الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

# ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

# X.1205

(2008/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات

---

## لمحة عامة عن الأمن السيبراني

التوصيـــة ITU-T X.1205


ITU-T

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

| | |
|---|---|
| الشبكات العمومية للمعطيات | |
| الخدمات والمرافق | X.19–X.1 |
| السطوح البينية | X.49–X.20 |
| الإرسال والتشوير والتبديل | X.89–X.50 |
| مظاهر الشبكة | X.149–X.90 |
| الصيانة | X.179–X.150 |
| الترتيبات الإدارية | X.199–X.180 |
| التوصيل البيني للأنظمة المفتوحة | |
| النموذج والترميز | X.209–X.200 |
| تعريفات الخدمات | X.219–X.210 |
| مواصفات بروتوكول بأسلوب التوصيل | X.229–X.220 |
| مواصفات بروتوكول بأسلوب دون توصيل | X.239–X.230 |
| جداول إعلان عن مطابقة تنفيذ بروتوكول | X.259–X.240 |
| تعرّف هوية البروتوكول | X.269–X.260 |
| بروتوكولات الأمن | X.279–X.270 |
| أشياء مسيرة على الطبقة | X.289–X.280 |
| اختبار المطابقة | X.299–X.290 |
| التشغيل البيني للشبكات | |
| اعتبارات عامة | X.349–X.300 |
| الأنظمة الساتلية لإرسال البيانات | X.369–X.350 |
| الشبكات القائمة على بروتوكول الإنترنت | X.379–X.370 |
| أنظمة معالجة الرسائل | X.499–X.400 |
| الدليـــل | X.599–X.500 |
| التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام | |
| توصيل الشبكات | X.629–X.600 |
| الفعالية | X.639–X.630 |
| نوعية الخدمة | X.649–X.640 |
| التسمية والعنونة والتسجيل | X.679–X.650 |
| ترميز نحو مجرد واحد (ASN.1) | X.699–X.680 |
| إدارة التوصيل البيني للأنظمة المفتوحة (OSI) | |
| الإطار والهيكل المعماري لإدارة الأنظمة | X.709–X.700 |
| خدمة اتصالات الإدارة وبروتوكولاتها | X.719–X.710 |
| هيكل معلومات الإدارة | X.729–X.720 |
| وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة | X.799–X.730 |
| الأمن | X.849–X.800 |
| تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI) | |
| الالتزام والتلازم والاستعادة | X.859–X.850 |
| معالجة المعاملات | X.879–X.860 |
| العمليات البُعدية | X.889–X.880 |
| التطبيقات التنوعية للترميز نحو مجرد واحد (ASN.1) | X.890-X.899 |
| المعالجة الموزعة المفتوحة | X.999–X.900 |
| **أمن الاتصالات** | **–X.1000** |

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

**التوصيـــة ITU-T X.1205**

# لمحة عامة عن الأمن السيبراني


## ملخص

تقدم التوصية ITU-T X.1205 تعريفاً للأمن السيبراني. وتوفر هذه التوصية تصنيفاً للتهديدات الأمنية من منظور المؤسسة. وتعرض التوصية التهديدات المتعلقة بالأمن السيبراني ومواطن الضعف فيه، بما في ذلك أكثر أدوات العابثين شيوعاً. وتناقش التهديدات على مستويات الشبكات المختلفة.

وتناقش مختلف تكنولوجيات الأمن السيبراني المتوفرة لمواجهة هذه التهديدات، بما في ذلك المسيّرات وجدران الحماية والحماية من الفيروسات وأنظمة كشف الاقتحام وأنظمة الحماية من الاقتحام والحوسبة الآمنة والتدقيق والمراقبة. وتناقش كذلك مبادئ حماية الشبكات مثل عمق الدفاع وإدارة النفاذ من حيث تطبيقها على الأمن السيبراني. وتناقش استراتيجيات وتقنيات إدارة المخاطر بما في ذلك أهمية التدريب والتوعية في حماية الشبكات. وتتناول أيضاً أمثلة لتوفير الأمن لمختلف الشبكات استناداً إلى التكنولوجيات التي تناولتها المناقشة.



## المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 18 أبريل 2008 على التوصية ITU-T X.1205 بموجب الإجراء الذي ينص عليه القرار 1 للجمعية العالمية لتقييس الاتصالات.

## تمهيـــد

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).

## ملاحظة

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

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه 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 بهذه 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) في الموقع http://www.itu.int/ITU-T/ipr/.

# المحتـــويات

**الصفحة**

**التوصيـــة ITU-T X.1205**

# لمحة عامة عن الأمن السيبراني

## 1 مجال التطبيق

تقدم هذه التوصية في الفرع 7 تعريفاً للأمن السيبراني. وتوفر تصنيفاً للتهديدات الأمنية من منظور المؤسسة.

**ملاحظة** – لا يشير استعمال مصطلح "هوية" في هذه التوصية إلى المعنى المطلق للمصطلح. وهو لا يشكل تحديداً أي إشارة إيجابية.

ويناقش الفرع 7 طبيعة بيئة الأمن السيبراني في المؤسسة ومخاطر الأمن السيبراني وأمن الاتصالات من طرف إلى طرف. ويناقش الفرع 8 الاستراتيجيات المحتملة لحماية الشبكات والتي تشمل: إدارة سياسة العروة المغلقة وإدارة النفاذ المنتظم. كما يتناول الفرع 8 تقنيات الاتصالات الآمنة ومختلف أعماق الأمن وضمان الأمن في مستوي الإدارة وطبقات الأمن ومدى صمود الشبكات حتى عندما تتعرض للهجوم.

ويتناول التذييل I تصنيفات التهديدات الأمنية والأدوات التي يستخدمها العابثون وتهديدات الأمن.

ويقدم التذييل II عرضاً لمجالات تكنولوجيات الأمن السيبراني التي تشمل: التجفير وتكنولوجيات التحكم في النفاذ وتقنيات حماية المحيط ومكافحة الفيروسات وسلامة النظام وتقنيات التدقيق والمراقبة والإدارة.

ويقدم التذييل III أمثلة على أمن الشبكات. وتشمل هذه الأمثلة تأمين النفاذ عن بُعد وتأمين المهاتفة باستعمال بروتوكول الإنترنت وتأمين عملاء نقل الصوت باستعمال بروتوكول الإنترنت (VoIP) وتأمين المكاتب عن بُعد وتأمين شبكات المنطقة المحلية اللاسلكية (WLAN).

## 2 المراجع

تحتوي التوصيات التالية الصادرة عن قطاع تقييس الاتصالات وغيرها من المراجع بعض الأحكام التي تشكل أحكاماً في هذه التوصية، بموجب الإحالة إليها في النص. ففي تاريخ نشر هذه التوصية كانت الطبعات المذكورة لا تزال صالحة. وبما أن جميع التوصيات والمراجع الأخرى تخضع للمراجعة، لذا يتعيَّن على مستعملي هذه التوصية السعي إلى تطبيق أحدث صيغ التوصيات والمراجع الأخرى الواردة أدناه. ويجري بانتظام نشر قائمة بالتوصيات السارية التي تصدر عن القطاع. والإحالة داخل هذه التوصية إلى وثيقة ما لا يضفي على هذه الوثيقة صفة توصية.

[ITU-T X.800] التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف*.

[ITU-T X.805] التوصية ITU-T X.805 (2003)، *معمارية أمن الأنظمة التي تكفل الاتصالات من طرف إلى طرف*.

[ITU-T X.811] التوصية ITU-T X.811 (1995)، | المعيار ISO/IEC 10181-2:1996، تكنولوجيا المعلومات - التوصيل البيني بين الأنظمة المفتوحة - *أطر الأمن في الأنظمة المفتوحة: إطار الاستيقان*.

[ITU-T X.812] التوصية ITU-T X.812 (1995) | المعيار ISO/IEC 10181-3:1996، *تكنولوجيا المعلومات - التوصيل البيني بين الأنظمة المفتوحة - أطر الأمن في الأنظمة المفتوحة: إطار التحكم في النفاذ*.

