	**MEC 33-MEC 37**
REQ 55:	من الضروري أن يكون بوسع عنصر الشبكة/نظام الإدارة تسجيل كل محاولة دخول ونتيجتها؛ وكل محاولة خروج أو إنهاء للدورة (سواء تمت عن بعد أم عبر وحدة التحكم).	**SER 8**	**MEC 33-MEC 37**
REQ 56:	يجب أن يكون بمستطاع عنصر الشبكة/نظام الإدارة التسجيل عن بعد عبر **مسير مونوق**.	**SER 5, SER 6, SER 8**	**MEC 33-MEC 37 MEC 19**
REQ 57:	ينبغي أن يضم كل قيد من قيود السجل المعلومات التالية: • وصف للإجراء أو الإجراء الفعلي الذي يجري تسجيله؛ • هوية المستعمل ومستوي الأمن لديه أو العملية التي استهلت الإجراء؛ • تاريخ ووقت حصول الإجراء؛ • معلومات عن مصدر الشبكة ومقصدها، في حال انطباق ذلك (عند الدخول مثلاً)؛ • إشارة إلى نجاح النشاط أو فشله.	**SER 8**	**MEC 33-MEC 37**
REQ 58:	يجب أن توفر جميع عناصر الشبكة/نظام الإدارة المقدرة اللازمة لتوجيه تبليغات للإنذارات بشأن أحداث مختارة.	**SER 9**	**MEC 41**
REQ 59:	يجب أن توفر جميع عناصر الشبكة/نظام الإدارة المقدرة اللازمة لإفساح المال أمام المستعمل ليحدد معايير اختيار الأحداث التي تُوجه بشأنها تبليغات للإنذار.	**SER 9**	**MEC 41**
REQ 60:	يجب أن تحول جميع عناصر الشبكة/نظام الإدارة التي لديها توصيلية قائمة على الرزم الحركة غير المطابقة للسياسة العامة للأمن التي تتبعها شبكة التحكم في المعطيات.	**SER 10**	**MEC 42**

التذييل I

اعتبارات أمن إضافية

تتسم إجراءات الأمن المبينة بالتفصيل في البنود التالية بطابع تعليمي. وهي لا تندرج ضمن نطاق المتطلبات المشروحة بالتفصيل التي تقدمها هذه التوصية، ولكن ينبغي بحثها لتوفير نظام مأمون. وتستخدم في بعض الحالات لغة تدل على الإلزام؛ غير أن هذا الاستخدام هو لأغراض الاطلاع على المعلومات ولا بد أن يكون بمثابة مثال لا أكثر. وتخضع البروتوكولات والتوصيات التي يضمها هذا التذييل لمناقشات وإسهامات تُقدم في المستقبل. وهي لا تعبر عن أي نية بصدد إدراج مضمونا في المعايير القائمة أو الناشئة أو استبعاده منها.

1.I قابلية انطباق الاعتبارات على حالات التشغيل والإدارة والصيانة والتوريد في المؤسسات

تطورت المؤسسات في يومنا هذا لتذهب إلى ما هو أبعد من الشبكات التقليدية للمؤسسات المعزولة التي كانت توجد في الماضي. فقد نمت لتصبح شركات تجارية تنتشر في مواقع عدة بحيث تمتد عبر مساحات جغرافية شاسعة وتتطلب توصيلها بالزبائن والشركاء في الأعمال التجارية عبر شبكة المواقع الشبكية على الإنترنت (إكسترانت). ويجب أن تفسح هذه المؤسسات المال أمام الزبائن والشركاء للحصول على سبيل للنفاذ إلى المعطيات الداخلية واتخاذ قرارات قائمة على هذه المعطيات فيما يتعلق بتشغيل الأعمال التجارية.

وتتولى المؤسسة بحد ذاتا تطوير شبكاتا وإدارتا أو يتم شراء هذه الشبكات من موردها الذي يشرف على إدارتا. وتفسح الخدمات التي يقدمها الموردون المال أمام المؤسسة لإدارة حصتها من الشبكة التي تشكل جزءاً من شبكة أكبر.

وبينما تمضي الصناعة قدماً، فإن متطلبات النفاذ إلى معطيات الكشف عن أعطال الشبكة وأدائها، وقدرة المؤسسة المتعاقدة على تشكيل مختلف مكونات الشبكة، تستوجب وضع آليات أمن ملائمة موضع التنفيذ. ويجب أن توفر هذه الآليات مستوى كاف من التحكم من أجل ألا تقتصر الحماية التي توفرها على الشبكة التي تديرها المؤسسة فحسب، بل تشمل أيضاً الشبكة الداخلية الخاصة بالموردين تحديداً. ويمكن أن تكون الشبكة الداخلية موصولة بينياً بذه الشبكات التابعة للمؤسسة وقد تشكل جزءاً من البنية الأساسية للاتصالات. وخلاصة القول، إن متطلبات الأمن اللازمة لتشغيل، وإدارة، وصيانة، وتوريد الحركة المبينة في هذا التذييل تنطبق انطباقاً تاماً على شبكات المؤسسات وشبكات مقدمي الخدمات/شبكات حمل الحركة.

2.I معمارية الوسيط العام لتوصيل طلبات المواضيع، والبروتوكول البسيط لإدارة الشبكة، ولغة التشفير القابلة للتوسيع، والبروتوكول البسيط للنفاذ إلى الهدف

ينبغي أخذ الاعتبارات التالية في الحسبان فيما يتصل بأمن كل من معمارية الوسيط العام لتوصيل طلبات المواضيع (CORBA)، والبروتوكول البسيط لإدارة الشبكة (SNMP)، ولغة التشفير القابلة للتوسيع (XML)، والبروتوكول البسيط للنفاذ إلى الهدف (SOAP). وإضافة إلى ذلك، توجد بروتوكولات أخرى قابلة للانطباق على حد سواء مثل بروتوكول تبادل الفدرات القابل للتوسيع. وبالرغم من عدم وجود مقترحات بصدد إدخال تعديلات على هذه البروتوكولات المتطورة، فبالإمكان الاستفادة من المناقشة التالية لتعزيز الأمن.

1.2.I معمارية الوسيط العام لتوصيل طلبات المواضيع (CORBA)

تشمل خدمات الأمن التي تقدمها معمارية الوسيط العام لتوصيل طلبات المواضيع (CORBA) العناصر الوظيفية للأمن المتعلقة باستيقان الجهات المستعملة (المستعملون من البشر والمواضيع)، والتصريح لهذه الجهات بالنفاذ إلى الأهداف، وتدقيق الأمن، وأمن الاتصال، وعدم الرفض، والإدارة. ومع هذا، يمكن أن تذهب جميع هذه الخدمات إلى ما هو أبعد مما تتطلبه تطبيقات كثيرة. وبدلاً من ذلك، فقد لا تحتاج هذه التطبيقات سوى إلى أمن الاتصال والعناصر الوظيفية لاستيقان المستعمل على مستوى النظام بالاستناد إلى تكنولوجيا أمن طبقة النقل (TLS) (وسلفها، طبقة مقابس الأمن (SSL)) وذلك لأسباب تتعلق

بالتيسر والبساطة. وأخيراً، قد لا تحتاج بعض التطبيقات إلى توفير الأمن. وبناء على ذلك، فإن المتطلبات الاختيارية المذكورة أدناه تعكس ثلاثة خيارات ممكنة، هي:

- عدم توافر الأمن؛
- استعمال وسيط توصيل طلبات المواضيع (ORB) تكنولوجيا أمن طبقة النقل (TLS) (أو طبقة مقابس الأمن (SSL)) لتوفير أمن الاتصالات والاستيقان على مستوى النظام، والذي هو أساساً أمن "الدورة"؛
- استعمال وسائط توصيل طلبات المواضيع (ORB) لخدمة أمن الاتصالات، والاستيقان، وعدم الإنكار، ولتزويد قوائم مراقبة النفاذ للمجموعات أو الأفراد الذين ينفذون إلى أحاد المواضيع أو العمليات.

وبالإمكان الاطلاع على المزيد من المعلومات عن الأمن الموفر في إطار معمارية الوسيط العام لتوصيل طلبات المواضيع (CORBA) في التوصية ITU-T Q.816، والمعنونة خدمات شبكة إدارة الاتصالات القائمة على بنية وسيط طلب المواضيع المشتركة والتوصية ITU-T Q.816.1، والمعنونة خدمات شبكة إدارة الاتصالات القائمة على بنية الوسيط العام لتوصيل طلبات المواضيع: تمديدات لدعم السطوح البينية المحبحبة.

وفي حال استخدام معمارية الوسيط العام لتوصيل طلبات المواضيع (CORBA) في السطوح البينية لعنصر الشبكة/نظام الإدارة (NE/MS)، ينبغي تطبيق آليات الأمن التابعة لهذه المعمارية (CORBA). ولا بد أن يتسم مستوى المطابقة في تنفيذ الأمن بواسطة المعمارية (CORBA) بالوضوح. وتقدم المناقشة التالية إرشادات بشأن أمن هذه المعمارية (CORBA). ولا ينبغي استنتاج أية محاولات بخصوص تحديد المعايير. وعند تقديم النواتج أو الأنظمة بالاستناد إلى المعمارية (CORBA)، تكون مستويات الأمن الأساسية كالتالي:

- المستوى 0: عدم توفير الأمن في التطبيق، والبرامج غير مدركة للأمن. وينبغي توفير الاستيقان، والتجفير، وتكاملية المعطيات، والتصريح بتنفيذ المواضيع، وحالات تسجيل التدقيق، وإدارة مجال الأمن.
- المستوى 1: قد تكون البرامج مدركة للأمن، ما يعني أنا قد تطلب سطحاً بينياً لبرمجة التطبيق من أجل النفاذ إلى خدمات إضافية من قبيل التحقق من الإشارات، وتدقيق النفاذ إلى المواضيع، وتدوين سجلات التدقيق.
- المستوى 2: يوفر هذا المستوى الدعم للإشارات الرقمية التي تسمح بتسجيل المعاملات وعدم إنكارها. ويكتسي هذا الأمر أهمية خاصة عند التشغيل عبر منظمات مختلفة، مثل التشغيل في سياق عمل تجاري إلى عمل تجاري أو ترتيب إدارة شبكات النظراء.

وتحدد مواصفات القدرة الشائعة على التشغيل البيني الآمن (CSI) معايير معينة عن طريق تشفير مواصفات القدرة على التشغيل البيني الآمن عند استخدام بروتوكول عام بين وسطاء عامين لتوصيل طلبات المواضيع (ORB)/وبروتوكول إنترنت بين وسطاء عامين لتوصيل طلبات المواضيع (ORB)، وذلك كما يلي:

- المستوى 1 للقدرة الشائعة على التشغيل البيني الآمن: تُنقل هوية المستعمل الطالب من المرسل إلى المستقبل.
- المستوى 2 للقدرة الشائعة على التشغيل البيني الآمن: تُنقل هوية المستعمل الطالب من المرسل إلى المستقبل، بيد أنه يمكن إرسال هذه الهوية إلى مواضيع أخرى كيما يتسنى لهذه المواضيع أن تنتحل شخصية المستعمل.
- المستوى 3 للقدرة الشائعة على التشغيل البيني الآمن: إضافة إلى نقل الهوية، قد تشتمل نعوت المستعمل الطالب المنقولة من الزبون إلى الهدف على معلومات أخرى عن التخويل، من قبيل عضويته في الأدوار أو المجموعات.

وينبغي أن يقوم الموردون بما يلي:

- الإلمام بشكل كامل بقدرات أمن التكنولوجيا المختارة للوسيط العام لتوصيل طلبات المواضيع؛
- ضمان تلبية هذه القدرات لمتطلبات الأمن المبينة في موضع آخر من هذه التوصية.

والمعمارية CORBA معنية بالأهداف، مثلما يدل اسمها على ذلك ضمناً. ويتعلق أمن الأهداف بمنع استعمال الهدف دون تصريح من خلال إنفاذ مجموعة من قواعد مراقبة النفاذ. ويكفل الأمن الذي توفره المعمارية CORBA مساءلة المستعمل عن الإجراءات التي يتخذها بشأن هدف معين أو داخله، ويضمن تيسر الأهداف.

ويختلف أمن الأهداف عن الكثير من جوانب الأمن الأخرى. ولا يحتاج المطور في الكثير من الأحيان إلى معرفة تفاصيل الأمن لأن الأمن يُطبق في مرحلة لاحقة، وكذلك الحال مع المغلف. وبناء عليه، توجد جوانب معينة غاية في الأهمية. وقد تُستنسخ الأسماء في المعمارية CORBA، أو قد لا تُوجد هذه الأسماء مطلقاً؛ وربما توجد فيها أرقام مرجعية حصراً. وينبغي أن تكون هناك إمكانية لتحديد سياسة الموضوع من دون معرفة اسمه. وبالمثل، يجب أن تكون هناك إمكانية لتحديد هذه السياسة فيما يتعلق أيضاً بالأهداف التي لديها الكثير من الأسماء، ولا بد من تطبيق هذه السياسة بصرف النظر عن الاسم المستخدم لتأمين الموضوع.

ولدى الأنظمة النموذجية الموجهة نحو المواضيع عشرات الآلاف من المواضيع، وليس من المعقول أن يُتوقع تحديد الأمن لأحاد المواضيع. ولذلك، ينبغي أن تكون هناك إمكانية لجمع الأهداف معاً وتحديد سياسة معينة تُطبق على مجموعة المواضيع التي تكون احتياجاتا من الحماية متماثلة.