[IETF RFC 1918] الرسالة IETF RFC 1918 (1996)، *توزيع العناوين على شبكات الإنترنت الخاصة* <http://www.ietf.org/rfc/rfc1918.txt?number=1918>.

[IETF RFC 2396] الرسالة IETF RFC 2396 (1998)، *معرفات هوية الموارد الموحدة (URI): قواعد التركيب التنوعية* <http://www.ietf.org/rfc/rfc2396.txt?number=2396>

## 3 التعاريف

### 1.3 مصطلحات معرفة في أماكن أخرى

تستخدم هذه التوصية المصطلحات التالية المعرفة في مكان آخر:

**1.1.3** تستخدم هذه التوصية المصطلحات التالية المعرفة في التوصية [ITU-T X.800]:

أ ) الترخيص؛

ب) معمارية الأمن؛

ج) سياسة الأمن؛

د ) المستعمل.

**2.1.3** تستخدم هذه التوصية المصطلحين التاليين المعرفين في التوصية [ITU-T X.805]:

أ ) بُعد الأمن؛

ب) خدمة الأمن.

**3.1.3** تستخدم هذه التوصية المصطلحين التاليين المعرفين في التوصية [ITU-T X.811]:

أ ) الاستيقان؛

ب) المبدأ.

**4.1.3** تستخدم هذه التوصية المصطلحات التالية المعرفة في التوصية [ITU-T X.812]:

أ ) معلومات التحكم في النفاذ؛

ب) النفاذ؛

ج) التحكم في النفاذ؛

د ) المستعمل.

**5.1.3** تستخدم هذه التوصية المصطلحين التاليين المعرفين في الرسالة [IETF RFC 2396]:

أ ) معرف الموارد الموحد؛

ب) مرجع معرف الموارد الموحد.

### 2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

**1.2.3** **نقطة النفاذ:** محور لا سلكي وفقاً للمعيار IEEE 802.11، نوع خاص من المحطات العاملة كنقطة نفاذ.

**2.2.3** **مجموعة خدمات أساسية (BSS):** منطقة تغطية تخدمها نقطة نفاذ واحدة (AP).

**3.2.3** **خوارزمية تجفير:** خوارزمية التجفير هي الوسيلة التي يتم بواسطتها تغيير البيانات وإخفائها في التشفير.

**4.2.3** **البيئة السيبرانية:** تشمل المستعملين والشبكات والأجهزة وجميع البرمجيات والمعالِجات والمعلومات المخزنة أو العابرة والتطبيقات والخدمات والأنظمة التي يمكن توصيلها مع الشبكات بصورة مباشرة أو غير مباشرة.

**5.2.3** **الأمن السيبراني:** مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين

والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية. ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن ما يلي:

- التيسر؛
- السلامة، التي قد تضم الاستيقان وعدم الرفض؛
- السرية.

**6.2.3 النظام الموزع**: وسيط غير مقيّس لربط مجموعات الخدمة الأساسية (BSS) داخل مجموعة الخدمات الموسعة (ESS).

**7.2.3 بروتوكول الاستيقان القابل للتمديد**: يشكل هذا التمديد في البروتوكول من نقطة إلى نقطة (PPP) الذي يوفر الدعم لطرائق الاستيقان الإضافية جزءاً من مواصفات [b-IEEE 802.1X].

**8.2.3 مجموعة الخدمات الموسعة**: شبكة منطقة محلية لا سلكية وحيدة مع مجموعات خدمة أساسية (BSS) داخل شبكة فرعية واحدة تعتمد بروتوكول الإنترنت.

**9.2.3 جدار الحماية**: نظام أو توليفة من الأنظمة تضع حدوداً بين شبكتين أو أكثر. بوابة تحد من النفاذ بين الشبكات وفقاً للسياسة الأمنية المحلية.

**10.2.3 وكيل أجنبي**: مسيّر الشبكة المزارة أو المضيفة الذي يخدم عقدة متنقلة عندما تزور الشبكة المضيفة. ويتناول الوكيل الأجنبي عملية التمرير والتسليم فيما بين العقدة المتنقلة والعقد الأخرى وبين الشبكة الأساس للخدمة المتنقلة والشبكة المضيفة.

**11.2.3 برمجية استدراج (Honeyspot)**: برمجية تحاكي شبكة لاجتذاب (وربما إرباك) المقتحمين وتتبّع ما يقومون به من أعمال. ويمكن استخدام نتائج هذه الأنظمة للاستدلال على نوايا المقتحمين وجمع القرائن ضدهم.

**12.2.3 وكيل الشبكة الأساس**: مسيّر يخدم العقدة المتنقلة عندما تزور شبكات أخرى ويحتفظ بالمعلومات المتعلقة بالموقع الحالي في تلك العقدة المتنقلة.

**13.2.3 مواقع ساخنة**: أماكن عامة تستضيف مستعملي الخدمة المتنقلة IEEE 802.11 لربطهم بالإنترنت.

**14.2.3 تنقلية بروتوكول الإنترنت**: آلية تمكّن من توفير توصيلية أكثر شفافية للعقد المتنقلة التي "تزور" شبكات فرعية مختلفة تعتمد بروتوكول الإنترنت أثناء انتقالها. وهي آلية للإدارة المتنقلة للعقد المتنقلة في الشبكات السلكية واللاسلكية على السواء.

## 4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

3DES معيار تجفير بيانات ثلاثي *(Triple Data Encryption Standard)*

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

ACL قائمة التحكم في النفاذ *(Access Control List)*

AES معيار تجفير متقدم *(Advanced Encryption Standard)*

AP نقطة نفاذ *(Access Point)*

ASP مورد خدمة تطبيقات *(Application Service Provider)*

BSS مجموعة خدمات أساسية *(Basic Service Set)*

CA سلطة إشهاد *(Certification Authority)*

CMP بروتوكول إدارة الشهادات *(Certificate Management Protocol)*

COPS خدمة سياسات مفتوحة مشتركة *(Common Open Policy Service)*

CRL قائمة إلغاء الشهادات *(Certificate Revocation List)*

DISA نفاذ مباشر إلى النظام الداخلي *(Direct Inward System Access)*

DNS نظام أسماء الميادين *(Domain Name System)*

EAP بروتوكول استيقان قابل للتمديد *(Extensible Authentication Protocol)*

EMS نظام إدارة العناصر *(Element Management System)*

ESS مجموعة خدمات موسعة *(Extended Service Set)*

ESSID معرّف مجموعة خدمات موسعة *(Extended Service Set Identifier)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HMAC شفرات استيقان الرسائل المعتمدة على دالة الفرم *(Hash function based MACs)*

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

IDS نظام كشف الاقتحام *(Intrusion Detection System)*

IKE تبادل مفاتيح الإنترنت *(Internet Key Exchange)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPSec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

ISP مورد خدمة الإنترنت *(Internet Service Provider)*

L2TP بروتوكول تمرير الطبقة 2 *(Layer 2 Tunneling Protocol)*

LAN شبكة المنطقة المحلية *(Local Area Network)*

MAC شفرة استيقان الرسالة *(Message Authentication Code)*

MD5 خوارزمية استيعاب الرسالة 5 *(Message Digest algorithm 5)*

MIC التحقق من سلامة الرسالة *(Message Integrity Check)*

MIME تمديدات بريد الإنترنت متعددة الأغراض *(Multipurpose Internet Mail Extensions)*

MPLS تبديل الواسمة متعددة البروتوكولات *(MultProtocol Label Switching)*

MU وحدة متنقلة *(Mobile Unit)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

NGN شبكات الجيل التالي *(Next Generation Network)*

NIC بطاقة السطح البيني للشبكة *(Network Interface Card)*

NOC مركز عمليات الشبكة *(Network Operations Centre)*

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

OCSP بروتوكول حالة الشهادات على الخط *(Online Certificate Status Protocol)*

OS نظام التشغيل *(Operating System)*

OSI التوصيل ما بين الأنظمة المفتوحة *(Open Systems Interconnection)*

PDP نقطة القرارات المتعلقة بالسياسات *(Policy Decision Point)*

PEAP بروتوكول الاستيقان التوسعي المحمي *(Protected EAP protocol)*

PEP نقطة إنفاذ السياسات *(Policy Enforcement Point)*

PGP خصوصية بدرجة معقولة *(Pretty Good Privacy)*

PKI بنية تحتية لمفتاح عمومي *(Public Key Infrastructure)*

PKIX بنية تحتية لمفتاح عمومي X.509 *(Public Key Infrastructure X.509)*

PoP برهان الملكية *(Proof of Possession)*

PPP بروتوكول نقطة-إلى-نقطة (*Point-to-Point Protocol*)

PSTN شبكة هاتفية عمومية تبديلية *(Public Switched Telephone Network)*

RADIUS خدمة الاستيقان عن بُعد من مستعمل بالمراقمة *(Remote Authentication Dial-in User Service)*

RSA خوارزمية مفتاح عمومي وضعها ريفتس وشامير وأدلمان *(Rivest Shamir Adleman public key algorithm)*

SHA-1 خوارزمية فرم مأمونة 1 *(Secure Hash Algorithm 1)*

SIP بروتوكول استهلال الدورة *(Session Initiation Protocol)*

SMTP بروتوكول نقل البريد بأسلوب بسيط *(Simple Mail Transfer Protocol)*

SNMP بروتوكول إدارة الشبكة بأسلوب بسيط *(Simple Network Management Protocol)*

SP مورد الخدمة *(Service Provider)*

SSH قشرة آمنة *(Secure Shell)*

SSID تعرّف مجموعة الخدمات *(Service Set Identification)*

SSO تسجيل دخول وحيد *(Single Sign On)*

TKIP بروتوكول سلامة مفتاح مؤقت *(Temporal Key Integrity Protocol)*

TLS بروتوكول أمن طبقة النقل *(Transport Layer Security Protocol)*

UE تجهيزات المستعمل *(User Equipment)*

URI معرّف الموارد الموحد *(Uniform Resource Identifier)*

UTC التوقيت العالمي المنسق *(Coordinated Universal Time)*

VAR بائع ثان بقيمة مضافة **(***Value-Added Reseller***)**

VLAN شبكة منطقة محلية افتراضية *(Virtual LAN)*

VoIP نقل الصوت باستعمال بروتوكول الإنترنت *(Voice-over-IP)*

VPLS خدمة شبكة منطقة محلية خاصة افتراضية *(Virtual Private LAN Service)*

VPN شبكة خاصة افتراضية (*Virtual Private Network*)

VPWS خدمة سلكية خاصة افتراضية *(Virtual Private Wire Service)*

WAN شبكة منطقة واسعة *(Wide Area Network)*

WEP خصوصية مكافئة للخصوصية السلكية *(Wired Equivalent Privacy)*

WLAN شبكة منطقة محلية لا سلكية *(Wireless LAN)*

WPA نفاذ Wi-fi محمي *(Wi-fi Protected Access)*

XML لغة توسيم موسعة *(eXtensible Markup Language)*

## 5 الاصطلاحات

يستعمل مصطلح تجهيزات المستعمل (UE) في هذه التوصية بمعناه الواسع ليشمل جميع أنواع الأجهزة والكيانات (القائمة على العتاد أو البرمجيات) المتنقلة و/أو الثابتة والحواسيب الشخصية والمطاريف (متعددة الوسائط) والهواتف وغيرها مما يوجد في أماكن المستعملين والتي غالباً ما تخرج عن قدرة تحكم المشغِّل أو مورد الخدمة فيها.

## 6 مقدمة

يمكن أن يؤدي استخدام الشبكات للربط بين شتى أنظمة تكنولوجيا المعلومات إلى تحقيق مكاسب في الإنتاجية للمؤسسات فضلاً عن قدرات جديدة تتيحها الأنظمة الموصولة بالشبكة. وقد أصبح من الميسور في يومنا هذا الحصول على المعلومات والاتصال ومراقبة أنظمة تكنولوجيا المعلومات والتحكم فيها عبر مسافات شاسعة. وعلى ذلك فإن شبكات اليوم تضطلع بدور رئيسي في البنى التحتية الحرجة لكثير من الدول والتي تشمل التجارة الإلكترونية والاتصالات الصوتية وإرسال البيانات والمرافق والتعاملات المالية والصحة والنقل والدفاع.

وتعتبر توصيلية الشبكات والنفاذ المتيسر في كل مكان في آن واحد عنصراً أساسياً في أنظمة تكنولوجيا المعلومات اليوم. ولعل انتشار مواطن الضعف على نطاق واسع يعود أساساً إلى الانتشار الواسع للنفاذ والترابط الطليق بين شبكات أنظمة تكنولوجيا المعلومات. فقد أخذت تتزايد التهديدات التي تواجه الأنظمة الموصولة بالشبكة، ومنها هجمات رفض الخدمة وسرقة البيانات المالية والشخصية وأعطال الشبكات وتعطيل الاتصالات الصوتية وإرسال البيانات.

وقد استحدثت بروتوكولات الشبكات المستخدمة اليوم في بيئة من الثقة. وأصبحت معظم عمليات الاستثمار والتطوير الجديدة تنصب على ابتكار وظائف جديدة وليس على حماية هذه الوظائف.

وتتزايد تهديدات الأمن السيبراني زيادة سريعة. وما فتئت تتزايد الفيروسات والديدان والبرمجيات المتسللة (أحصنة طروادة) وهجمات الاحتيال و"انتحال الهوية"[1] والرسائل الاقتحامية والهجمات السيبرانية. ولذا فإن ثمة حاجة إلى فهم الأمن السيبراني من أجل إقامة أساس للمعارف التي يمكن أن تساعد في حماية شبكات الغد.

وحريّ بالمؤسسات والوكالات الحكومية أن تنظر إلى الأمن بوصفه عملية أو وسيلة للتفكير بكيفية حماية الأنظمة والشبكات والتطبيقات والموارد. والتفكير الأساسي هو أن الشبكات المترابطة تنطوي على مخاطر متأصلة. غير أنه ينبغي ألا يكون الأمن عقبة أمام الأعمال التجارية. والهدف هو كيفية تقديم الخدمات اللازمة بطريقة مأمونة.

ومفهوم الحدود يتلاشى في بيئة الأعمال اليوم، كما تتلاشى الحدود بين الشبكات الداخلية والخارجية. فالتطبيقات تجري فوق الشبكات طبقة فوق أخرى. ويفترض توافر الأمن بين كل من هذه الطبقات. والمنهج الطبقي إزاء الأمن يُمكِّن المؤسسات من استحداث مستويات دفاع متعددة ضد التهديدات.

## 7 الأمن السيبراني

يتعين على المؤسسات أن تستحدث خطة شاملة لمعالجة احتياجاتها الأمنية. وحريّ بالمؤسسات أن تنظر إلى الأمن بوصفه عملية أو وسيلة للتفكير بكيفية حماية الأنظمة والشبكات والتطبيقات والموارد.

---

[1] يعني مصطلح "انتحال الهوية" الاستعمال المحظور لمجموعة معرّفات ومعلومات أخرى تشكل مجتمعة سمة هوية مستعمل محدد. وعلى النقيض من المفهوم العادي للسرقة حيث ينتزع الغرض المقصود من الضحية بشكل محسوس، فإن انتحال الهوية ينطوي عموماً على استخراج تفاصيل الهوية أو نسخها على نحو لا يكون فيه صاحب الهوية المشروع مدركاً للسرقة.

## 1.7 ما هو الأمن السيبراني؟

يعرّف مصطلح الأمن السيبراني في هذه التوصية في الفقرة 5.2.3.

وتستخدم تقنيات الأمن السيبراني لضمان تيسر النظام وسلامته وأصالته وسريته وعدم رفضه. ويمكن استخدام الأمن السيبراني لضمان احترام خصوصية المستعمل. ويمكن استخدام تقنيات الأمن السيبراني لمعرفة جدارة المستعمل بالثقة.