- *الاستيقان الطرف إلى الطرف*: بإمكان المعمارية CORBA نقل سياق المستعمل إلى تطبيق آخر. وقد يكون قبول هذه المعلومات من دون إجراء المزيد من التحقق ممكناً في الحالات التي تُقام فيها علاقة ثقة قوية بين هذه الأنظمة. ومع ذلك، فقد يكون اقتران أمن الأنظمة الأخرى اقتراناً وثيقاً بأمن المعمارية CORBA أمراً ضرورياً في الحالات التي لا توجد فيها آليات أخرى. والاستيقان من طرف إلى طرف مهم للغاية، وإجراء تحقق مما إذا كانت الجهة البائعة توفر هذا الاستيقان أمر جدير بالاهتمام.
- *مراقبة النفاذ*: تقدم المعمارية CORBA الدعم لفكرة تسجيل الدخول على أساس الدور. وينبغي دوماً تطوير الأنظمة بالاستفادة من هذه الخاصية لأنا لا تقلل تكاليف الإدارة فحسب، وإنما تبسطها، مما يعني ضعف احتمال وجود أخطاء في التشكيل.
- *التجفير*: يجب أن يكون استخدام التجفير داخل المعمارية CORBA متفقاً مع المتطلبات المذكورة في هذه التوصية. ومن الضروري الاستفادة من خصائص هذه المعمارية (CORBA) استفادة قصوى فيما يتعلق بالتكاملية، والسرية، واستيقان المصدر، ولا سيما عند الاتصال عبر شبكة من أي نمط.
- *إدارة السياسات العامة*: إدارة السياسات العامة للمعمارية CORBA مسؤولة عن تحديد معلومات عن الحالات، والمستعملين، وسياسة النفاذ إلى مواضيع الأدوار، وسياسة حماية الرسائل، وسياسة التدقيق. وينبغي أن يتسم تصميم جميع الجوانب المتعلقة بتسمية الحالات والمواضيع بكل الوضوح. ولا بد من تحديد الأدوار بوضوح بقصد ضمان الفصل بين المهام كما ينبغي.

2.2.I أمن البروتوكول البسيط لإدارة الشبكة (SNMP)

يوفر البروتوكول البسيط لإدارة الشبكة (SNMP)، وهو الطريقة واسعة الاستخدام لإدارة طائفة متنوعة من المعدات القائمة على المعالج، القدرة على القيام بما يلي:

- الحصول على معلمات تشكيلة الأجهزة؛
- تحديد هذه المعلمات؛
- إرسال إنذارات من الجهاز المُدار إلى نظام تحليل مركزي.

ويشوب الكثير من الصيغ الموزعة للبروتوكول البسيط لإدارة الشبكة أوجه ضعف شديدة تتعلق بالأمن. ففي الصيغتين 1 و2 من هذا البروتوكول، تُرسل كلمة السر (المعروفة على أنا السلسلة المشتركة) في نص واضح غير مشفر. وإضافة إلى ذلك، وعلى الرغم من إمكانية إجراء عمليات تحقق للتثبت من صحة عنوان زبون بروتوكول الإنترنت، فبإمكان أي جهة تشن هجوماً على النظام وتكون قابلة للتحديد بشكل معقول أن تُقلد عناوين بروتوكول الإنترنت المستخدمة. وتعرض الصيغتان 1 و2 من البروتوكول SNMP لعمليات كشف أمنية هامة في عدة شبكات. وبناء على ذلك، ينبغي عدم استخدام هاتين الصيغتين إلا كملاذ أخير. وتعكف لجنة الدراسات 4 التابعة لقطاع تقييس الاتصالات في الاتحاد (ITU-T) على دراسة إمكانية تحديد حزمتي بروتوكول جديدتين، هما:

- حزمة الصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3) أو V2C بالتلازم مع تحقيق أمن طبقة النقل (TLS) عبر بروتوكول مراقبة الإرسال (عدم وجود مراقبة للنفاذ)؛
- وحزمة الصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3) المقترن بنموذج أمن المستعمل عبر بروتوكول داتاغرام المستعمل (كحزمة استشرافية).

وحيثما يُنشر البروتوكول البسيط لإدارة الشبكة (SNMP)، فإن الصيغة 3 منه هي المستوى المفضل. وهي صيغة أكثر أمناً وينبغي استخدامها في جميع الأنظمة الجديدة لأنها توفر الحماية ضد تعديل المعطيات، والتنكر، وإعادة ترتيب الرسائل، وفقدان السرية. ولا بد من مراعاة التدابير المضادة التالية لتأمين النفاذ بالصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3) إلى عناصر الشبكة (NE)، وهي كالتالي:

- ينبغي أن يرسل الموظف القائم على برنامج إدارة البروتوكول البسيط لإدارة الشبكة إنذاراً إلى المدير في حال تلقيه أمراً من مصدر مجهول.
- يجب استخدام مراقبة النفاذ لإفساح المال أمام استقبال رسائل البروتوكول الصادرة حصراً عن مدير مصرح له بذلك. ومن الضروري رفض رسائل هذا البروتوكول الواردة من جميع المصادر الأخرى ومعاملتها وفقاً لسياسات الأمن التي تناسبها. وربما يُفضل حجب الطلبات غير المصرح بها في جهاز الاستقبال وفي محيط الشبكة.
- ينبغي عدم استخدام السلسلة المشتركة المحددة بالتغيب.
- يجب تسجيل الانتهاكات والأخطاء المرتكبة بشأن النفاذ.
- تستخدم الصيغة 3 من البروتوكول البسيط لإدارة الشبكة (SNMPv3) معيار تجفير المعطيات بوصفه معياراً محدداً بالتغيب؛ غير أنه يمكن استخدام خوارزميات ذات مأمونية أكبر.
- لا بد من استخدام الصيغة SNMPv3 على الأقل مع صيغة الاستيقان بدون خصوصية (AuthNoPriv) التي تؤمن الاستيقان لكن دون توفير سرية المعاملات. ويفضل استخدام صيغة الاستيقان مع الخصوصية (AuthPriv).
- يجب تمكين الموظف القائم على تشغيل البروتوكول البسيط لإدارة الشبكة (SNMP) على التسجيل.
- يجب تعطيل جميع الخدمات أو القدرات غير المطلوبة صراحة، بما فيها البروتوكول البسيط لإدارة الشبكة (SNMP) إذا كان في حالة تمكين.

3.2.I لغة التشفير القابلة للتوسيع (XML)

يوفر معيار لغة التشفير القابلة للتوسيع (XML) لغة تستعمل في تحديد هياكل المعطيات. والمعيار المستخدم حالياً هو 1.0. والصيغة 1.1 هي توصية مرشحة قيد النظر. وتسعى اللجنة التقنية لخدمات الأمن التابعة لمنظمة تطوير معايير المعلومات المنسقة (OASIS) إلى توسيع نطاق العناصر الوظيفية للأمن عن طريق تعزيز لغة التشفير القابلة للتوسيع (XML). وتواصل منظمة تطوير معايير المعلومات المنسقة (OASIS) عملها بشأن وضع لغة التشفير المتداولة في توكيد الأمن (SAML) في صيغتها النهائية. وتستند اللغة (SAML) إلى أربعة تأكيدات، هي كالآتي:

- *الاستيقان* - استيقان المصدر من الموضوع؛
- *النعت* - معرف هوية مورد محدد متجانس أو مخطط للتوسيع يحدد النعت؛
- *القرار* - يبلغ مدى صحة الاستيقان؛
- *التخويل* - الموضوع مأذون له بالنفاذ إلى المورد (الموارد).

ويجب أن تشتمل تأكيدات اللغة (XML) على ما يلي:

- *معلومات أساسية* - تضم معرف هوية أو اسم وحيد للتأكيد ويشمل عموماً تاريخ ووقت الإصدار والفترة الزمنية لنفاذ صحة التأكيد؛
- *وادعاء* - وثيقة تصف استعمال التأكيد؛

- *وشرط* - قد يخضع التأكيد لشروط تقضي بصحته أو عدمها؛
- *ومشورة* - تقدم معلومات إضافية من قبيل التأكيدات المستفاد منها في اتخاذ قرار بشأن السياسات العامة.

4.2.I البروتوكول البسيط للنفاذ إلى الهدف (SOAP)

البروتوكول البسيط للنفاذ إلى الهدف (SOAP) 1.1 هو التوصية الحالية الصادرة عن اتحاد شبكة الويب العالمية. وهذا البروتوكول (SOAP) هو عبارة عن نسق لترتيب الرسائل لا يرتبط ببروتوكول معين. ويستخدم عموماً بروتوكول نقل النصوص الفائقة (HTTP)، بيد أن بإمكانه استخدام بروتوكولات أخرى مثل البروتوكول البسيط لنقل البريد الإلكتروني (SMTP) أو بروتوكول نقل الملفات (FTP). وعند استخدام البروتوكول (SOAP) مع بروتوكول نقل النصوص الفائقة (HTTP)، فإن جدار الحماية يعتبر البروتوكول (SOAP) بمثابة البروتوكول (HTTP) وعادة ما يفسح المال أمامه للمرور. ومن المحتمل أن يقوم جدار الحماية بترشيح البروتوكول البسيط للنفاذ إلى الهدف (SOAP)، حتى في حالة عدم إدراكه لهذا البروتوكول (SOAP). ومع ذلك، فإن هذا الترشيح ليس مهمة سهلة وهو عرضة للأخطاء. وهو يمثل تحدياً لأن بإمكان التجفير أن يخفي مضمون المعطيات المنقولة وسياقها (أي لغة التشفير القابلة للتوسيع (XML))، وليس لدى البروتوكول (SOAP) مخططاً متجانساً للعناوين أو هيكلاً داخلياً (ما معناه أن الرأسيات وأسماء الطرائق اختيارية).

3.I المراقبة الإلكترونية المخوّلة قانونياً

ينبغي أن تراعي حاملات الاتصالات اعتبارات الأمن التالية فيما يخص تنفيذ المراقبة الإلكترونية المخوّلة قانونياً (LAES).

ولا بد أن تتسم ممارسات الأمن المتصلة بأنشطة المراقبة الإلكترونية المخوّلة قانونياً (LAES) بالقوة وكذلك الحال بالنسبة لأي عنصر مهم من عناصر الشبكة، أو نظام دعم التشغيل (OSS)، أو نظام الإدارة مع بعض الحالات الاستثنائية التي ترد أدناه. وتتعلق هذه الممارسات بضرورة الحفاظ على سرية أنشطة المراقبة الإلكترونية المخوّلة قانونياً.

- المشاركة في أنشطة المراقبة الإلكترونية المخوّلة قانونياً مقصورة على الموظفين المرخصين بذلك.
- المعلومات المتعلقة بالمراقبة الإلكترونية المخوّلة قانونياً، بما في ذلك هوية الهدف والوكالة (الوكالات) المعنية بإنفاذ القانون والمشاركة في المعلومات المتعلقة بمستوى النداء وبتحديد النداء ستتم حمايتها من الكشف عنها لموظفين غير مصرح لهم بذلك.
- لا يسمح بالنفاذ إلى أوامر وعمليات المراقبة الإلكترونية المخوّلة قانونياً سوى للموظفين المصرح لهم بذلك.
- يتعين الاحتفاظ بقائمة محدثة بأسماء الموظفين المصرح لهم بالنفاذ إلى أنشطة وعمليات وإجراءات المراقبة الإلكترونية المخوّلة قانونياً والمحافظة عليها وإدارتها وتوجيهها.
- تُوثق أنشطة، وسياسات، وإجراءات أمن المراقبة الإلكترونية المخوّلة قانونياً توثيقاً صحيحاً وتُيسر للموظفين المصرح لهم بذلك.
- تُحفظ سجلات الأمن وقيود الأنشطة المتصلة بالمراقبة الإلكترونية في مرفق مؤمن وتُخزن فيه.
- يتم تنفيذ عملية موثقة ودقيقة لتحديد الوكالات المعنية بإنفاذ القانون واستيقانا ومعالجة طلبات المراقبة الإلكترونية (LAES).

4.I اعتبارات الأمن المادي

ينبغي مراعاة الاعتبارات التالية المتعلقة بالأمن المادي. وعند إعداد متطلبات الأمن، فإن الأمن المادي يعد مكوناً مهماً. وتفترض معظم معماريات الأمن أن البيئة المادية محمية. ففي السابق، كانت جميع عناصر الشبكة موجودة في بنايات مكاتب مركزية (CO). ويوجد في هذه البنايات موظفون يعملون على مدار الساعة من أجل تشغيل هذه المعدات، وتزويدها باحتياجاتا، وإدارتا، وصيانتها. ويعرف الموظفون بعضهم بعضاً، ولا يمكن للدخلاء أن يحصلوا على سبيل للنفاذ إلى هذه المواقع من دون أن يشاهدهم أحد الموظفين ويعترض على وجودهم. ولكن البيئة اليوم مختلفة تماماً. وثمة ميل إلى تركيب

المعدات اللاسلكية في العراء في بيئة غير مؤمنة. كما أن الكثير من المكاتب المركزية (CO)، إن لم يكن معظمها، هي مراكز غير مزودة بالموظفين ومعتمة معظم الوقت. وتنفذ الطواقم الجوالة وأحاد الجوالين الموفدين من موقع مركزي، مهام تحسينات ومهام صيانة مجدولة زمنياً. ويُعتبر اليوم وجود حراس أمن يعملون ليلاً ونارا طوال أيام الأسبوع (7/24) استثناء نادراً. وتُستخدم أيضاً المكاتب المركزية (CO) من جانب موظفين من خارج المحطة بوصفها مكاناً مناسباً للاجتماع وخزن الأدوات والمعدات. وفيما يلي خصائص المرفق المؤمن:

- يُسجل ويُقيد دخول جميع الموظفين وخروجهم.
- تخضع الجهات البائعة والموظفون المتشاركون في الموقع لفحص دقيق ويخضع دخولهم/خروجهم للتسجيل والتقييد.
- يكون النفاذ المادي إلى عنصر الشبكة مقصورا على الموظفين المصرح لهم بذلك.
- يخضع الموظفون المتشاركون في الموقع لنفس متطلبات النفاذ شأنهم في ذلك شأن مقدم الخدمة القائم بالتشغيل.
- لا يجوز لأي فرد حاصل على سبيل نفاذ مادي مشروع إلى البناية أن يحصل على نفاذ منطقي إلى عناصر الشبكة (NE)، وحدات التحكم، أنظمة دعم تشغيل (OSS) أجهزة النفاذ إلى الشبكة دون استيقانه استيقاناً محمياً.
- يتعين الكشف عن النفاذ غير المصرح به والاستجابة لمقتضياته بطريقة مناسبة التوقيت.
- يتعين تيسير خدمات من قبيل المياه، والطاقة الكهربائية، والاتصالات.
- تخضع المواقع للمراقبة من جانب موظفي الأمن الجوالين فيها على نحو عشوائي، وأنظمة الإنذار التي تراقب وتسجل فتح الأبواب والنوافذ وإغلاقها، وكاشفات الحركة، والكاشفات الاستدلالية، ومراقبة المواقع الحساسة بالفيديو عن بعد.
- ينبغي توثيق مسألة حفظ وسائط المراقبة وسجلاتها. ويتباين طول فترة الحفظ تبعاً لمستوى الخطورة.