وتوسع بعض التكنولوجيات، مثل الشبكات اللاسلكية ونقل الصوت باستعمال بروتوكول الإنترنت (VoIP)، من نطاق الإنترنت واتساعها. وفي هذا الصدد، تشمل البيئة السيبرانية المستعملين والإنترنت والأجهزة الحاسوبية الموصولة بها وجميع التطبيقات والخدمات والأنظمة التي يمكن توصيلها بصورة مباشرة أو غير مباشرة بالإنترنت وببيئة شبكات الجيل التالي، وتوصيل هذه الشبكات بالأشكال العامة والخاصة منها. وعلى ذلك فإن الهاتف المكتبي يصبح باستخدام تكنولوجيا نقل الصوت باستعمال بروتوكول الإنترنت، جزءاً من البيئة السيبرانية. بل إن الأجهزة المنفصلة قد تكون أيضاً جزءاً من البيئة السيبرانية إذا كانت قادرة على أن تتقاسم المعلومات مع الأجهزة الحاسوبية الموصولة من خلال وسائط قابلة للإزالة.

وتشمل البيئة السيبرانية البرمجيات التي تديرها الأجهزة الحاسوبية والمعلومات المختزنة (المرسلة أيضاً) في هذه الأجهزة أو المعلومات التي تولدها هذه الأجهزة. وكذلك فإن المنشآت والمباني التي تضم هذه الأجهزة تشكل جزءاً من البيئة السيبرانية. ويتعين على الأمن السيبراني أن يأخذ هذه العناصر في الاعتبار.

ويهدف الأمن السيبراني إلى ضمان أمن البيئة السيبرانية، وهو نظام قد يشمل أصحاب المصلحة الذين ينتمون إلى العديد من منظمات القطاعين العام والخاص، باستخدام مكونات متنوعة وأساليب مختلفة لتحقيق الأمن. ومن هذا المنطلق من المفيد النظر إلى الأمن السيبراني من المنظور التالي:

- جمع السياسات والإجراءات التي تستخدم في حماية الشبكات الموصولة (بما في ذلك الحواسيب والأجهزة والمعدات والمعلومات المختزنة والمعلومات العابرة) من النفاذ غير المرخص به ومن التعديل أو السرقة أو التشويش أو الانقطاع أو غير ذلك من التهديدات.
- عملية تقييم ومراقبة جارية للسياسات والإجراءات المشار إليها أعلاه لضمان استمرار نوعية الأمن في مواجهة الطابع المتغير للتهديدات.

وتضع التوصية [b-ITU-T Y.2201] شروطاً على شبكات الجيل التالي من شأنها أن تعزز الأمن السيبراني لهذه الشبكات. ويتطلب العمل توفير الاستيقان مع إمكانية استيقان الأجهزة والمستعملين كل على حدة. وفي شبكات الجيل التالي يقلل الاستيقان الثنائي متعدد العوامل، إلى جانب الترخيص على أساس كل خدمة على حدة، من مخاطر الهجمات التي تهدد المستعمل.

## 2.7 طبيعة بيئة الأمن السيبراني في المؤسسة

يتعين على المنظمات أن تضع خطة شاملة لمعالجة احتياجاتها الأمنية. فالأمن ليس حلاً واحداً يناسب جميع الأحوال (انظر التوصية [ITU-T X.805]). ولا يمكن تحقيق الأمن بواسطة مجموعة من الوحدات النموذجية المترابطة. وحريّ بالمنظمات أن تنظر إلى الأمن بوصفه عملية أو أسلوب تفكير بشأن كيفية حماية الأنظمة والشبكات والتطبيقات وخدمات الشبكة.

وينبغي أن يكون الأمن شاملاً عبر جميع طبقات الشبكة. فاعتماد منهج من عدة طبقات لتوفير الأمن يمكنه، عندما يقترن بإدارة وإنفاذ السياسات القوية، أن يتيح لخبراء الأمن المهنيين اختيار حلول أمنية تكون مؤلفة من وحدات نموذجية وتتسم بالمرونة وإمكانية التوسع.

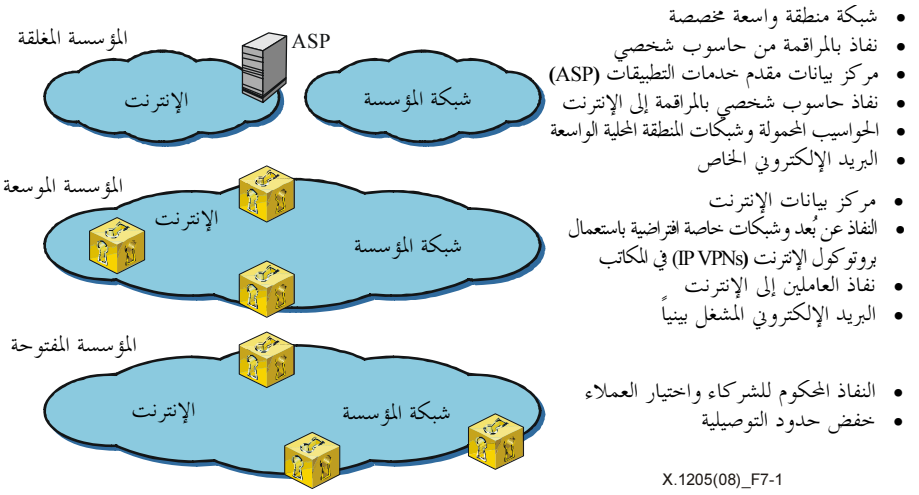
والواقع أن الأمن صعب الاختبار والتنبؤ والتنفيذ. فالأمن ليس حلاً واحداً يناسب جميع الأوضاع. فالاحتياجات الأمنية والاستراتيجية الأمنية الموصى بها لكل منظمة فريدة ومختلفة. فعلى سبيل المثال، قد يكون لأي مؤسسة أو مورد اتصالات أو مشغل شبكة أو مورد خدمات مجموعة فريدة من احتياجات العمل، وتكون قد طورت بيئتها الشبكية لتلبية هذه الاحتياجات.

فالمؤسسة المغلقة مثلاً تستخدم خطوطاً منطقية (ترحيل رتل مثلاً) أو خطوطاً خاصة مادية بين المواقع، ويوفر النفاذ عن بُعد بصورة انتقائية للعاملين الذين يحتاجون إلى النفاذ إلى الإنترنت. ويتحقق وجود الويب من خلال مركز لبيانات الإنترنت يوفره مورد خدمة (يكون مسؤولاً عن إقامة بيئة مأمونة). وتوفر المنظمة أيضاً النفاذ التقليدي بالمراقمة للعاملين عن بعد (مثل العمل من فندق). وتستخدم الشركة البريد الإلكتروني الخاص بين العاملين دون نفاذ خارجي. كما تستخدم شبكة المنطقة المحلية اللاسلكية أيضاً.

وبإمكان المؤسسة الموسعة أو مورد الاتصالات أو مشغل الشبكة أو مورد الخدمة، من خلال نماذج تجارية مختلفة، تقديم الدعم لنفاذ العاملين عن بُعد والمكاتب عن بُعد عن طريق شبكات خاصة افتراضية (VPN) باستعمال بروتوكول الإنترنت (IP) عبر شبكة الإنترنت أو توفير توصيلية بسرعة أعلى وتكاليف أقل، ومنها النفاذ للأغراض العامة لجميع العاملين إلى الإنترنت مثل التشغيل بين أنظمة البريد الإلكتروني الداخلية وبقية العالم.

وفي المؤسسة المفتوحة يمكن للنموذج التجاري أن يستغل الإنترنت من خلال السماح للشركاء والموردين والعملاء بالنفاذ إلى مركز بيانات الإنترنت الذي تديره المؤسسة، بل والسماح بالنفاذ الانتقائي إلى قواعد البيانات والتطبيقات الداخلية (كجزء من نظام إدارة سلسلة توريد مثلاً). وهكذا بإمكان المستعملين الداخليين والخارجيين النفاذ إلى شبكة المؤسسة من المنازل أو المكاتب عن بُعد أو الشبكات الأخرى باستخدام الأجهزة السلكية أو المتنقلة. وعليه فإن متطلبات الأمن في مثل هذه المؤسسة مختلفة عما هي في المؤسسات الأخرى.

ويلخص الشكل 7-1 أنماط هذه المؤسسات:




**الشكل 7-1 – أنماط المؤسسات عموماً**

ويتطلب الأمن السيبراني إدارة المخاطر. وتتناول هذه العملية مهمة تحديد مجموعة المكونات التي تحتاج إلى حماية. ومن المفيد، لتيسير تحليل المخاطر، تصنيف الهجمات حسب الفئات التالية:

1) هجمات لتعطيل الخدمة: تؤدي هذه الهجمات إلى تعطيل نفاذ المستعمل إلى الخدمات المستهدفة سواء بصورة مؤقتة أو دائمة. مثال ذلك، انعدام النفاذ إلى موقع الويب أو العجز عن إجراء معاملة مالية ما أو عن استهلال نداء صوتي. وقد تؤدي أنماط عديدة من الهجمات إلى اضطراب الخدمة. فقد يؤدي منع الخدمة (DoS) أو الهجمات الموزعة لمنع الخدمة (DDoS) أو إتلاف المباني التي تحوي البنية التحتية الأساسية إلى منع المستعملين من النفاذ إلى الخدمة.

2) الإضرار بالأصول: تتناول هذه الهجمات السرقة أو سوء استخدام البنية التحتية. وقد يكون لها تأثير على الأمن السيبراني إذا نفذت على نطاق واسع.

3) قرصنة المكونات: ترمي هذه الهجمات إلى السيطرة على بعض الأجهزة ثم استخدامها لإطلاق هجمات جديدة ضد مكونات أخرى في البيئة السيبرانية.

وقد ينطوي أي عنصر في البيئة السيبرانية على خطر أمني يعتبر عموماً بمثابة تقييم مجموع التهديدات. وتشمل عملية تحليل التهديدات مهمة وصف نمط الهجمات المحتملة، والمهاجمين المحتملين وطرائق هجماتهم وعواقب نجاح الهجمات. ومن ناحية أخرى، تشير قابلية التأثر في هذه التوصية إلى نقطة ضعف يمكن أن يستغلها المهاجم. ويتيح تقييم المخاطر المقترن بتحليل التهديدات للمنظمة تقييم المخاطر المحتملة التي تهدد شبكاتهم.

ويمكن أن تنشأ الهجمات في البيئة السيبرانية، بواسطة الديدان أو غير ذلك من برمجيات الأذى، من خلال الهجوم المباشر على البنية التحتية الأساسية، مثل كبلات الاتصالات، أو من خلال أعمال يرتكبها شخص موثوق به من الداخل. ويمكن أيضاً حدوث توليفة من هذه الهجمات. وتتصف المخاطر عادة بأنها عالية أو متوسطة أو منخفضة. ويتفاوت مستوى المخاطر بين مختلف مكونات البيئة السيبرانية.

ومسألة الأمن تتلخص في إدارة المخاطر. ويمكن استخدام الكثير من التقنيات لإدارة المخاطر. إذ يمكن مثلاً: وضع استراتيجية دفاع تحدد التدابير المضادة لهجمات محتملة، أو تحري الخطر باكتشاف الهجوم أثناء وقوعه أو بعده، أو إعداد استجابة تحدد فيها مجموعة التدابير المضادة لأي هجوم إما لوقفه أو للحد من تأثيره، أو وضع استراتيجية نهوض تمكّن الشبكة من استئناف التشغيل اعتباراً من حالة معروفة.

### 3.7 التهديدات التي تواجه الأمن السيبراني ومنهجية معالجتها

تتضمن التهديدات التي تواجه نظام اتصالات البيانات، بحسب ما جاء في التوصية ITU-T X.800، ما يلي:

أ ) إتلاف المعلومات و/أو الموارد الأخرى؛

ب) إفساد المعلومات أو تعديلها؛

ج) سرقة المعلومات و/أو الموارد الأخرى أو إزالتها أو خسارتها؛

د ) إفشاء المعلومات؛

هـ ) تعطيل الخدمات.

وطبقاً للتوصية [ITU-T X.800]، يمكن تصنيف التهديدات تبعاً لما إذا كانت عارضة أو متعمدة، وقد تكون نشيطة أو سلبية. والتهديدات العارضة تحدث دون سابق عزم. ومن أمثلة التهديدات العارضة سوء أداء النظام وأخطاء التشغيل الفادحة وأخطاء البرمجيات. وقد تتراوح التهديدات المتعمدة من مجرد الفحص العابر، باستخدام أدوات الرصد المتيسرة بسهولة، إلى الهجمات المتطورة باستخدام المعارف الخاصة بالنظام. ويمكن اعتبار التهديد المتعمد، إذا تحقق، بمثابة "هجمة". والتهديدات السلبية، إذا تحققت، لا تسفر عن أي تعديل في أي من المعلومات في النظام أو الأنظمة ولا يحدث أي تغيير في تشغيل النظام أو في حالته. كما أن التنصّت السلكي السلبي لمراقبة المعلومات التي يجري إرسالها على خط اتصالات يمثل تهديداً سلبياً. أما التهديدات النشيطة فتشمل تغيير المعلومات في النظام أو إجراء تغييرات في حالة النظام أو في تشغيله. ويعتبر التغيير المؤذي في جداول تسيير نظام ما من قِبل مستعمل غير مرخص له مثالاً لتهديد نشيط. ويقدم التذييل I ملخصاً موجزاً لبعض الأنماط المحددة من الهجمات.

وتنطبق تهديدات الأمن الواردة في التوصية X.800 أيضاً على البيئة السيبرانية. وطبقاً للتوصية [ITU-T X.800]، فإن تدابير الأمن تزيد عادة من تكاليف النظام وقد تزيد من صعوبة استعماله. ولذا يوصى، قبل تصميم أي نظام مأمون، بتحديد التهديدات التي يستدعي الأمر الوقاية منها. وهذا ما يعرف بتقييم التهديدات. وينطوي أي نظام على الكثير من نقاط الضعف إلا أن بعضاً منها فقط يمكن أن يتعرض للاستغلال إما لأن المهاجم لا يجد الفرصة أو لأن النتيجة لا تبرر الجهد أو التعرض لاحتمال الكشف.

وتستهدف التهديدات الأصول، ولذا يتعين كخطوة أولى وضع قائمة بالأصول التي تتطلب الحماية. أما الخطوة الثانية فهي تحليل التهديد ثم تحليل قابلية التأثر (بما في ذلك تقييم الأثر) والتدابير المضادة والآليات الأمنية.

وعلى الرغم من أن تفصيل مسائل تقييم التهديدات تقع خارج نطاق هذه التوصية، فإنها تشمل بصورة إجمالية ما يلي:

أ ) تحديد مواطن الضعف في النظام؛

ب) تحليل احتمالية التهديدات التي تهدف إلى استغلال مواطن الضعف هذه؛

ج) تقييم العواقب في حالة تنفيذ كل تهديد بنجاح؛

د ) تقدير تكلفة كل هجمة؛

ه ) تقدير تكاليف التدابير المضادة المحتملة؛

و ) اختيار آليات الأمن المسوّغة (ربما باستخدام تحليل نسبة التكلفة إلى الفائدة).

وفي بعض الحالات، قد تكون التدابير غير التقنية، مثل التغطية بالتأمين، من البدائل الفعالة من حيث التكلفة. وعموماً لا يمكن تحقيق أمن تقني كامل. ولذا يتعين أن يكون الهدف جعل تكلفة أي هجوم عالية بحيث ينخفض الخطر إلى مستويات مقبولة.

### 4.7 أمن الاتصالات من طرف إلى طرف

تحدد التوصية [ITU-T X.805] إطار أمن الشبكة اللازم لتوفير أمن الشبكة من طرف إلى طرف. وتنطبق التوصية [ITU-T X.805] على أنماط مختلفة من الشبكات حيث يكون أمن الشبكة من طرف إلى طرف موضع اهتمام. والمعمارية مستقلة عن التكنولوجيا الأساسية للشبكة.