وتقدم البنود الآتية معلومات إضافية عن الأمن المادي. ويمكن الاطلاع على وصف مفصل لمسائل الأمن المادي في *إرشادات تقييم أمن شبكة التبديل العمومية*، سبتمبر 2000، الصادرة عن نظام الاتصالات الوطني.

1.4.I أمن المباني المادي

تنفذ المنظمات عادة مستويات مختلفة من مراقبة النفاذ إلى المباني وفقاً لأهمية الأصول الموجودة داخل المرفق. وغالباً ما تشيد الشركات الكبرى مرافق للأمن مستقلة بدرجة عالية تُخصص لأهم مكونات الشبكة، مثل البدالات أو مراكز المعطيات. وتحدد أهمية الأصول الموجودة داخل المرفق مستوى الأمن. ويتحقق هذا التحديد أثناء مراجعة مراحل الاكتشاف واستعراض تقييم الأصول. ويرد في الفقرات التالية بنود لتقييم مرفق يأوي أصولاً قيمة للغاية أو مهمة. وستجرى عمليات استعراض تتطلب بذل جهود أقل بشأن المرافق الأقل حساسية. ويجب أن يحد التقييم العام للأمن المادي مستوى الحماية اللازم والجودة النسبية لآليات الحماية القائمة.

1.1.4.I أمن المباني العام

على الرغم من أن أبواب المبنى ونوافذه عادة ما تعتبر النقاط الرئيسية للنفاذ إليه، فإنه ينبغي النظر في نقاط أخرى (مثل فتحات التهوية، ونقاط دخول المياه، والغاز، والاتصالات، والكهرباء، وقنوات التصريف)، وذلك اعتماداً على أنواع التهديدات. ومن الضروري النظر في نقاط دخول إضافية من قبيل أقبية الكبلات الموجودة في المكتب المركزي (CO)، فضلاً عن أماكن أخرى يكون فيها احتمال إلحاق الضرر بالمبنى قائماً. وعلاوة على ذلك، لا بد من النظر في المال الفاصل بين العامة والمبنى تحديداً. ويمكن أن تسهم المساحات الخضراء، ونباتات الزينة، والإنارة، والحواجز في توفير الطبقة الأولي من الدفاع عن محيط المبنى لأنها تُبطئ من محاولات الاقتراب خفية من المبنى أو تمنعها. وبالإمكان استخدام حواجز مادية مثل أعمدة الخرسانة أو أحواض الخرسانة الضخمة المستعملة لزرع نباتات الزينة بغية منع اقتراب السيارات، أو الشاحنات، أو المركبات الأخرى التي يحتمل أن تنوي إلحاق الضرر بالمبنى. وتعمل آلات التصوير المركبة خارج المبنى وسائر معدات المراقبة على زيادة تعزيز هذا المال الفاصل أو توسيع مساحته.

2.1.4.I الحراس، والأقفال، والشارات المعرفة للهوية

يحمي حراس المباني المحيط الخارجي للمبنى وأحياناً المناطق الداخلية. وفيما يتعلق بالمرافق الحساسة، ينبغي أن يكفل الاستعراض ما يلي:

- إقفال جميع الأبواب التي يتم الدخول منها إلى المرفق أو إخضاعها للحراسة في جميع الأوقات.
- تزويد جميع الأبواب التي لا تستخدم عادة، مثل مخارج الطوارئ، بأجهزة إنذار. ولا بد أن يكفل الاستعراض عمل أجهزة الإنذار كما ينبغي ووجود إجراءات للاستجابة لمقتضيات الإنذارات التي توجهها.
- تركيب الأبواب بصورة صحيحة كيما لا يتسنى خلعها من الخارج (كأن تكون مفصلات الأبواب وترابيسها محمية مثلاً من العبث بها من الخارج).
- ضرورة وجود حراس عند المداخل والمخارج أثناء الفترات التي يبلغ فيها الدخول والخروج ذروتهما. وينبغي مراقبة الأبواب خلال الفترات التي هي ما دون الذروة، ومن الضروري أن تكون هناك وسيلة أخرى للدخول (مثل البطاقات الإلكترونية، والبطاقات التقاربية المصورة، والمفاتيح).
- ينبغي أن يكون الدخول من الأبواب غير الخاضعة للحراسة باستخدام طريقة تتطلب التعريف بهوية الشخص الداخل.
- تُزود الأبواب غير الخاضعة للحراسة التي تسمح بالدخول عبرها بواسطة المفاتيح أو وسيلة أخرى بآليات تحول دون "تتبع الدخول"[5]. ويمكن استخدام شراك الإيقاع بالدخلاء، والأبواب الدوارة، والكاشفات لمنع تتبع الدخول أو توجيه إنذار بشأن حصوله.
- يتعين أن تكون مؤهلات التوظيف، والتدريب، وطرائق الحجز المستخدمة في توظيف الحراس كافية وملائمة. ويكتسي هذا الأمر أهمية خاصة فيما يتعلق بخدمات الحراسة التي يتم التعاقد عليها، وهي خدمات شائعة.
- ينبغي أن يكون لدى الموظفين، والجهات البائعة الموجودة في الموقع، والمتعاقدين، وغيرهم من الأفراد المصرح لهم شارات يعرضونها طوال فترة تواجدهم في المبنى.
- يُمنح الزوار من غير الموظفين معرف هوية مؤقت، من قبيل جواز مرور خاص بهم، وهم مطالبون بعرضه بوضوح.
- يتعين وجود إجراءات وشروط يتسنى للزوار الدخول بموجبها إلى المبنى والعمل فيه من دون مرافقة الحراس لهم، وشروط أخرى ينبغي بموجبها أن يكون الحرس برفقتهم.
- ينبغي أن تحمل شارة الموظف صورة ملونة. ويجب أن تكون الصورة كبيرة بما فيه الكفاية كيما لا يضطر الموظف إلى إعطاء الشارة إلى الحارس ليراها. ولا بد أن تكون الصورة مثبتة داخل الشارة لكي يتعذر تغييرها أو استبدالها. ومن الضروري أن تكون واضحة بما فيه الكفاية كيما يتمكن الحارس من مقارنتها بوجه حاملها.
- يتعين أن تعرض الشارة اسم الموظف وأية معلومات أخرى تحدد هويته (مثل الرقم، شفرة الأعمدة) عرضاً واضحاً.
- ينبغي أن تحمل الشارة علامة أو إشارة تميز الموظفين عن غير الموظفين فيما يتعلق بالدخول إلى المباني.
- يتعين أن تكون الشارة متينة وتقاوم البلى، أو التلف، أو التغيير قدر المستطاع.
- ينبغي أن تضم الشارة معلومات إلكترونية أو مغنطيسية قد تحتاجها أجهزة قراءة البطاقات.
- يمكن أن تتضمن الشارة رقاقة ذكية تحوي معلومات إضافية، من قبيل معطيات بيولوجية إحصائية أو شهادات المعيار X.509.
- لا بد أن توصل أنظمة الاستيقان من الشارات والتصريح بها بدليل مركزي للأمن لإفساح المجال أمام تغيير امتيازات الدخول أو إلغائها فوراً.

[5] يشير تعبير تتبع الدخول إلى تصرف شخص غير مصرح له يتمثل في تعقبه الدخول من باب يفتحه شخص مصرح له بفتحه.

- يتعين أن تدعم الشارات القدرة على تقييد الدخول إلى بعض مناطق حرم المؤسسة، بالمقارنة مع الدخول الكامل، وذلك حسب الاقتضاء.
- ينبغي أن يكون للشارة عنوان يمكن إرسالها عليه من دون سداد أجور البريد في حال فقدانا، أو في حال عثر عليها فرد من غير الموظفين.
- يتعين أن يكون بوسع أمن المؤسسة أو المبنى أن يعطل أو يلغي صلاحية أي شارة مفقودة، أو شارة لا يسمح لحاملها بعد الآن بالدخول إلى البناية أو إلى حرم المؤسسة.
- ينبغي أن يقوم أحد الأفراد (المدير، حارس المبنى، أمن المؤسسة) بحجز الشارة أو إتلافها عندما ينهي حاملها فترة توظيفه كيما يتعذر استخدامها بصورة غير شرعية.

وليس الحراس وحدهم هم الموظفون المسؤولون عن الحفاظ على الأمن الداخلي لمبنى معين. وغالباً ما يعزز أمن هذا المبنى الموظفون المصرح لهم بالتواجد فيه من خلال التيقظ والمراقبة السلبية. وينبغي أن يحدد التقييم ما إذا كان الموظفون مخولين حق الاعتراض على وجود الموظفين غير المصرح بتواجدهم في المناطق الخاضعة للمراقبة. وإجراء اختبار للتسلل إلى هذه المناطق يمكن أن يكون قيماً من أجل التحقق من مدى التدريب الذي حصل عليه الحراس بالنسبة لأهمية الأمن المادي. وقد يحاول المستعرضون في هذا الاختبار التسلل من أمام الحراس أو التحدث في طريق العبور أمامهم أو يحاولون إغواء الموظفين للسماح لهم بالدخول عبر المداخل غير الخاضعة للحراسة.

3.1.4.I إدارة المفاتيح المادية والمنطقية

نادراً ما تستخدم المفاتيح المادية التقليدية في المرافق الحساسة لأنه من الصعب جردها واستردادها وهي لا توفر تسجيلاً تدقيقياً للمستعمل. وغالباً ما يقتصر استخدامها على الدخول إلى الأقسام الداخلية من المبنى، مثل المخازن، وغرف الحراسة، ومقصورات الأسلاك. ومع ذلك، لا يزال استخدامها شائعاً، حيث توجد شركات تجارية ومنشآت تستخدم أقفالاً تفتح بمفاتيح بوصفها وسيلتها الرئيسية للدخول إلى المباني أو النفاذ إلى المناطق الحساسة الموجودة داخل هذه المباني. وعندما يصُح ذلك، تكون التحفظات التالية مهمة:

- ينبغي وضع إجراءات بشأن ترخيص توزيع المفاتيح على الأفراد، بما في ذلك مراقبة المفاتيح وتسجيل النفاذ والتوزيع؛
- لا بد أن تُرقم المفاتيح بصورة فردية؛
- من الضروري حفظ قائمة جرد كاملة بالمفاتيح ومالكيها وتدقيقه؛
- يجب أن تكون هناك معايير موضوعة موضع التنفيذ لاستبدال الأقفال عند فقدان مفاتيحها؛
- ينبغي تنفيذ عمليات تدقيق دورية لجرد المفاتيح، ومن الضروري وضع إجراءات موضع التنفيذ للتوفيق بين أوجه التناقض التي تشوب الموضوع؛
- يتعين وضع إجراءات موضع التنفيذ لاسترداد المفاتيح عندما لا يكون هناك داع للنفاذ أو عند تغيير التراخيص.

وينبغي تقييم الإجراءات المتعلقة بالمفاتيح المنطقية (مثل البطاقات التقاربية المصورة) على أساس نفس المعايير. وإجراءات استرداد المفاتيح، وتسجيل الدخول والخروج، ومنح التراخيص هي إجراءات تبسطها المفاتيح المنطقية لأن هذه الأنظمة توفر مرافق مركزية تستخدم في المراقبة، ومنح التراخيص، وتعطيل المفاتيح. ومع ذلك، يجب وضع إجراءات موضع التنفيذ لضمان إخطار المسؤولين عن حفظ قائمة الجرد الخاصة بالمفاتيح، وقاعدة معطيات التصاريح بمغادرة الأفراد أو حصول تغيير في المتطلبات اللازمة لدخولهم. وينبغي تقييم الأقفال التي تُفتح بتوليفة أرقام أو حروف، وهي حالة خاصة من الأقفال المنطقية، لضمان عدم القدرة على التعرف على توليفات الأرقام والحروف من آثار البلى أو/من التوليفات المدونة. ولا بد من تغيير توليفات فتح الأقفال في حال تغيير تصاريح الدخول.

4.1.4.I الفصل الوظيفي بين مراقبة المرافق ومراقبة النفاذ المتعدد المستويات

ينطبق الأمن المادي على الأقسام الداخلية لمبنى ما فضلاً عن انطباقه على المحيط الخارجي للمبنى. وينبغي مراقبة النفاذ إلى المناطق الداخلية للمبنى التي تعتبر حساسة أو مهمة من حيث التشغيل عندما يكون النفاذ إلى محتوياتها مقيداً لأي سبب كان (كأن تتضمن مثلاً معطيات، أو اختبارات، أو معدات حساسة). ويتعين عموماً القيام بما يلي:

- يجب وضع المرافق الحساسة لأجهزة الحاسوب والشبكة داخل مناطق لديها آليات مستقلة لمراقبة النفاذ المادي إلى هذه المرافق. ولا ينبغي السماح بالنفاذ إليها سوى للذين يحتاجون إلى ذلك.
- يجب وضع إجراءات موضع التنفيذ لضمان حفظ المعلومات الخاصة في مرافق آمنة عندما لا تكون قيد الاستخدام. ومن الضروري إقفال المكاتب وغرف الملفات التي تُحفظ فيها هذه المواد عادة. ويجب أيضاً إقفال الخزانات التي تُحفظ فيها المعلومات الخاصة.
- يجب التحكم في جميع النقاط التي يحتمل الدخول منها إلى المرافق الحساسة لأجهزة الحاسوب والشبكة (مثل وحدات التحكم، ومراكز التشغيل) بأسلوب يتناسب مع مراقبة النفاذ إلى المرفق بحد ذاته.
- يجب حفظ سجل بالنفاذ إلى جميع هذه الحالات المراقبة.
- يجب تجفير وسائط خزن المعلومات البالغة الأهمية أو إيوائها في مناطق مقفلة يكون النفاذ إليها مقيداً.
- ينبغي عدم الكشف عن عنوان مادي لنظام بالغ الأهمية لمن لا يحتاجون إلى معرفته.

ويمكن تعزيز مراقبة المناطق الداخلية لمبنى ما عن طريق فصل الأدوار والمسؤوليات. فمثلاً، لا يحتاج الموظفون الإداريون للنفاذ إلى الغرف التي تضم أجهزة حاسوب المنظمة. وبالمثل، لا يحتاج المهندسون عموماً للنفاذ إلى غرفة مراقبة الوثائق. وينبغي أن يقيم الاستعراض ما إذا كان الفصل بين الوظائف القائم ملائماً. وإضافة إلى ذلك، يمكن استخدام مفاتيح الدخول المزدوج أو الأقفال التي تُفتح بتوليفة أرقام أو حروف إذا كانت درجة الخطورة تتطلب ذلك.