وتتصدى معمارية الأمن للتحديات الأمنية العالمية التي تواجه موردي الخدمة والمؤسسات والمستهلكين، وتنطبق على الشبكات اللاسلكية والبصرية والصوتية السلكية وشبكات البيانات والشبكات المتقاربة. وتتناول المعمارية الشواغل الأمنية المتعلقة بإدارة ومراقبة واستخدام البنى التحتية والخدمات والتطبيقات ذات الصلة بالشبكة. وتمكن التوصية [ITU-T X.805] من الكشف الاستباقي لمواطن الضعف الأمنية إزاء التهديدات المعروفة ومن تخفيفها. وتقسم معمارية الأمن بصورة منطقية المجموعة المعقدة من جوانب أمن الشبكة من طرف إلى طرف إلى مكونات معمارية منفصلة. ويتيح هذا الفصل توفير أسلوب منهجي إزاء الأمن من طرف إلى طرف يمكن استخدامه لتخطيط حلول أمنية جديدة فضلاً عن تقييم أمن الشبكات القائمة.

وتعرّف التوصية [ITU-T X.805] البعد الأمني بأنه مجموعة من التدابير الأمنية المصممة لمعالجة جانب معين من جوانب أمن الشبكة. وتعرّف التوصية [ITU-T X.805] ثمانية أبعاد تحمي من جميع التهديدات الأمنية الرئيسية. وهذه الأبعاد لا تقتصر على الشبكة بل تمتد أيضاً لتشمل التطبيقات ومعلومات المستعمل النهائي. وتسري الأبعاد الأمنية على موردي الخدمة أو المؤسسات التي تقدم خدمات أمنية لعملائها. وهذه الأبعاد الأمنية هي:

1) التحكم في النفاذ؛

2) الاستيقان؛

3) عدم الإنكار؛

4) سرية البيانات؛

5) أمن الاتصالات؛

6) سلامة البيانات؛

7) التيسر؛

8) الخصوصية.

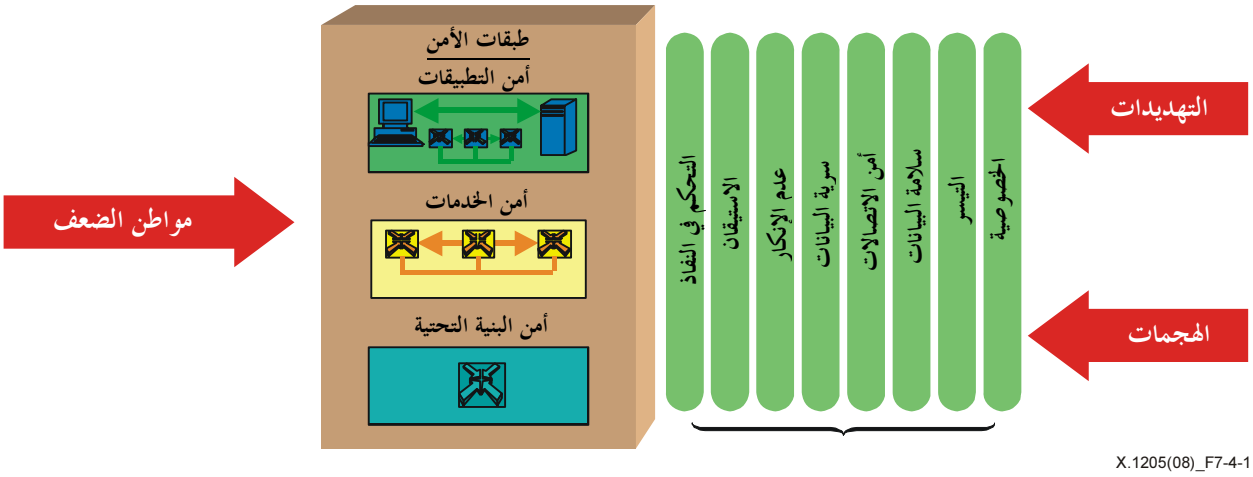
وينبغي، لتوفير حل أمني من طرف إلى طرف، تطبيق الأبعاد الأمنية على تراتب من معدات الشبكة ومجموعات المرافق التي تعرف باسم طبقات الأمن. وتتناول التوصية طبقات الأمن الثلاث التالية:

1) طبقة أمن البنية التحتية؛

2) طبقة أمن الخدمات؛

3) طبقة أمن التطبيقات.

وتحدد طبقات الأمن أين تتخذ تدابير الأمن في المنتجات والحلول من خلال توفير منظور تعاقبي لأمن الشبكة. فعلى سبيل المثال، تعالج أولاً مواطن ضعف الأمن في طبقة البنية التحتية ثم في طبقة الخدمات وتعالج مواطن ضعف الأمن في طبقة التطبيقات. ويبين الشكل 7-1.4 كيفية تطبيق الأبعاد الأمنية على الطبقات الأمنية للحد من مواطن الضعف الموجودة في كل طبقة.




**الشكل 7-1.4 – تطبيق الأبعاد الأمنية على الطبقات الأمنية**

وتصف التوصية [ITU-T X.805] مستوي الأمن بأنه نمط معين من نشاط الشبكة تحميه أبعاد أمنية. وتحدد التوصية [ITU-T X.805] ثلاثة مستويات للأمن لتمثيل الأنماط الثلاثة من الأنشطة المحمية في الشبكة. ومستويات الأمن هي:

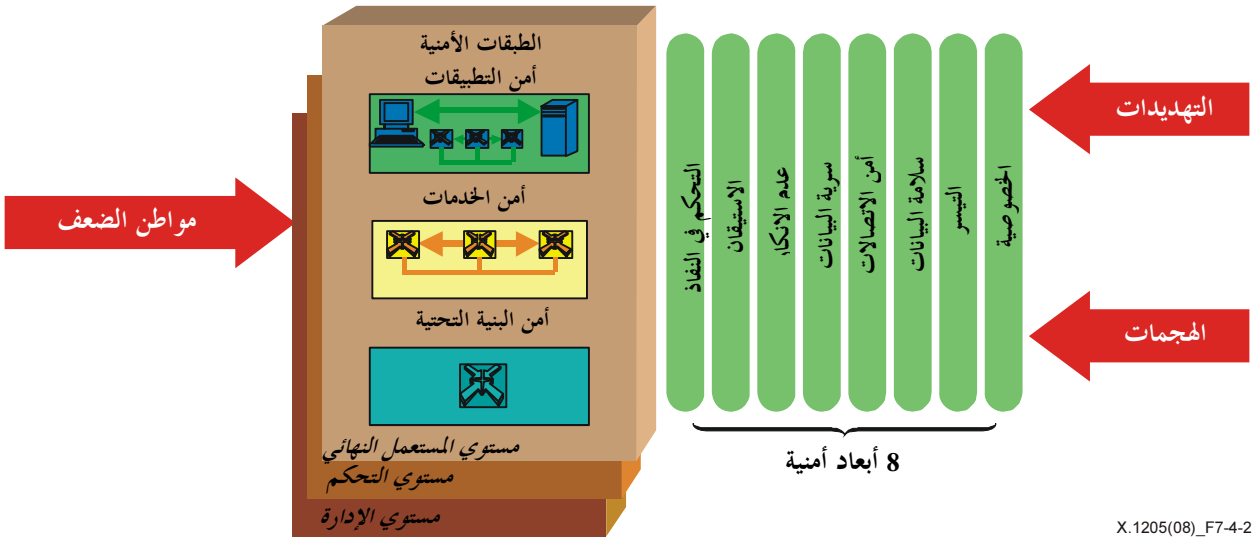
1) مستوي الإدارة؛

2) مستوي التحكم؛

3) مستوي المستعمل النهائي.

وتعالج هذه المستويات الأمنية احتياجات أمنية معينة مرتبطة بكل من أنشطة إدارة الشبكة، والتحكم في الشبكة أو أنشطة التشوير، وأنشطة المستعمل النهائي. وتقترح التوصية [ITU-T X.805] ضرورة تصميم الشبكات بحيث تبقى الأحداث التي تجري في مستوي أمني معزولة عن مستويات الأمن الأخرى. فعلى سبيل المثال، ينبغي ألا تؤدي موجة كبيرة من عمليات البحث في نظام أسماء الميادين (DNS) في مستوي المستعمل النهائي، ناجمة عن طلبات من المستخدم النهائي، إلى تعطيل السطح البيني للعمليات والإدارة والصيانة والتزويد (OAM&P) في مستوي الإدارة لكي يتمكن مدير الشبكة من تصحيح المشكلة.