2.4.I خدمات المباني

تعتمد عمليات أي منظمة اعتماداً كبيراً على مدى تيسر الخدمات، من قبيل توفير المياه، والطاقة الكهربائية، والاتصالات، والتخلص من النفايات.

1.2.4.I المرافق (المياه والطاقة الكهربائية والاتصالات والتخلص من النفايات)

يتعذر على أي منظمة أن تعمل بفعالية، بل يستحيل عليها ذلك تماماً، من دون تيسر خدمات المياه والطاقة الكهربائية والاتصالات والتخلص من النفايات. وغالباً ما يتم التهوين من شأن الاعتماد على هذه الخدمات. وينبغي أن يقيم الاستعراض الاستجابات التي خططت لها المنظمة إزاء حالات انقطاع الخدمة. وفيما يتعلق بالخدمات الضرورية لاستمرار المؤسسة التجارية في أداء وظيفتها، من المهم اتخاذ الخطوات التالية:

- يجب أن تكون مصادر التزويد بالطاقة الكهربائية مزدوجة ومفصولة جغرافياً للحيلولة دون انقطاع التيار الكهربائي عرضياً.
- ينبغي تيسير الطاقة الكهربائية في حالات الطوارئ لإفساح المال أمام استمرار التشغيل لفترة أطول من متوسط مدة حالات انقطاع الكهرباء. ومن الضروري أن تكون قدرات توليد الطاقة الكهربائية متيسرة من أجل وزعها قبل استنفاذ إمدادات الطوارئ. (يمكن امتلاك مولدات متنقلة للطاقة الكهربائية أو التعاقد بشأن الحصول عليها.)
- لا بد من تيسير ما يكفي من مخزون المياه في الموقع (أو خدمات التزود بها) لدعم استمرار تشغيل مكونات المرفق الحساسة.
- يجب أن يكون للاتصالات الخارجية احتياطي بديل وفعال، أو ينبغي أن تكون قوية بما فيه الكفاية لتعمل في حالة حدوث أزمة، وكذلك الحال بالنسبة للاتصالات الداخلية. ومن الضروري أن تكون القدرات كافية لمناولة الحركة على مستوى الأزمة.

- ينبغي أن تؤدي مرافق دورة المياه ومجاري التصريف وظيفتها أثناء الأزمات، أو لا بد من وضع ترتيبات مؤقتة موضع التنفيذ (على أساس التعاقد على الأقل) من أجل تنشيط أدائها بسرعة.
- ينبغي توفير احتياطي لتكييف الهواء في غرف أجهزة الحاسوب وغيرها من المناطق التي تتطلب بيئات متحكم في درجة حرارتها للحيلولة دون عطب المكائن أو تلفها من جراء الحرارة المفرطة.
- ينبغي على وجه السرعة توفير حاويات مقفلة للتخلص من المعلومات الخاصة أو إتلافها حيثما تستخدم هذه المواد. وينبغي أن يتعقب الاستعراض مسار التخلص من هذه المواد لضمان حدوث الإغلاق.

ومن المهم بالنسبة للتقييم فحص توزيع هذه الخدمات داخل المباني. ويجب أن يقدر التقييم مدى تحمل المرفق الكلي لانقطاع الخدمة من مصدرها عند مقدم الخدمة وحتى مسارات توزيعها داخل البناية.

I.2.2.4 مرافق الطوارئ

لا بد أن يقيم الاستعراض مدى كفاية مرافق الطوارئ مثل الكشف عن الحرائق وإخمادها، والتزويد بالطاقة الكهربائية، وتكييف الهواء، والتهوية، وسائر أنظمة حماية البيئة اللازمة لاستمرار تشغيل الأنظمة البالغة الأهمية. ويجب أن تستجيب هذه الأنظمة بطرائق تتيح القيام بما يلي:

- إخلاء المباني من الناس؛
- حماية المعدات (على الأقل لفترة طويلة كافية لحين وصول شركات الإطفاء أو غيرها من الشركات)؛
- تمكين المرافق من الحفاظ على التكاملية الهيكلية؛
- حماية محتويات المبنى من البيئة الخارجية قدر المستطاع.

وأهمية مرافق الطوارئ بعد حدوث خرق للأمن تماثل أهميتها في حالة وقوع حوادث وكوارث طبيعية، مثلما يشير إلى ذلك البند السابق.

I.3.2.4 زيادة توفير النقل والحماية المادية لأهم المرافق

ينبغي جغرافياً نشر أهم مرافق أنظمة الحاسوب والاتصالات إلى أقصى مدى ممكن من دون التأثير أكثر من اللازم على تكاليف التشغيل، والأداء، والأمن. وبالإضافة إلى ذلك، يجب بصورة فائقة توفير وصلات تسيير أهم الاتصالات (مثل الدارات الهامة بين المكاتب، ووصلات التشوير) ونشرها جغرافياً داخل المرفق وخارجه كي يتسنى القيام عند الحاجة بإعادة تسيير الاتصالات فوراً عبر طرق تسيير احتياطية ومتنوعة من الناحية المادية. ويجب تصميم شبكات الاتصالات اللازمة لصيانة الخدمة بطريقة لا يؤدي فيها عطب أي نقطة واحدة إلى حدوث انقطاع للخدمة واسع النطاق أو انقطاع جسيم للخدمة.

I.3.4 التهديدات البيئية والجغرافية

من الضروري استعراض المواقع الحساسة لتحديد أية مخاطر يمكن أن تنشأ عن مكان وجود المواقع في مناطق يحتمل أن تشهد حصول كوارث طبيعية، وحوادث خطيرة (من قبيل حالات انسكاب المواد الكيميائية، انفجارات خطوط أنابيب الغاز)، حالات انقطاع الكهرباء، وما يتصل بذلك من مشاكل. وينبغي أيضاً أن يدرس الاستعراض الآثار المترتبة على عوامل بيئية بسيطة، مثل الحرارة اللافحة أو البرودة القارسة، والأضرار التي تسببها الأملاح والتلوث، وحالات الطقس القاسي.

وتشمل المسائل الجغرافية ردود فعل السكان المحليين، مثل الأعمال العدائية، ومدى استجابة خدمات الطوارئ المحلية، ومستوى السلامة الموفرة للموظفين في موقع المرفق وعلى الطريق إليه. ونظراً إلى أن أنشطة الإنسان ودوافعه تتغير عبر الزمن نتيجة للاضطرابات، أو المشاكل السياسية، أو وجهات النظر الدينية، أو غيرها من العوامل، فإنه ينبغي تكرار عمليات الاستعراض بصفة دورية وفقاً لجدول زمني محدد مسبقاً. وعلى الرغم من أنه غالباً ما يكون ترك المرافق الموجودة في المناطق التي تتفشى فيها هذه المخاطر أمراً غير عملي، فقد يكون من الملائم مضاعفة عدد الأنظمة والموارد المهمة التي تضمها المرافق المعرضة لمخاطر جسيمة أو نقل هذه الأنظمة والموارد إلى مواقع أخرى.

ولا بد من وضع خطط بشأن استمرار تشغيل المؤسسات التجارية والإغاثة من الكوارث بحيث تتطرق هذه الخطط إلى مسألة التصدي للأحداث الناشئة عن هذه التهديدات والمسائل. وينبغي أن تشمل الخطط إجراءات للتحكم، والمراقبة، والاتصالات، ومن الضروري اختبارها على أساس منتظم. ويجب أيضاً أن تشتمل خطط عمليات الإغاثة على أحكام وعقود قابلة للتنفيذ بسرعة استجابة للحالات المتعلقة بمواد خطرة (HAZMAT). كما ينبغي أن تبحث هذه الخطط أن الاستعادة الكاملة للبيئة الآمنة للمرفق يمكن أن تمنع النفاذ إليه بشكل عادي لفترة طويلة من الزمن. وقد تتطلب إعادة المعالجة المحتملة نقل المرفق إلى مرفق احتياطي أو توفير موظفين مدربين على التعامل مع المواد الخطرة ومجهزين بالمعدات اللازمة لذلك لتشغيل المرفق في أثناء هذه الفترة.

4.4.I إجراءات التشارك في الموقع

يشير تعبير التشارك في الموقع إلى حالة تسود عندما تكون هناك محطة تعود إلى مقدمي خدمات متعددين موجودين في نفس الموقع المادي. وإن ما يثير الاهتمام بوجه خاص فيما يتعلق بأغراض عمليات استعراض الأمن المادي هو أن توفير نفاذ من هذا القبيل يعني غالباً أن المتنافسين (عدة متنافسين أحياناً) يطلبون النفاذ إلى المكونات والمرافق المادية لمقدم الخدمات المضيف. ولا بد أن يشير الاستعراض إلى ما يلي:

- ينبغي عزل المعدات الحساسة بحواجز مادية؛ ومع ذلك، يخضع الموظفون المشتركون في الموقع لنفس متطلبات النفاذ التي يخضع لها مقدم الخدمة الملزم بذلك.
- توضع إجراءات لتوزيع المفاتيح، والمحاسبة، والتدقيق موضع التنفيذ. وتُنفذ عمليات معينة لضمان تيسير إمكانية مراقبة حالات تغيير الموظفين في جميع الشركات التي تشترك في الموقع.
- ينبغي ألا تُلفت المعدات والمرافق الحساسة النظر إليها. وأصبحت الطريقة التقليدية لوضع علامات واضحة على المعدات ومرافق النقل المهمة (المعروفة باسم "الختم باللون الأحمر"[6]) خطراً محتملاً في أي بيئة مفتوحة وينبغي تلافيها.

5.I عملية التطوير

1.5.I أساليب التمهيد والتركيب وتشخيص الأعطال

يجب مراعاة الاعتبارات التالية بشأن إجراءات الأمن المتعلقة بأساليب التمهيد والتركيب وتشخيص الأعطال.

وينبغي إتمام العديد من الجهود المتميزة المبذولة لتأمين التنفيذ من "منشأة جديدة" طوال عمر التنفيذ. ومن أجل التطرق إلى هذه المسائل، فإن من الضروري البدء بفهم التهديدات المحدقة بالتنفيذ. وترد إشارة إلى هذه التهديدات في المعيار ANSI T1.233-2004، *التشغيل، والإدارة، والصيانة، والتوريد – إطار أمن السطوح البينية لشبكة إدارة الاتصالات*، والوثيقة ISO/IEC 10181، *التوصيل البيني للأنظمة المفتوحة – الوثائق المتعلقة بمعايير أطر أمن الأنظمة المفتوحة*. وتعمل التوصيلية العامة بالأنظمة المفتوحة على توسيع نطاق تديدات من قبيل ما يلي:

- فيروسات التمهيد؛
- والنفاذ غير المصرح به؛
- والتنكر؛
- وتديد سلامة المعطيات؛
- وتديد السرية؛
- ورفض الخدمة (DoS)؛
- والإنكار.

---

6 ينبه الختم باللون الأحمر موظفي الدعم إلى أن الدارة تكتسي أهمية خاصة وأنه ينبغي الاهتمام بألا تُعرض للتشويش عرضاً.

2.5.I عملية تصحيح البرامج

يتعاقد مقدمو الخدمة مع الجهات البائعة التي تستحدث وتقدم على حد سواء تطبيقاً معيناً ومنصة يُركب عليها هذا التطبيق، أو برمجيات تطبيق حصراً. وفي الحالة الأخيرة، يركب مقدمو الخدمة البرمجيات على المنصة التي اشتروها سابقاً.

وتستحدث الجهات البائعة برمجيات تصحيح لتصويب أو تعديل برمجيات نظام التشغيل (OS) أو برمجيات التطبيق، أو كليهما، فيما بين حالات الطرح عموماً. وعقب اختبار برمجيات التصحيح كما يجب، تُطرح البرمجيات على مقدم الخدمة. وفي بعض الحالات، يمكن أن تقوم جهة بائعة لبرمجيات التطبيق بطرح برمجيات تصحيح في شكل "رزم"، ولربما اقترن ذلك بتعاقد على أساس منتظم معين. وليس من الغريب أن تتم عمليات طرح كل ستة أشهر.

وعموماً، لا ينبغي أن تؤثر برمجيات تصحيح نظام التشغيل (OS) على الأسلوب الذي يُشغل به تطبيق ما؛ ولكن الحال ليس كذلك دوماً. وبناء عليه، ينبغي على مقدم الخدمة، عندما تقوم جهة بائعة للمنصات بطرح برمجيات لتصحيح نظام التشغيل، أن يحصل على تأكيد من هذه الجهة بأن برمجيات التصحيح هذه (OS) لن تؤثر تأثيراً عكسياً على تشغيل التطبيق/تطبيق معين.

وفي الحالات التي تزود فيها جهة ما تبيع التطبيقات مقدم الخدمة بتطبيق ومنصة عتاديات على حد سواء، ولا تكون هذه الجهة البائعة هي الجهة الأصلية المصنعة للمعدات (OEM) التي صنعت المنصة، وتقوم الجهة المصنعة OEM للمنصة بطرح برمجيات لتعزيز أمن نظام التشغيل (OS)، فإنه ينبغي على الجهة البائعة للتطبيق ومقدم الخدمة على حد سواء أن يكونا على بينة من طرح برمجيات تعزيز الأمن وأن يضعا ترتيبات لاختبار برمجيات التعزيز هذه في الوقت المناسب، من أجل التثبت من أنها لن تؤثر تأثيراً عكسياً على تشغيل التطبيق.

ويجب إعطاء تطبيق برمجيات تعزيز الأمن أولوية فيما يتعلق باستعراضه من جانب الجهة التي باعته (وهو أمر يستغرق أسابيع بدلاً من شهور). وعلى هذا الأساس، ينبغي إرساء عملية روتينية في هذا الصدد من قبيل أنه عندما يبلغ مقدم خدمة ما جهة تبيع التطبيقات قلقه بخصوص برمجيات معينة لتعزيز الأمن، فإن على الجهة البائعة أن تعجل باتخاذ ما يلزم من إجراءات. وبالإضافة إلى ذلك، تكفل الجهة البائعة أن تركيب برمجيات التعزيز لا يفسد برمجيات تعزيز الأمن المركبة سابقاً.