ويبين الشكل 7-2.4 معمارية الأمن بما فيها مستويات الأمن. ويتيح مفهوم مستويات الأمن التمييز بين شواغل الأمن المعنية المقترنة بتلك الأنشطة والقدرة على معالجتها بصورة مستقلة. فعلى سبيل المثال، ينبغي في خدمة نقل الصوت باستعمال بروتوكول الإنترنت، والتي تتناولها طبقة أمن الخدمات، أن تكون مهمة ضمان أمن إدارة الخدمة مستقلة عن مهمة ضمان التحكم في الخدمة. وهذه المهمة مستقلة عن مهمة ضمان أمن بيانات المستعمل النهائي التي تقوم الخدمة بنقلها (مثل الخدمات الصوتية للمستعمل).




**الشكل 7-2.4 – مستويات الأمن تعكس الأنماط المختلفة لأنشطة الشبكة**

## 8 الاستراتيجيات الممكنة لحماية الشبكة

يشمل الأمن جميع الطبقات المعمارية في الشبكة. ويوفر هذا النهج نقطة بداية جيدة لتصميم شبكات آمنة. ويمكّن هذا التفكيك طبقة أعلى من تحديد متطلباتها الأمنية الخاصة عند هذه الطبقة المحددة فضلاً عن تمكينها من استخدام خدمات الأمن في المستويات الأدنى. ويتيح نهج الأمن المقسم إلى طبقات وضع حلول أمنية مرنة وقابلة للتعديل من حيث المقياس عبر مستوى الشبكة ومستوى التطبيقات ومستوى الإدارة لجميع المنظمات.

### 1.8 إدارة سياسات العروة المغلقة

تمثل السياسة الأمنية حسنة التصميم والتنفيذ مطلباً مطلقاً لجميع أنماط المؤسسات والمنظمات. وتكون السياسة الأمنية عموماً وثيقة وعملية حية يجري إنفاذها وتنفيذها وتحديثها وفقاً لأحدث التغييرات في البنية التحتية ومتطلبات الخدمة في المؤسسة أو المنظمة.

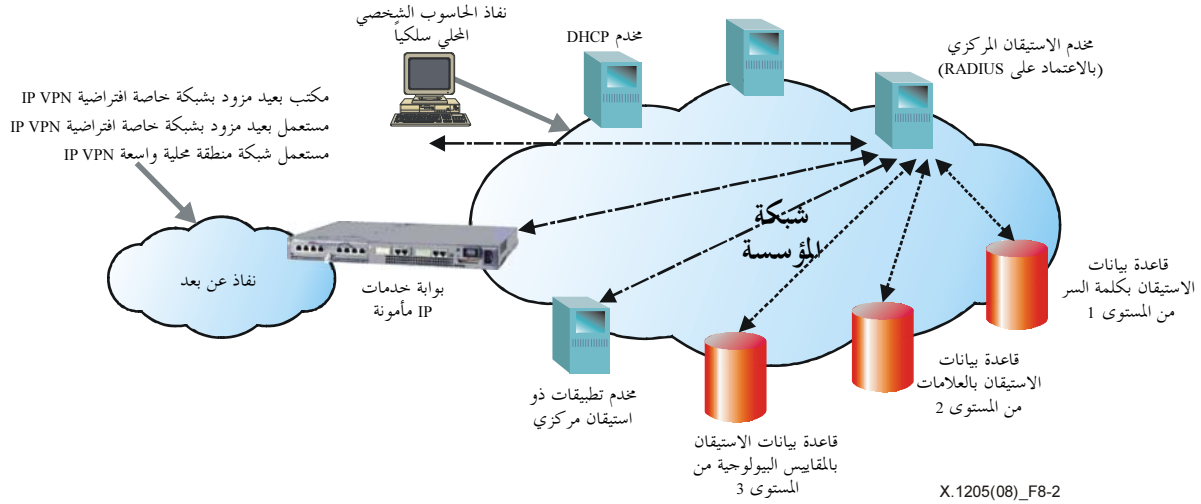
وتحدد السياسة الأمنية بوضوح الموارد في المنظمة (أو المؤسسة) المعرضة للخطر كما تحدد منهجيات التخفيف من التهديدات الناشئة. وتشمل السياسة الأمنية إمكانية تقييم مواطن الضعف والخطر، وتعرّف القواعد الملائمة للتحكم في النفاذ. وتجري عملية تقييم الخطر ومواطن الضعف على جميع مستويات الشبكة. وتكون السياسة قادرة على أن تساعد في التعرف على الانتهاكات الأمنية واكتشافها وأن تحدد الاستجابات المحددة لهذه الانتهاكات.

ويوصى بأن يستخدم القائمون على إدارة تكنولوجيا المعلومات والشبكات أدوات لإجراء تقييم لمواطن الضعف في شبكاتهم. ويتّبع مبدأ النفاذ بأقل الامتيازات. ومن مهام القائمين على إدارة تكنولوجيا المعلومات والشبكات ضمان استعراض سجلات التدقيق ومن ثم إغلاق العروة المتعلقة بإدارة السياسات. وإذا أسفر التدقيق عن مشاكل، يتعين على هؤلاء القائمين ضمان تحديث السياسة لتعكس الإجراءات المعدلة.

والسياسة الأمنية التي لا تنفذ عديمة القيمة. ويعتمد إنفاذ السياسة الأمنية على الناس. وينبغي توضيح المسؤولية والمساءلة فيما يتعلق بإنفاذ السياسات.

## 2.8 إدارة النفاذ الموحد

يستخدم مصطلح إدارة النفاذ لتعريف الأنظمة التي قد تستفيد من كل من خدمات الاستيقان والترخيص للتحكم في استخدام الموارد. والاستيقان هو العملية التي يطلب فيها مستعمل أو كيان تحديد معرّف له في الشبكة. ويحدد الترخيص مستوى الامتيازات التي يتمتع به ذلك الكيان على أساس التحكم في النفاذ. ويستند التحكم في مستوى النفاذ إلى تعريف سياسة التحكم وإنفاذها. ويبين الشكل 8-2 النموذج المرجعي لضمان أمن الاستيقان والترخيص.




**الشكل 8-2 – النموذج المرجعي لضمان أمن الاستيقان والترخيص**

وانطلاقاً من الشكل 8-2 تنبثق التوصيات التالية:

1) استخدام آلية الاستيقان المركزي لتيسير الإدارة والاستغناء عن كلمات سر مختزنة محلياً (تميل كلمات السر المختزنة محلياً إلى أن تكون ساكنة وضعيفة).

2) استخدام نظام الترخيص المركزي، المقترن بصورة وثيقة بنظام الاستيقان، على أساس خشونة فرز ملائمة للمؤسسة المعنية.

3) إنفاذ قواعد كلمات سر قوية (معقدة) بالنسبة لجميع كلمات السر.

4) ضمان تخزين جميع كلمات السر في نسق مجفر (مظلل) في اتجاه واحد.

5) مبدأ البساطة الذي يعني سهولة الاستخدام وسهولة الإدارة. والنظام البسيط نظام مأمون نظراً لزيادة احتمال التقيد بالضوابط.

6) ضمان تسجيل جميع الأحداث ذات الصلة بالأمن فيما يتعلق بالاستيقان والترخيص.

وتشمل أساليب إدارة النفاذ ما يلي: تقنيات ترشيح مصادر بروتوكول الإنترنت وتقنيات التفويض والاعتماد النُهُج. ولكل نهج مزاياه وقيوده. وبحسب نمط المؤسسة، وداخل نمط معين، يمكن استخدام أكثر من نهج أو توليفة من النُهُج. فعلى سبيل المثال، قد تختار المؤسسة إدارة النفاذ لمحطات العمل باستخدام ترشيح مصادر بروتوكول الإنترنت وقد تختار استخدام المخطط القائم على أساس الاعتماد للمستعملين الآخرين.