وإذا كشف اختبار برمجيات تعزيز الأمن النقاب عن تأثير البرمجيات على تطبيق ما، لا بد من اتخاذ ما يلزم من إجراءات تصحيحية في الوقت المناسب لتشخيص المشكلة وصياغة خطط ترمي إلى تصحيح الحالة التي تسبب فشل التطبيق، وتطبيق برمجيات تعزيز الأمن فيما بعد.

وينبغي أخذ اعتبارات الأمن التالية في الحسبان عند تطبيق برمجيات تصحيح على برمجيات نظام التشغيل أو برمجيات التطبيق.

- يجب أن توفر الجهات البائعة للمعدات أو الجهات القائمة على تكامل الأنظمة للجهات القائمة على الإدارة كتيبات مرجعية وكتيبات تدريب في مجال الأمن تتضمن تفاصيل عن نظام التشغيل ووظائف وإجراءات تطبيق الأمن وإجراءات نفاذ المستعمل.
- ينبغي التحقق من أن برامج تعزيز أمن نظام التشغيل وغيرها من البرامج متفقة مع تطبيقات عنصر الشبكة ونظام الإدارة.
- برمجيات نظام التشغيل (OS): ينبغي ألا تطبق سوى برامج التصحيح التي تصادق عليها جهة أصلية مصنعة للمعدات (OEM) فيما يتعلق بتشغيل عناصر الشبكة أو نظام تشغيل منصة الإدارة.
- برمجيات تطبيق الإدارة: ينبغي ألا تطبق سوى برامج التصحيح التي تصادق عليها جهة أصلية تبيع تطبيقات الإدارة فيما يتعلق بتشغيل تطبيقات الإدارة.
- يجب توزيع برامج التصحيح شديدة التأثير في الوقت المناسب وينبغي عدم فرض قيود عليها من خلال إجراء عمليات دورية لنشرها.
- ينبغي تأمين جميع عمليات استقبال أو إرسال أية معطيات تتعلق بالبرمجيات أو التشكيلات عن طريق الاستيقان الشديد من مصدر المعطيات والحماية المنيعة لسلامة المعطيات. ومن الناحية المثالية، بالإمكان توفير الإرسال

والاستقبال على حد سواء بواسطة الإشارة الرقمية لمورد البرمجيات. وإضافة إلى ذلك، يمكن أن يختار مورد البرمجيات تجفير البرمجيات أو معطيات التشكيلة.

- ينبغي القيام في وقت التسليم بتقديم وصف عن الإجراء (الإجراءات) المتعلقة بالحصول على آخر نسخة من برامج تعزيز الأمن ودمجها في برمجيات النظام وبرمجيات التطبيق داخل كل عنصر.
- ينبغي القيام في وقت التسليم بتقديم وصف عن عملية اختبار كل برنامج من برامج تعزيز الأمن قبل المصادقة على طرحها على مقدم الخدمة.
- يجب القيام في وقت التسليم بتحديد مستوى التوافق الرجعي لحالات طرح برمجيات النظام وحالات طرح برامج تصحيح صيانة الأمن.
- يجب أن تتبع برمجيات النظام أو عملية ما برامج التصحيح وبرامج التحديث المطبقة. وينبغي أن تكون حالة هذه البرامج قابلة للتدقيق.

3.5.I أمن دورة حياة التطوير

يتوقف أمن ناتج أو خدمة معينة على كامل عملية دورة الحياة. والأمن مسألة مهمة أثناء تصميم ناتج ما من الناحية المفاهيمية وتبقى كذلك خلال تصميم أدق تفاصيل هذا الناتج، وتطويره، ونشره، وإخراجه من الخدمة. وفيما يتعلق بالنواتج أو الخدمات التي تتعامل مع معلومات حساسة، فقد يكون الأمن مطلوباً حتى بعد إخراج الناتج أو الخدمة من الخدمة الفعلية. والمراقبة والاختبارات الملائمة أثناء كامل عملية دورة الحياة ضرورية لتوفير مستويات أمن مقبولة.

1.3.5.I إدارة الموظفين

تعتبر جدارة الموظفين بالثقة مسألة جوهرية تتعلق بالأمن غالباً ما يتم إغفالها. وينبغي أن يكون جميع الموظفين المتاح لهم سبيل للنفاذ إلى تصميم البرمجيات، وتطويرها، واختبارها جديرين بالثقة.

- يجب أن يخضع جميع الموظفين، والمتعاقدين، والمتعاقدين من الباطن، والمستشارين، والعاملين المشاركين في تطوير واختبار مكونات برمجيات حساسة لفحص يتم بواسطته التأكد من ماضيهم.

2.3.5.I الوعي والتدريب في مجال الأمن

يجب أن يكون جميع الموظفين على علم بالسياسات العامة للأمن وبإجراءاته وبضرورة حماية أصول المعلومات. وغالباً ما يكون المشاركون من الموظفين هم الحلقة الأضعف في مجال الأمن. ويعضد الوعي والتدريب في مجال الأمن هذه الحلقة بشكل كبير. ويقلل الوعي عدد الإجراءات غير المصرح بها التي يحاول الموظفون القيام بها؛ ويزيد فعالية المراقبة التي تستهدف الحماية؛ ويساعد في منع تزوير موارد الحاسوب، وتبديدها، وإساءة استخدامها.

- ينبغي توعية الموظفين كافة وتدريبهم في مجال الأمن، بمن فيهم المتعاقدون والمتعاقدون من الباطن والمستشارون والعاملون.

3.3.5.I إدارة المخاطر

إدارة المخاطر جانب جوهري لتحقيق أمن المعلومات. وتُعرف هذه الإدارة على أنها تحديد الخسارة المقترنة "بحدث" معين، وتحليلها، والتحكم فيها، وتقليلها إلى أدنى حد. وتشمل الخطوات الأولية لتحديد المخاطر تشخيص التهديدات الفعلية، والتبعات المترتبة على تديد معين محسوس، واحتمال تواتر حصول التهديدات، وإمكانية تحقق التهديد المحسوس. ولا تنطوي إدارة المخاطر على إجراء تحليل للمخاطر بالتلازم مع تحليل فائدة تكلفة عمليات الحماية فحسب، وإنما تقوم بتنفيذ هذه الحماية واستعراضها وصيانتها أيضاً.

ويشخص تحليل المخاطر الأخطار المحدقة ويقدم مسوّغاً للتدابير المضادة عن طريق نسبة منافعها إلى تكاليفها. وتستخدم هذه المعلومات للتأثير على عملية اتخاذ القرارات في جميع مراحل دورة الحياة، بما في ذلك القرارات المتعلقة باختيار المواقع،

وتصميم المباني، والتشييد. وتُحدد الخسارة المتوقعة سنوياً (ALE) للبت فيما إذا كان يمكن منح ضمان. و(تكون الخسارة المتوقعة سنوياً (ALE) قبل تنفيذ الضمان) – (الخسارة المتوقعة سنوياً (ALE) بعد تنفيذه) = قيمة الضمان. وتجدر الإشارة إلى أن تنفيذ الضمان ينبغي أن يشمل التكاليف السنوية للتشغيل والصيانة.

- وينبغي إجراء تحليل مخاطر لكل ناتج أو خدمة جديدة. ولا بد أن يضم هذا التحليل تقريراً رسمياً يبين بإيجاز النهج المطبق في التحليل ونتائجه. ويجب أن يعين التقرير كحد أدنى جميع المعطيات التي يمكن النفاذ إليها والجهة المالكة لها (أي، شركة، مقدم خدمة إنترنت)، وأن يقدر قيمة المعطيات أو الخدمة المعرضة للخطر أو يحددها، ويحدد الآثار التي يحتمل أن يخلفها التهديد في الاتجاهين الصاعد والنازل على عناصر الشبكة (NE) أو أنظمة دعم تشغيل (OSS).

4.3.5.I المتطلبات

- ينبغي توثيق متطلبات الأمن خلال مرحلة جمع المتطلبات اللازمة لتطوير الناتج أو الخدمة.

5.3.5.I التصميم

- ينبغي التطرق إلى متطلبات الأمن في مرحلة التصميم، وعدم إضافتها بعد بدء التصميم.
- لا بد من إجراء استعراض لتصاميم الأمن لتعيين مواطن الخلل فيها التي تؤثر على الأمن.
- يجب أن توثق جميع نقاط النفاذ إلى النظام توثيقاً صحيحاً وأن تقدم الدعم لتحديد الهوية والاستيقان.
- لا ينبغي السماح بالحصول على سبل نفاذ سرية أو أبواب نفاذ سري للصيانة تنتهك سياسة الأمن.

6.3.5.I فصل المهام

يمكن أن تُوجد الوظائف التي لا تلحق الضرر بوسط مؤمن أوجه قصور تخل بالأمن عند استخدامها في أوساط غير مؤمنة. ومثال ذلك، تم تصميم مترجم فوري للنصوص لفحص الوثائق. ويمكن أن تستعمل وثيقة غير مؤمنة الوظائف الموجودة داخل هذا المترجم بطرق ضارة، من قبيل عمل النسخ وحذف الملفات.

- يجب أن يدعم النظام ثلاثة مستويات على الأقل من مستويات المستعمل، وهي: المستعمل والجهة القائمة على إدارة النظام/مشغل النظام والجهة القائمة على إدارة الأمن.
- يجب أن يكون لكل وظيفة المستوى الأدنى من الامتيازات اللازمة لتأدية وظيفة العمل.

7.3.5.I التنفيذ

- يجب تنظيف الموارد المعاد استخدامها من جميع المعلومات قبل استخدامها مجدداً (أي، الملفات والذاكرة والخزن المؤقت).
- يجب أن تتبع الجهات المطورة أفضل الممارسات بشأن البرمجة المؤمّنة (أي، إدارة الدوارئ كيما لا تتعرض لحالات فيض).
- يجب إجراء عمليات تدقيق دورية للأمن على أوساط التطوير، والاختبار، والدعم.
- ينبغي ألا تستخدم أوساط التطوير في أعمال تجارية غير تابعة لشركات.
- ينبغي ألا تستورد برمجيات القطاع العام، أو تستخدم، أو توزع من أجل استعمالها في أنظمة التطوير، أو الاختبار، أو الدعم ما لم تكن متيسرة بشفرة المصدر ويكون قد تم فحص هذه الشفرة للكشف عن أي شفرة ضارة.

8.3.5.I الوثائق

- يجب وضع علامات خاصة على الوثائق حسب الاقتضاء.
- ينبغي أن تصف وثائق المستعمل النهائي العناصر الوظيفية للأمن غير المتسمة بالشفافية للمستعمل، وتوضح عملها، وتقدم إرشادات بشأن استخدامها.

- يجب أن يشمل دليل الجهة القائمة على إدارة النظام ما يلي:
  - تحوطات بشأن الوظائف والامتيازات التي ينبغي التحكم فيها عند التشغيل بأسلوب مؤمّن؛
  - الاستفادة في التوثيق من وظائف التدقيق؛
  - وضع إجراءات لفحص سجلات التدقيق والحفاظ عليها؛
  - إنشاء هياكل مفصلة لسجلات التدقيق؛
  - وضع إجراءات لإيجاد سجل تدقيق وحذفه؛
  - وضع إجراءات لفحص مقدار الحيز الشاغر المتيسر لسجلات التدقيق.

9.3.5.I نظام التشغيل

ينبغي أن يكون بوسع نظام التشغيل (OS) توفير مراقبة فعالة لعتاديات والبرمجيات لتأمين الحماية اللازمة لقيمة المعطيات والموارد المُدارة. وفيما يتعلق بمعمارية الأمن المقترحة، فإن من المفترض أن يوفر نظام التشغيل مستوى الأمن اللازم لإدارة المعطيات والموارد. وقد يكون هذا الافتراض بحاجة إلى استعراض من أجل تلبية احتياجات معينة لمقدمي الخدمة. وفي حال عدم تلبية نظام التشغيل لهذه الاحتياجات، قد يكون من الضروري أن تُركب البرمجيات في نظام تشغيل آخر يوفر مستويات أعلى من الأمن.

- يجب أن تُركب في نظام التشغيل برامج مهمة لتعزيز الأمن.
- ينبغي تشكيل نظام التشغيل بطريقة مؤمّنة ويجب أن يُسلم بتشكيلة مقيدة من امتيازات النفاذ إلى الأمن. وتوجد عدة وثائق ومواقع على شبكة الويب تناقش أمن نظام التشغيل. وعلى الرغم من أن ضرب أمثلة على ذلك هو أمر لا يندرج ضمن نطاق هذه التوصية، فإن بعض الأمثلة تشمل المعايير الشائعة، الملامح العامة لحماية نظام التشغيل.[7] [8] [9]
- لن يمكّن سوى الحد الأدنى من الخدمات اللازمة للتشغيل بواسطة التغيب.

10.3.5.I هندسة البرمجيات

الأمن جزء لا يتجزأ من هندسة البرمجيات. ويجب استخدام تقنيات برمجة وبروتوكولات مؤمّنة من أجل استحداث ناتج مؤمّن. وبإمكان تقنيات البرمجة غير المؤمّنة أن تتحايل على أفضل بروتوكولات وآليات الأمن. فمثلاً، إذا كان هناك مبرمج معين لا يدير الدوارئ بصورة صحيحة، فقد يحصل فيض في الدوارئ ومنح المستعمل امتيازات أكثر مما ينبغي.

- يجب أن تتبع الجهات البائعة عمليات تطوير موثقة رسمياً، مثل نموذج نضج القدرات الذي وضعه معهد هندسة البرمجيات. ويجب تطبيق أفضل ممارسات البرمجة المؤمّنة في تصميم البرمجيات، وتطويرها، واختبارها، وتوزيعها.

11.3.5.I التيسر والأداء

التيسر والأداء مكملان لأي نظام مؤمن. ويمكن أن يتعرض أداء النظام للانحطاط إلى درجة يتعذر فيها استخدام النظام.

- ينبغي أن يعمل كل من التصميم، والتطوير، والتنفيذ على تقليل آثار هجمات رفض الخدمة (DoS) إلى أدنى حد.
- يجب أن يكفل كل من التصميم، والتطوير، والتنفيذ التيسر بمستوٍ عالٍ.
- ينبغي ألا يكون لمعمارية الشبكة والتنفيذ نقطة عجز واحدة.

---

7 المعايير الشائعة آخذة في طريقها لأن تصبح معياراً معترف به دولياً لتقييم الأمن رسمياً (http://www.commoncriteria.org/).

8 الملامح العامة لحماية نظام التشغيل الصادرة عن المحفل المعني بالأطر التقنية لتأمين المعلومات، http://www.iatf.net/protection_profiles/operating_systems.cfm

9 المعهد الوطني للمعايير والتكنولوجيا، مركز موارد أمن الحاسوب، http://csrc.nist.gov/.

12.3.5.I برمجيات النظام

ينبغي أن يكون للبرمجيات المستخدمة لتشغيل أنظمة الحاسوب وصيانتها (أنظمة التشغيل (OS)، والخدمات، وأنظمة الإدارة (MS)) القدرة على أن تخضع للتشكيل والصيانة على نحو مأمون. ويجب إجراء اختبارات للتثبت من تنفيذ خصائص المكونات والأمن تنفيذاً قوياً وتشكيلها بشكل صحيح.

- يجب توخي الأمن في تركيب وتشكيل برمجيات النظام ونواتج برمجيات التحويل، بما في ذلك تركيب برامج تعزيز الأمن. وينبغي تسليم البرمجيات بتشكيلة مقيدة من امتيازات النفاذ إلى الأمن.

13.3.5.I الإرسال

- ينبغي تيسير خيار تأمين إرسال المعطيات ليستعمل حسب تقدير مقدم الخدمة. وينبغي تيسر خيارات تأمين عمليات الإرسال من الزبون إلى وحدة خدمة الحاسوب، ومن النظام إلى النظام، على حد سواء.

14.3.5.I الخزن المؤمن

- ينبغي لمقدم الخدمة أن يوفر خيارات قابلة للتشكيل من أجل خزن المعطيات على نحو مؤمن. ويجب أن يكون مقدم الخدمة قادراً على تحديد الحالات التي تخزن على نحو مؤمن.

15.3.5.I تأمين البرمجيات

ينبغي التطرق إلى موضوع تأمين البرمجيات من منظورين، هما: اختبار خصائص الأمن واختبار احتمالات انتهاك سياسة الأمن.

- يجب فصل مهام مجموعات تطوير البرمجيات عن مهام مجموعات اختبارها.
- يجب توثيق خطة لاختبار الأمن، وإجراءات الاختبار، والنتائج.
- ينبغي اختبار جميع خصائص الأمن.
- يجب أن تشمل الاختبارات المحاولات الرامية إلى تحديد موضع انتهاكات السياسة العامة للأمن (أي، أوجه القصور من مثل مراقبة النفاذ).
- ينبغي إجراء تحقق، كجزء من الاختبار، لكي لا يوجد النظام أو التطبيق المطور حديثاً أوجه قصور في الهياكل، والشبكات العادية، والأنظمة القائمة.
- ينبغي إجراء تحقق من تقنيات البرمجة المؤمنة. وبالإمكان إجراؤه بواسطة عمليات استعراض الشفرات أو أدوات البرمجيات.
- ينبغي أن تُصحح جميع مواطن ضعف الأمن، أو تُزال، أو يُبطل مفعولها وأن يُختبر النظام مجدداً.

16.3.5.I إعداد الرزم وتسليمها

ينبغي استخدام نظام لإدارة تشكيلة البرمجيات طوال دورة حياة الناتج بحيث تتسنى مواصلة مراقبة التغيرات المدخلة على شفرة المصدر والوثائق.

- ينبغي ألا تضطلع الجهات المطورة بالمسؤولية عن استيفاء نظام إدارة تشكيلة البرمجيات.
- يجب ألا يتاح للجهات المطورة سبيل للنفاذ إلى أنظمة الإنتاج إلا بموجب أحكام طوارئ مراقبة تم اعتمادها وتسجيلها.
- ينبغي ألا تُضاف إلى خط أساس المصدر القابل للتسليم سوى الشفرات المصرح با والتعديلات المصرح بإدخالها عليها.
- يجب توثيق واستعراض جميع التغييرات.
- ينبغي إيجاد أدوات أو إجراءات معينة لاستحداث صيغة جديدة للنظام من شفرة المصدر.

- ينبغي إيجاد أدوات أو إجراءات معينة لحماية شفرة المصدر من أي تعديلات غير مصرح بإدخالها.
- ينبغي إيجاد أدوات أو إجراءات معينة للتحقق من الصيغ ومستويات وحدات مصدر المكونات التي استخدمت.
- من الضروري أن يضم الناتج آليات تكامل كيما يتسنى بموجبها التحقق من أن البرمجيات المركبة متفقة مع البرمجيات المسلمة (أي، لم تُدخل عليها أية تعديلات غير مصرح بها).
- ينبغي في حال تيسر أداة فرز آلية، إكمال فرز أوجه القصور التي تشوب برمجيات نظام التشغيل أو برمجيات التطبيق بعد إجراء عمليات تحسين أو إدخال تغييرات كبيرة أخرى على هذه البرمجيات.
- ينبغي توفير إصلاحات أو "تقويمات" لأوجه القصور المخلة بالأمن في الوقت المناسب وبما يتناسب مع التهديد.
- ينبغي وجود قاعدة معطيات رئيسية تضم نسخاً من جميع البرمجيات المسلمة. ويجب أن تحمل البرمجيات رقم الطرح ومواصفات أنظمة التشغيل والعتاديات المناسبة.

17.3.5.I التركيب والتشكيل والتشغيل المؤمن

- يجب تحديد معلمات مؤمنة لتشكيل البرمجيات.
- يجب تحديد وتوثيق إجراءات مؤمنة لتشغيل البرمجيات.
- يجب أداء أي دعم عن بعد إلى البرمجيات بطريقة مؤمنة.
- يجب أن تسلم جميع معرفات هوية المستعمل المحددة بالتغيب في حالة خمول تقتضي اتخاذ إجراء صريح من قِبل الجهة القائمة على الإدارة/الجهة المركبة للبرمجيات كي يمكن استعمالها.
- يجب أن تكون جميع عمليات التركيب مؤمنة وينبغي ألا تعتمد على علاقات الثقة (أي، تقاسم الأقراص).

التذييل II

مبادئ توجيهية بشأن الإطار والتصميم

1.II الإطار والنموذج

يقصد بتأمين جانب معين في سياق هذه التوصية حمايته من النفاذ إليه، أو استخدامه، أو تنشيطه من دون تخويل (مثل أجهزة الحاسوب، أو الشبكات، أو المعطيات، أو غيرها من الموارد). وفقدان المعطيات، ورفض الخدمة (DoS)، وسرقة الخدمات ما هي إلا بعض نتائج الأحداث ذات الصلة بالأمن. والجهات القائمة على إدارة النظام والشبكة بحاجة إلى حماية الأنظمة والعناصر المكونة لها من المستعملين الداخليين والخارجيين ومن الجهات المهاجمة للأنظمة. وعلى الرغم من تعدد أوجه الأمن (عمليات التجسير، والأمن المادي، والاتصالات، والمعالجة، والموظفين)، فإن الشاغل المثار هنا هو مشاكل الأمن الناجمة عن جوانب الضعف المتأصلة في التشكيلات والتكنولوجيات المستخدمة بشكل شائع. ويتألف أي تديد من فضح عناصر المعلومات، واستخدامها دون تصريح، وإدخال تعديلات عليها، ورفض الخدمة، ولكنه لا يقتصر على ذلك. ويدرج الجدول 1.II بعض التهديدات المحدقة بالأمن.

الجدول M.3016.1/1.II - التهديدات

فئة التهديد (ملاحظة)	أمثلة على التهديد
نفاذ غير مصرح به	النفاذ إلى أنظمة الحاسوب من دون تصريح نفاذ إلى النظام لشن هجمات سرقة الخدمة
تنكر	تكرار الدورة النفاذ غير المصرح به إلى الدورة متطفل على طرفين في منتصف الهجمة
تديدات لتكاملية النظام	معالجة غير مصرح بها لملفات تشكيلة النظام معالجة غير مصرح بها لمعطيات النظام
تديدات لتكاملية الاتصالات	معالجة غير مصرح بها للمعطيات قيد العبور
تديدات للسرية	التنصت الخفي تسجيل معطيات الدورة وكشفها انتهاكات الخصوصية
رفض الخدمة	غمر SYN بروتوكول التحكم في الإرسال (TCP) بالتحقيق المتزامن للرزم فيه هجمات برزم مشوهة توزيع رفض الخدمة (DoS)

ملاحظة - مستنبطة من المعيار T1.233-1993 (R 1999) الصادرة عن المعهد الأمريكي المعني بالمعايير الوطنية (ANSI)، *التشغيل، والإدارة، والصيانة، والتزويد - إطار أمن السطوح البينية لشبكة إدارة الاتصالات*، والوثيقة 2-7498:1989 الصادرة عن المنظمة الدولية للتوحيد القياسي (ISO)، *أنظمة معالجة المعلومات – التوصيل البيني الرابط للأنظمة المفتوحة - النموذج المرجعي الأساسي – الجزء 2: معمارية الأمن.*

ويمكن تقليل هذه التهديدات إلى أدنى حد أو تخفيفها داخل نظام ما من أنظمة الشبكة أو منصة معينة لعناصر الشبكة أو تطبيق ما عن طريق إدراج خدمات الأمن (على غرار ما هو محدد في الوثيقة 2-7498:1998 الصادرة عن المنظمة الدولية للتوحيد القياسي (ISO)، *أنظمة معالجة المعلومات - التوصيل البيني فيما بين الأنظمة المفتوحة - النموذج المرجعي الأساسي - الجزء 2: معمارية الأمن*)، وذلك لإنفاذ ما يلي:

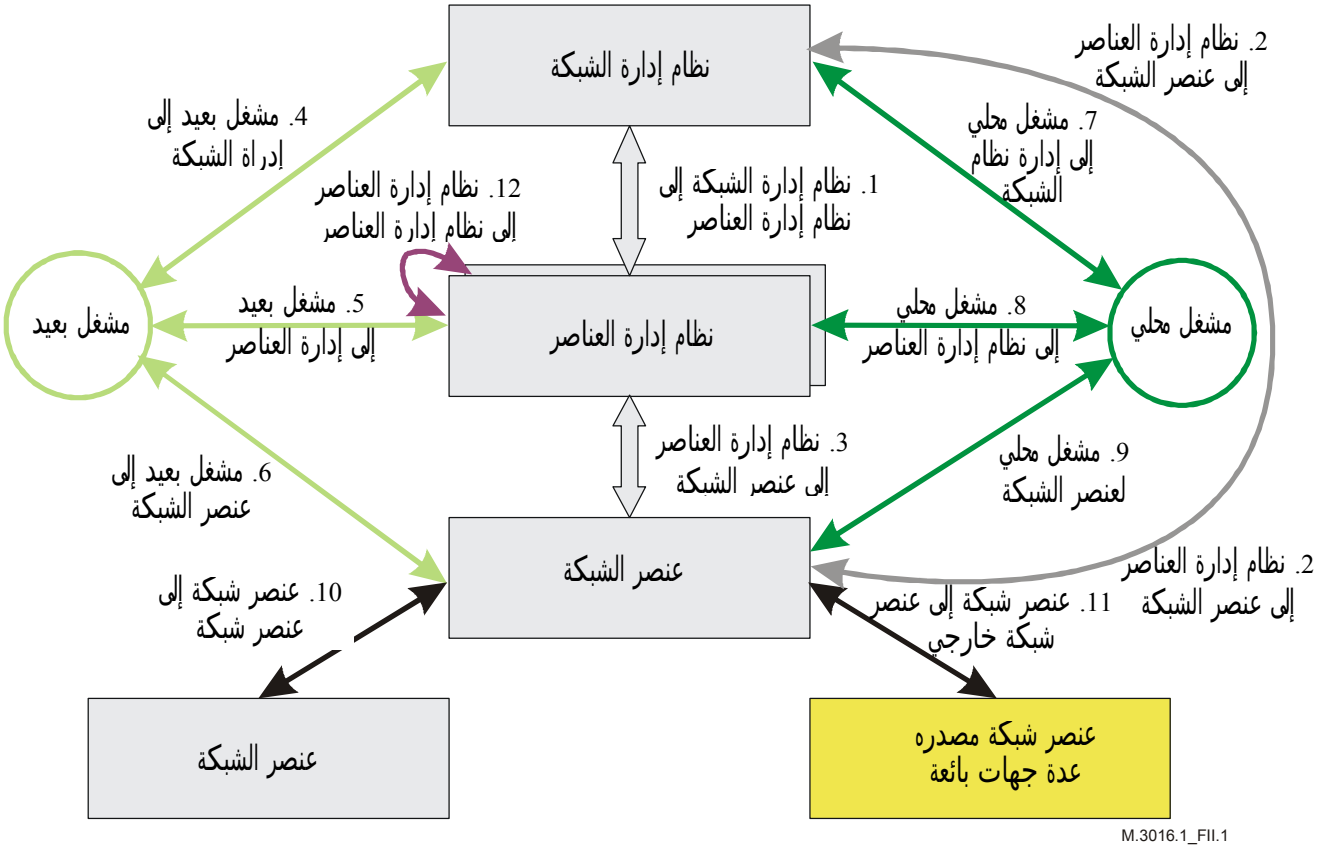
- تحديد الهوية **والاستيفان**؛
- التخويل ومستوي **مراقبة النفاذ**؛
- تكاملية المعطيات؛
- الحفاظ على الخصوصية والسرية؛
- عدم الإنكار.

وتتناول هذه التوصية أمن مستوي الإدارة، أي بعبارة أخرى، سمات الأمن من أجل ضمان التمكن من إدارة الشبكة والتحكم فيها بأسلوب مؤمن. ومع ذلك، يمكن أن توجد أوجه قصور معينة، حتى بعد الأخذ بالنصائح الواردة في هذه التوصية. وترد أدناه مخاطر من بين تلك القادرة على تعريض مستوي الإدارة للخطر، وهي:

- قيام المستعملين المصرح لهم أو الجهات المهاجمة باتخاذ إجراءات غير مناسبة. ويمكن أن تكون هذه الإجراءات متخذة عن سوء قصد أو عن غير قصد.
- تجسير أمن مستوي المراقبة (مثل بروتوكولات التشوير، والتسيير، والتسمية، والاكتشاف).
- آثار أوجه الضعف الكائنة في بروتوكولات معينة.
- برمجيات التخريب (من قبيل الفيروسات، أو برامج حصان طروادة للتلصص، أو برامج وورم (WORM) التخريبية، أو غيرها من الشفرات المطمورة في النظام). وحالما تنجح برمجيات التخريب في إلحاق الضرر بأي عنصر من عناصر الشبكة/نظام الإدارة، فبإمكانها أن تستخدم الوصلات التي تستعملها الشبكة في الاتصال المؤمن، وذلك لإرسال الهجمات إلى مكونات أخرى لعناصر الشبكة/نظام الإدارة. وقد تستمر هذه الهجمات حتى يكتشفها القائمون على إدارة الشبكة ويتخذون إجراءات للقضاء عليها.

وتتعلق هذه التوصية بأمن حركة الإدارة، وخاصة عندما تجتاز شبكات تخالط حركة المستعملين النهائيين. ويوضح الشكل 1.II نموذجاً مرجعياً يستخدم في تحديد حلول لأمن إدارة الشبكة. ويستعمل هذا النموذج في تفحص مسارات الاتصالات المنطقية داخل الشبكة ككل وفي تحديد كم البروتوكولات المستخدمة في الاتصالات عبر كل مسار. وباستعمال هذا النموذج، يمكن تفحص التهديدات وأوجه الضعف في كل مسار، وتطبيق آليات أمن ملائمة في هذا الصدد.

وعناصر الشبكة (NE) التي مصدرها عدة جهات بائعة مبينة في أسفل النموذج الوارد في الشكل 1.II. أما أنظمة إدارة العناصر (EMS)، التي تؤدي وظائف معينة في مجال الإدارة لعنصر شبكة معين، فهي موضحة فوق خانة عنصر الشبكة. ويرد نظام إدارة الشبكة (NMS) تحديداً في أعلى النموذج. ويدير هذا النظام (NMS) عنصر الشبكة ونظام إدارة العناصر (EMS) إدارة شاملة، ويضم التطبيقات المتعلقة تحديداً بإدارة الخدمة وتطبيقات إدارة الأعمال التجارية، من قبيل أنظمة التشكيل والفوترة. ويبين النموذج أيضاً مشغلي الشبكة عن بعد ومشغليها المحليين ويوضح مسارات الاتصال مع جميع عناصر النظام الأخرى.



الشكل M.3016.1/1.II - النموذج المرجعي لأمن إدارة الشبكة

وقد يكون النموذج المرجعي للأمن (الشكل 1.II) مفيداً أيضاً في إقامة علاقة متبادلة بين سطوح بينية محددة لشبكة إدارة الاتصالات (TMN) مع نموذج الأمن. ويرد تعريف شبكة إدارة الاتصالات (TMN) في التوصية ITU-T M.3010، *المبادئ المتعلقة بشبكة إدارة الاتصالات*. وتُعرف هذه الشبكة (TMN) على أنا معمارية إدارة تشمل التخطيط في مجال معدات الاتصالات وشبكاتا وخدماتا، وتوريد هذه المعدات والشبكات والخدمات، وتركيبها، وصيانتها، وتشغيلها، وإدارتا.

2.II مبادئ توجيهية بشأن التصميم

يقدم الجدول 2.II أهداف المبادئ التوجيهية المتعلقة بالتصميم التي تسعى إلى تلبية المتطلبات الواردة في البند 6 للتخفيف من وطأة التهديدات المقترحة في الجدول 1.II.

الجدول M.3016.1/2.II - المبادئ التوجيهية للتصميم قيد البحث

المبادئ التوجيهية	الوصف
العزل	عزل حركة الإدارة عن حركة المستعملين
سياسات الأمن الفعالة	يجب أن تفسح المتطلبات والمعماريات التي تقدم الدعم للتصميم المجال أمام وضع سياسات قابلة للتحديد، ومرنة، وقابلة للإنفاذ، والتدقيق، والتحقق، وموثوقة، وقابلة للاستخدام.
الاستيقان الشديد، والتخويل، والمحاسبة (AAA)	محاسبة موثوقة للدورات المصرح با كما ينبغي بين الكيانات التي تم استيقانا.
تحقيق أعلى منفعة بالنسبة إلى التكاليف	تعزيز الأمن من خلال تطبيق آليات أمن قياسية، وتيسير عمليات التنفيذ على نطاق واسع، ونشرها على نطاق واسع، كيما يتسنى فسح المجال أمام تقييم آليات الأمن من خلال اللجوء إلى سجل الأحداث الماضية.

المبادئ التوجيهية	الوصف
مسار التحسين	بحث الخطوات المقبلة الرامية إلى تعزيز وتحسين أمن إدارة الشبكة للاستمرار في تلبية بعض المتطلبات اللازمة للتكنولوجيات والآليات الآخذة في التطور أو تلبية متطلبات الأمن المحددة حديثاً.
جدوى الجانب التقني	يجب تلبية المتطلبات اللازمة بالنواتج، و/أو الحلول، و/أو التكنولوجيات المتيسرة في الوقت الحاضر.
الصيانة عن بعد	ينبغي أن تكون المتطلبات متفقة مع الإجراءات القياسية لتشغيل إدارة الشبكة كما يجب.
المعايير المفتوحة	الاستفادة من الأفكار والمفاهيم الموحدة قياسياً فعلياً أو التي يجري توحيدها قياسياً من جانب المنظمات المعنية بوضع المعايير (مثل أمن بروتوكول الإنترنت (IPsec)، الإشارات الرقمية). ويجب دراسة جميع جوانب المعايير المفتوحة، بما فيها المتعلقة بالأنظمة والبروتوكولات، والأساليب والخوارزميات والخيارات وأحجام المفاتيح والتشفير.

التذييل III

معاني المصطلحات المستخدمة في سلسلة التوصيات M.3016.x

ترد المصطلحات التالية **بالبنط العريض** عندما تستخدم في عبارة تتضمن متطلباً معيناً.

1.III مراقبة النفاذ: منع أي استخدام غير مصرح به لمورد بما في ذلك منع استخدام المورد على نحو غير مصرح به.[10]

2.III وحدة خدمة مراقبة النفاذ (ACS): عنصر مساعد من عناصر الشبكة يُنشر لإنفاذ واستيقان النفاذ إلى أحد أنظمة الإدارة على أساس **كلمات سر معقدة**، وذلك في الحالات التي يعجز فيها عنصر الشبكة عن أداء هذه المهمة الوظيفية مباشرة.

3.III الجهة القائمة على إدارة التطبيق: عبارة عن دور مسؤول عن تفعيل تطبيق معين لعنصر الشبكة/نظام الإدارة، ورعايته، واستخدامه بشكل صحيح. وتشمل مهام إدارة التطبيقات تحسين برمجيات التطبيق.[11]

4.III الجهة القائمة على إدارة أمن التطبيق: عبارة عن دور مسؤول عن تنشيط خصائص أمن طبقة التطبيق لعنصر الشبكة/نظام الإدارة، ورعاية هذه الخصائص، واستخدامها بشكل صحيح. وهي تمثل أعلى مستوى لسلطة توفير الأمن لحالة تطبيق لعنصر الشبكة/نظام الإدارة. وقد تتضمن المهام ما يلي:

- تحديد وتخصيص امتيازات جديدة للمستعملين والمجموعات على مستوى التطبيق؛
- الاحتفاظ بسجل بجميع طلبات الحصول على معرفات هوية تسجيل الدخول إلى التطبيق؛
- إضافة المستعملين وحذفهم على مستوى التطبيق؛
- مراقبة جميع سجلات أمن التطبيق؛
- تحديد تشكيلة تسجيلات وإنذارات أمن التطبيق.
- إدارة عمليات تسجيل أمن التطبيق؛
- إنهاء دورة مستعمل التطبيق.

5.III الاستيقان: هو فعل التحقق من هوية مزعومة.

---

[10] مأخوذ من البند 1.3 الوارد في المعيار T1.233-1993 (R 1999) الصادرة عن المعهد الأمريكي المعني بالمعايير الوطنية (ANSI)، *التشغيل، والإدارة، والصيانة، والتوريد – إطار أمن السطوح البينية لشبكة إدارة الاتصالات*.

[11] قد تكون هذه المهمة وظيفة من وظائف **الجهة القائمة على إدارة النظام**، إذا كانت سلطة **المستعمل الثانوي** ضرورية لإتمام هذه المهمة. ويمكن استحداث عمليات للتحكم في النفاذ إلى حساب **المستعمل الثانوي**.

6.III كلمات السر المعقدة: توصف كلمة السر بأنها "معقدة" عندما تكون مكونة من توليفة معينة من الحروف الأبجدية والأرقام والرموز الخاصة، والتي ينبغي أن يكون تخمينها بواسطة وسيلة اجتماعية هندسية أو مؤتمتة أمراً صعباً أو غير محتمل الحدوث.

7.III مستوي التحكم: يؤدي مستوي التحكم وظيفتي التحكم في النداء والتحكم في توصيله. ويقوم هذا **المستوي** بواسطة التشوير بإنشاء التوصيلات وإطلاقها، وقد يستعيد التوصيل في حال فشله.[12]

8.III أهم إجراءات إدارة الأمن: الجهة القائمة على إدارة أمن النظام مسؤولة عن اتخاذ أهم إجراءات إدارة الأمن التي تفسح المجال أمام تفعيل خصائص أمن نظام معين (عنصر الشبكة/نظام الإدارة)، ورعايتها، واستخدامها بصورة صحيحة. وتشتمل **أهم إجراءات إدارة الأمن**، على ما يلي دون أن تقتصر عليه:

- تحديد امتيازات المستعمل وتخصيصها؛
- إضافة معرفات هوية المستعملين وحذفها؛
- تعطيل معرفات هوية مستعملين معينين عن العمل بوصفها معرفات هوية مستخدمة في تسجيل الدخول؛
- تشكيل كلمات السر المستخدمة في تسجيل الدخول وإعادة تحديدها؛
- تشكيل مفاتيح التجفير وتغييرها؛
- تحديد عتبة تقادم النظام بالنسبة لكلمات السر المستخدمة في تسجيل الدخول إليه؛
- تحديد حد الدخول إلى النظام على أساس عدد محاولات تسجيل الدخول الفاشلة لكل معرف من معرفات الهوية المستخدمة في تسجيل الدخول؛
- إلغاء إغلاق النظام، أو تغيير قيمة مؤقت إغلاقه؛
- تحديد قيمة مؤقت خمول النظام؛
- تحديد تشكيلة التسجيل والإنذار بشأن أمن النظام؛
- إدارة عمليات التسجيل المتعلقة بالأمن؛
- تحسين برمجيات الأمن؛
- إناء أية دورة من دورات المستعمل أو النظام.

9.III تعطيل/معطل: يدل التعبير عندما يشير إلى معرف هوية مستعمل إلى حالة يتعذر فيها استخدام هذا المعرف في تسجيل الدخول حتى يتم تمكينه بموجب إجراء معين يتخذه معرف هوية مستعمل آخر يتمتع بامتيازات التخويل الملائمة (مثل **الجهة القائمة على إدارة أمن النظام أو الجهة القائمة على إدارة أمن التطبيق**).

10.III نظام إدارة العناصر (EMS): هو النظام الذي يؤدي وظيفة نظام التشغيل في طبقة إدارة العناصر.

11.III قوة المفتاح: عبارة عن خوارزميات تحمل رموزاً سرية مختلفة بدرجات أمن تتباين بتباين مدى صعوبة خرقها. وتعتبر الخوارزمية الحاملة للرمز السري قوية إذا كان من المتعذر خرقها من الناحية الحسابية، أي بعبارة أخرى، أنها تتسم بالتعقيد بما فيه الكفاية بحيث يتعذر خرقها في غضون فترة زمنية "معقولة" بالموارد المتيسرة لذلك سواء في الوقت الحالي أم في المستقبل القريب. وغالباً ما يُقاس التعقيد من الناحية الحسابية على أساس مدى تعقيد المعالجة، أو الفترة الزمنية والمجال الشاغر المتيسر في الذاكرة اللازم لتنفيذ هجمة ما. وعلى الرغم من أن مدى التعقيد الذي تتسم به هجمة ما يبقى ثابتاً بالنسبة لخوارزمية معينة وحجم مفتاح معين، فإن القدرة الحسابية تزداد بثبات. وتُصمم أنظمة الترميز الجيدة بطريقة يتعذر خرقها باستخدام القدرة الحسابية التي يُتوقع أن تتطور في غضون العديد من السنوات المقبلة. ونتيجة للتطور السريع الطارئ على التكنولوجيات والطرائق الجديدة لتحليل الرموز، فإن حجم المفتاح الصحيح المستعمل في تطبيق معين يتغير باستمرار.

---

[12] التوصيتان G.8080/Y.1304 الصادرتان عن قطاع تقييس الاتصالات (ITU-T)، *معمارية الشبكة البصرية المبدلة أوتوماتياً (ASON)*، نوفمبر 2001 (متيسرتان في مكتبة الاتحاد (ITU) لبيع الكتب المطبوعة في نسخ إلكترونية).

12.III إغلاق/مغلق: يدل التعبير عندما يشير إلى معرف هوية مستعمل إلى حالة يتعذر فيها استخدام هذا المعرف في تسجيل الدخول حتى تُلغى حالة الإغلاق باتخاذ إجراء أو أكثر من الإجراءات المناسبة. وتشتمل هذه الإجراءات على ما يلي دون أن تقتصر عليه:

- إعادة تحديد مؤقتة بعد انقضاء الفترة الزمنية لعتبة ما (بعد 60 دقيقة مثلاً)؛
- أو إعادة تحديد مؤقتة بعد النجاح في إتمام عملية التحديد المعينة مسبقاً (مثلاً، بعد إجابة الجهة المالكة على مجموعة من الأسئلة المطبوعة إجابة صحيحة)؛
- أو إعادة التحديد من خلال إجراء معين يتخذه معرف هوية مستعمل آخر يتمتع بامتيازات الترخيص المطلوبة (مثل **الجهة القائمة على إدارة أمن النظام** أو **الجهة القائمة على إدارة أمن التطبيق**).

13.III إجراءات الإدارة: هي عبارة عن إجراءات تتخذها **الجهة القائمة على إدارة النظام** أو تُتخذ بالنيابة عنها.

14.III اتصالات بالإدارة: هو أي اتصال يتعلق **بإجراء إداري**.

15.III مستوي الإدارة: يؤدي **مستوي الإدارة** وظائف إدارة **مستوي النفل، ومستوي المراقبة**، والنظام ككل. ويتولى أيضاً التنسيق بين جميع المستويات. وتؤدي على **مستوي الإدارة**[13] المجالات الوظيفية المتعلقة بالأداء، والعطب، والتشكيل، والمحاسبة، وإدارة الأمن، وهي مجالات محددة في التوصية ITU-T M.3010، *المبادئ المتعلقة بشبكة إدارة الاتصالات*.

16.III عنصر الشبكة: انظر التوصية ITU-T M.3010.

17.III نظام إدارة الشبكة (NMS): هو النظام الذي يؤدي وظيفة نظام التشغيل في طبقة إدارة الشبكة.

18.III عنصر الشبكة/نظام الإدارة (NE/MS): تعبير إجمالي يستخدم لوصف كامل العناصر الموجودة داخل شبكة الاتصالات بما فيها عناصر الشبكة (NE) وأنظمة إدارة العناصر (EMS) وأنظمة إدارة الشبكة (NMS) وأنظمة دعم التشغيل (OSS).

19.III الاستيقان المحمي: يشمل **الاستيقان الشديد**، أو **الاستيقان المؤلف من عاملين**، أو **استيقان المسير الموثوق**، أو استيقان الرموز السرية التي يحملها طرف ثالث (مثل Kerberos)، أو استيقان كلمات السر المستعملة لمرة واحدة.

20.III الدورة: هي سلسلة من العمليات التي تتم، إما من الآلة إلى الآلة أو من الإنسان إلى الآلة، وتكون مقترنة بعملية فريدة من نوعها أو معرف هوية وحيد يستخدمه المستعمل.

21.III الاستيقان المكثف: هو استيقان يعتمد على استخدام تقنيات الترميز السري (من قبيل تجفير المفاتيح العامة، وتجفير المفاتيح المتناظر، والإشارات الرقمية، وتقنيات التضليل الرقمية). وينبغي أن يشمل **الاستيقان الشديد** الاستيقان باتجاهين الذي يمكن استخدامه لصد الهجمات الفعالة.

22.III التجفير المكثف: هو عبارة عن هجمة بقوة عاتية تحدث عندما تحاول الجهة التي تشنها تجريب جميع ما يمكنها تجريبه من توليفات المفاتيح باستخدام موارد الحاسبة المتيسرة للكشف عن رسالة مجفرة. وبهذه الطريقة، يمكن عموماً إيجاد المفتاح الصحيح بعد تجريب نصف العدد الكلي للتوليفات المحتملة للمفاتيح. والوقت المتوقع استغراقه في تجريب نصف عدد هذه التوليفات هو مقياس لمدى كثافة التجفير. وبناء على ذلك، تستخدم آليات **التجفير المكثف** في أي وقت محدد خوارزميات ومفاتيح تجعل أي جهة مهاجمة تستغرق أكثر من سنتين لخرق التكنولوجيا الحالية.

---

[13] يرد وصف لمعمارية شبكة إدارة الاتصالات (TMN) في التوصية ITU-T M.3010، المبادئ المتعلقة بشبكة إدارة الاتصالات، وتقدم توصيات السلسلة M تفاصيل إضافية عن مستوى الإدارة. التوصيتان Y.1304/G.8080 الصادرتان عن قطاع تقييس الاتصالات (ITU-T)، معمارية الشبكة البصرية المبدلة أوتوماتياً (ASON)، نوفمبر 2001 (متيسرتان في مكتبة الاتحاد لبيع الكتب المطبوعة في نسخ إلكترونية).

III.23 الجهة القائمة على إدارة النظام: عبارة عن دور مسؤول على مستوى نظام التشغيل عن العمليات والإجراءات المتصلة بتركيب منصة التشغيل وتشغيلها وصيانتها، وتركيب البرمجيات على المنصة، ومراقبة سلطة **المستعمل الثانوي**. وقد تشمل المهام ما يلي:

- تنسيق تركيب منصة جديدة؛
- تحديد وتخصيص امتيازات جديدة للمستعملين والمجموعات على مستوى نظام التشغيل (OS)؛
- حفظ سجل بجميع طلبات الحصول على معرفات الهوية المستعملة في تسجيل الدخول إلى نظام التشغيل؛
- إضافة المستعملين وحذفهم على مستوى نظام التشغيل؛
- تعطيل معرفات هوية معينة عن العمل بوصفها معرفات هوية مستخدمة في تسجيل الدخول (bin,sys,uucp)؛
- تركيب برامج تحسين وبرامج تصحيح في نظام التشغيل؛
- تركيب برمجيات تطبيق وقواعد معطيات في نظام التشغيل؛
- مراقبة جميع سجلات النظام؛
- الحفاظ على سبيل النفاذ بواسطة كلمة السر التي يستخدمها **المستعمل الثانوي** ومراقبة هذا السبيل والتغيرات في كلمة السر؛
- مراقبة النفاذ إلى حساب **المستعمل الثانوي**، لإفساح المجال أمام النفاذ إليه كما ينبغي حسبما تقتضيه المهمة؛
- إدارة عمليات التسجيل المتعلقة بالنظام؛
- منح تخويلات إدارية لأشخاص معينين يضطلعون بأدوار أخرى، بما في ذلك **الجهات القائمة على إدارة التطبيق**؛
- إنهاء أية دورة مستعمل أو نظام.

III.24 الجهة القائمة على إدارة أمن النظام: عبارة عن دور مسؤول عن تفعيل خصائص أمن النظام لعنصر الشبكة/نظام الإدارة، وصيانة هذه الخصائص، واستخدامها بشكل صحيح. وهي تمثل أقصى مستوى لسلطة أمن حالة النظام/التطبيق. وقد تتضمن المهام ما يلي:

- تحديد وتخصيص امتيازات جديدة للمستعملين والمجموعات على مستوى نظام التشغيل؛
- حفظ سجل بجميع طلبات الحصول على معرفات هوية لتسجيل الدخول إلى نظام التشغيل؛
- إضافة المستعملين وحذفهم على مستوى نظام التشغيل؛
- تعطيل معرفات هوية معينة عن العمل بوصفها معرفات هوية مستخدمة في الدخول (bin,sys,uucp)؛
- مراقبة جميع سجلات أمن النظام؛
- تشكيل مفاتيح تحمل رموزاً سرية وتغييرها؛
- تحديد عتبة تقادم النظام بالنسبة لكلمات السر المستخدمة في الدخول إليه؛
- تحديد حد الدخول إلى النظام على أساس عدد محاولات الدخول الفاشلة لكل معرف من معرفات الهوية المستخدمة في تسجيل الدخول؛
- إلغاء إغلاق النظام، أو تغيير قيمة مؤقت إغلاقه؛
- تحديد قيمة مؤقت خمول النظام؛
- تحديد تشكيلة التسجيل والإنذار بشأن النظام؛
- إدارة عمليات التسجيل المتعلقة بأمن النظام؛
- منح تخويلات أمنية لأشخاص معينين يضطلعون بأدوار أخرى، بما في ذلك **الجهات القائمة على إدارة أمن التطبيق**؛
- إنهاء أية دورة للمستعمل أو للنظام.

25.III مستوي النقل: يوفر **مستوي النقل** سبيلاً لنقل معلومات المستعمل باتجاه ثنائي أو أحادي من عنصر شبكة إلى آخر. ويمكن أن يوفر أيضاً سبيلاً لنقل بعض المعلومات المتعلقة بمراقبة الشبكة وإدارتها. **ومستوي النقل** مؤلف من طبقات؛ وهو يكافئ شبكة النقل المحددة في التوصيتين ITU-T Y.1304/G.8080، *معمارية الشبكة البصرية المبدلة أوتوماتياً (ASON)*[12].

26.III المسير الموثوق: هو عبارة عن آلية يُكفل بموجبها تأمين جميع تفاعلات المستعمل/المشغل إلى نظام أو تفاعلات نظام إلى نظام مع نظام معين. ولا يمكن تفعيل هذه الآلية إلا من جانب المستعمل/المشغل أو النظام كما لا يمكن محاكاتها. **والمسير الموثوق** إما أن يكون مسيراً مادياً مخصصاً (أي، مطراف موصول بالنظام مباشرة) أو مسيراً مجفراً يشمل حماية التكاملية والتكرار (مثل الشبكة الخاصة التقديرية "المؤمنة"، ونفق طبقة مقابس الأمن (SSL)، وبرنامج شل للدخول الآمن (SSH)).[14]

27.III الاستيقان المؤلف من عاملين: هو عبارة عن مصطلح يستخدم بشكل عام في وصف عملية استيقان تتطلب حيازة كيان مادي (من قبيل الإذنة أو البطاقة) ومعرفة سر معين (مثل كلمة سر أو عبارة سر).

[14] معدلة عن وثائق المركز الوطني لأمن الحاسوب، NCSC-TG-004-88، *مسرد مصطلحات أمن الحاسوب*، أكتوبر 1998 (متيسر على العنوان التالي http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

بيبليوغرافيا

تقدم البنود الواردة في هذه البيبليوغرافيا معلومات إضافية عن الكثير من المواضيع التي تناولها التذييلان I وII.

– ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*

– ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation,* (available from the ANSI X9 Electronic Standards Store, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80).

– ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* (available from the ANSI X9 Electronic Standards Store, http://webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).

– ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*

– ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.

– ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*

– ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*

– ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.

– ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

– ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Network Elements – Implementation Agreements Version 1.1,* (available at ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

– BARRETT (D.), SILVERMAN (R.): SSH, The Secure Shell: The Definitive Guide, *O'Reilly*, January 2001.

– BELLOVIN (S.): An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.

– BLEICHENBACHER (D.): Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.

– BONEH (D.): Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, February 1999, (available at http://www.ams.org/notices/199902/boneh.pdf).

– BONEH (D.), JOUX (A.), NGUYEN (P.): Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.

– Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, September 1999.

– General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, March 2002 (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GR-1194, *Bellcore Operations Systems Security Requirements*, December 1998, (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GUTMANN (P.): Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998, (available at http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf).

– Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.

– IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*, (available at IEEE Standards Online, http://standards.ieee.org/catalog/olis/ busarch.html).

– IETF RFC 768, *User Datagram Protocol*, J. Postel, August 1980 (available at http://www.ietf.org/rfc/rfc0768.txt?number=768).

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/ rfc0791.txt?number=791).

– IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/rfc0792.txt?number=792).

– IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification*, (available at http://www.ietf.org/rfc/rfc0793.txt?number=793).

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, (available at http://www.ietf.org/rfc/rfc0826.txt?number=826).

– IETF RFC 859 (1983), *Telnet Status Option,* (available at http://www.ietf.org/rfc/rfc0859.txt?number=859).

– IETF RFC 959 (1985), *File Transfer Protocol (FTP),* (available at http://www.ietf.org/rfc/rfc0959.txt?number=959).

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (available at http://www.ietf.org/rfc/rfc1157.txt?number=1157).

– IETF RFC 1288 (1991), *The Finger User Information Protocol,* (available at http://www.ietf.org/rfc/rfc1288.txt?number=1288).

– IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* (available at http://www.ietf.org/rfc/rfc1905.txt?number=1905).

– IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,* (available at http://www.ietf.org/rfc/rfc2045.txt?number=2045).

– IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1,* (available at http://www.ietf.org/rfc/rfc2202.txt?number=2202).

– IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL),* (available at http://www.ietf.org/rfc/rfc2222.txt?number=2222).

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0,* (available at http://www.ietf.org/rfc/rfc2246.txt?number=2246).

– IETF RFC 2271 (1998), *An Architecture for Describing SNMP Management Frameworks,* (available at http://www.ietf.org/rfc/rfc2271.txt?number=2271).

– IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP),* (available at http://www.ietf.org/rfc/rfc2272.txt?number=2272).

– IETF RFC 2273 (1998), *SNMPv3 Applications,* (available at http://www.ietf.org/rfc/rfc2273.txt?number=2273).

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, (available at http://www.ietf.org/rfc/rfc3414.txt?number=3414).

– IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol* (*SNMP)*, (available at http://www.ietf.org/rfc/rfc2275.txt?number=2275).

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, (available at http://www.ietf.org/rfc/rfc2401.txt?number=2401).

– IETF RFC 2402 (1998), *IP Authentication Header,* (available at http://www.ietf.org/rfc/rfc2402.txt?number=2402).

– IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, (available at http://www.ietf.org/rfc/rfc2406.txt?number=2406).

– IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* (available at http://www.ietf.org/rfc/rfc2451.txt?number=2451).

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1,* (available at http://www.ietf.org/rfc/rfc2616.txt?number=2616).

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method,* (available at http://www.ietf.org/rfc/rfc2631.txt?number=2631).

– IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core,* (available at http://www.ietf.org/rfc/rfc3080.txt?number=3080).

– IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP,* (available at http://www.ietf.org/rfc/rfc3081.txt?number=3081).

– ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture,* (available at ISO Online Store, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1 =35&ICS2=100&ICS3=1).

– ITU-T Recommendation M.3010 (2000), *Principles for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).

– ITU-T Recommendation M.3013 (2000), *Considerations for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).

– JANSEN (W.A.): A Revised Model for Role Based Access Control, *NIST-IR 6192*, July 1998, (available at http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

– JONSSON (J.), KALISKI (B.): On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, August 2002.

– KELSEY (J.), SCHNEIER (B.), FERGUSON (N.): Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual*

Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1999, (available at http://www.counterpane.com/yarrow-notes.html).

– KRAWCZYK (H.): Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, August 2002.

– LENSTRA (A.), VERHEUL (E.): Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

– National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms.* October 1988, (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

– National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000, (available at http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, March 2002, (available at http://cgi.omg.org/docs/formal/02-03-11.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* March 2001, (available at http://cgi.omg.org/docs/formal/01-03-08.pdf).

– Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, September 2001, (available at http://www.pcis.org/library.cfm?urlSection=WG).

– RESCORLA (E.): SSL and TLS, Addison-Wesley, 2001.

– SCHNEIER (Bruce.): Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

– SILVERMAN (R.): The Mythical MIPS Year, *IEEE Computer*, August 1999.

– SILVERMAN (R.): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, April 2000.

– VAUDENAY (S.): Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, April-May 2002.

– World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, February 1998, (available at http://www.w3.org/TR/1998/REC-xml-19980210).

– World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, May 2000, (available at http://www.w3.org/TR/SOAP/).

– WU (T.): The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, March 1998, (available at http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

– YLÖNEN, T.: SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, July 1996, (available at http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية وتعدد الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	**نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية**
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2005