ويمكن استخدام العديد من الطرائق لاستيقان المستعمل. وتشمل التقنيات: كلمات السر، والنفاذ لمرة واحدة، وتقنيات القياسات البيولوجية، والبطاقات الذكية، والشهادات. وينبغي للاستيقان القائم على كلمات السر أن يستخدم كلمات سر قوية (أي تتكون من ثماني سمات على الأقل من حيث الطول وحرف أبجدي واحد على الأقل وسمة عددية وأخرى خاصة). وقد لا يكفي الاستيقان على أساس كلمات السر فقط، وقد يكون من الضروري، اعتماداً على تقييم مواطن الضعف، الجمع بين الاستيقان على أساس كلمات السر وعمليات الاستيقان والترخيص الأخرى مثل الشهادات وبروتوكول النفاذ للدليل

خفيف الوزن (LDAP) وخدمة الاستيقان عن بعد من المستعمل بالمراقمة (RADIUS) وبروتوكول استيقان الشبكة (Kerberos) والبنية التحتية للمفاتيح العامة (PKI).

وتنطوي جميع آليات الاستيقان على مزايا وعيوب. فالتوليفات بين هوية المستعمل وكلمة السر بسيطة ومنخفضة التكلفة وسهلة الإدارة، إلا أن تذكّر العديد من كلمات السر المعقدة يشكل صعوبة بالغة للمستعملين. وتضيف أنظمة الاستيقان بعاملين وثلاثة عوامل قوة إضافية للاستيقان إلا أنها كلها باهظة التكلفة وتزيد من التعقيد ومن الصعب الحفاظ عليها.

وقد يكون نظام "كلمة السر الوحيدة" مدعوماً بكلمات سر قوية مفروضة حلاً جيداً للاستيقان والترخيص في مؤسسة ما. ويوفر هذا النظام أمن استيقان على درجة عالية، وترخيصاً متمايزاً ومزيداً من سهولة الإدارة. ويجري في إطار هذا النظام تزامن كلمة السر الوحيدة القوية لدى المستعمل مع الكثير من التطبيقات والأنظمة على مستوى المؤسسة بغية الاستيقان والترخيص. وتحيل جميع أنظمة وتطبيقات المؤسسة بصورة أوتوماتية وظائف الاستيقان والترخيص إلى نظام كلمات السر الوحيدة. ونظراً لأنه يتعين على المستعمل أن يتذكر مجرد كلمة سر واحدة قوية، فإن ذلك يجعل النظام بسيط الاستخدام ويستبعد احتمال تجاوزه. وفيما يلي مزايا نظام كلمة السر الأحادية:

- طريقة متساوقة أحادية للاستيقان لوضع كلمات السر.
- طريقة متساوقة أحادية للاستيقان والترخيص.
- طريقة أحادية لتسجيل حسابات المستعمل وإنهائها.
- إنفاذ مبادئ توجيهية لكلمة سر مؤسسية قوية.
- الاتساق – يعرف المستعمل ما عليه أن يفعل.
- التوحيد القياسي – سهولة الدعم والتطبيق.
- سطح بيني معياري سريع وسطوح بينية لبرمجة التطبيقات (API).
- انخفاض التكلفة، انخفاض نداءات طلب المساعدة.

وتواجه المؤسسة المفتوحة والموسعة أضخم التحديات لدى تصميم سياسة إدارة النفاذ فيها. ومن المفيد اعتبار إدارة النفاذ بمثابة عنصر أساسي من عناصر السياسة الأمنية. ولذا يتعين على المنظمات أن تصمم نظاماً موحداً لإدارة النفاذ له قواعد تفصيلية دقيقة ويكون متوائماً مع كل من:

- أدلة وقواعد بيانات خصائص الهوية
- أنظمة استيقان متعددة مثل كلمة السر وبروتوكول استيقان الشبكة (Kerberos) وبروتوكول التحكم في النفاذ (TACACS) وخدمة الاستيقان (RADIUS)
- الكيانات المضيفة والتطبيقات ومخدمات التطبيقات.

وينبغي للنظام الموحد لإدارة النفاذ أن يقوم بإدارة الدورة لكل مستعمل بعد استيقانه. ويوصى باستخدام التشكيل المرن وإنفاذ السياسات على أساس قواعد تفصيلية دقيقة قادرة على التعامل مع مواضيع معينة، وكذلك المراقبة والمحاسبة وسجلات التدقيق المأمونة. كما يوصى باستخدام حسابات وحيدة لكل مدير شبكة مع المساءلة عن الإجراءات التي يمكن عزوها إلى كل فرد.

### 3.8 الاتصالات المأمونة

بوسع الشبكات الموحدة أن تحمل رزم الصوت والبيانات والفيديو. والغرض من تأمين حركة الشبكة هو ضمان السرية وسلامة اتصالات الشبكة ودقتها. وينبغي توافر الأمن لحركة النداءات والتشوير في شبكات المهاتفة. وتستخدم تكنولوجيا التحفير في شبكات الصوت والبيانات والشبكات المتنقلة.

ويمكن تحقيق التحفير من خلال:

- تقنيات الشبكة الخاصة الافتراضية باستخدام أمن بروتوكول الإنترنت مع رأسية استيقان وكبسلة الحمولة النافعة للأمن أو عملية تمرير نفق من خلال استخدام بروتوكول نسق التمرير في الطبقة 2 (L2TP).

- إدارة المفاتيح على أساس تبادل مفاتيح الإنترنت (IKE).
- إدارة الشهادات على أساس البنية التحتية للمفاتيح العامة الواردة في التوصية [ITU-T X.509] (PKIX).
- بروتوكول إدارة الشهادات (CMP) (انظر [b-IETF RFC 2510]) وبروتوكول حالة الشهادات على الخط مباشرة (OCSP) (انظر [b-IETF RFC 4557]).
- عند مستوى طبقة التطبيقات، باستخدام بروتوكول أمن طبقة النقل (TLS) (انظر [b-IETF RFC 4366]) مع مفاتيح قوية.

ومن المهم استخدام المعايير التي تستند إلى خوارزميات التجفير وعمليات الفرم مثل DES و3DES وAES وRSA وDSA (انظر [b-IETF RFC 2828]) وينبغي استخدام MD5 (انظر [b-IETF RFC 1321]) وSHA-1 (انظر [b-IETF RFC 3174]) لضمان سلامة الرسالة وDiffie-Hellman (انظر [b-IETF RFC 2631]) وRSA (انظر [b-IETF RFC 2828]) لتبادل المفتاح.

**ملاحظة** – يشجع المعهد الوطني للمقاييس والتكنولوجيا (NIST) الآن استعمال الخوارزمية SHA-256 (خوارزمية الفرم الآمن مع مفاتيح مشفرة بمقدار 256 بتة) بدلاً من الخوارزمية SHA-1.

وتعرّف الخصوصية المكافئة للخصوصية السلكية (WEP)، على النحو الوارد في المعايير [b-IEEE 802.11]، تقنية لحماية الإرسال عبر الهواء بين نقاط النفاذ لشبكة المنطقة المحلية اللاسلكية وبطاقات السطح البيني للشبكة (NICs). وقد تبين أن هذا البروتوكول غير آمن. وينبغي استخدام تدابير إضافية للحماية، مثل أمن بروتوكول الإنترنت، لضمان أمن شبكة المنطقة المحلية اللاسلكية على أساس الخصوصية المكافئة للخصوصية السلكية. ويمكن بدلاً من ذلك استخدام النفاذ المحمي Wi-Fi زيادة في الحماية.

### 4.8 الأمن متغير العمق

الشبكة المحلية الافتراضية (VLAN) هي مجموعة أجهزة في شبكة ما، مثل المخدِّمات وموارد الشبكة الأخرى، تتشكل بحيث تعمل كما لو كانت موصولة إلى مقطع شبكة وحيد. وتبقى موارد المستعملين الآخرين ومخدِّماتهم في هذه الشبكة غير مرئية من طرف أي مستعمل آخر فيها. وتساعد هذه الشبكات على تلبية احتياجات الأداء من خلال تقطيع الشبكة بصورة فعالة. وتحد هذه الشبكات من انتشار البث الإذاعي كما تحد من الحركة من عقدة إلى عقدة على نحو يتقلص فيه عبء الحركة الخارجية داخل الشبكة بأكملها. وتتيح هذه الشبكات أيضاً لجميع الرزم المنقولة فيما بينها أن تمرَّ في مسيِّر بحيث يمكن استخدام تدابير أمنية قائمة على المسيِّر من شأنها أن تضبط النفاذ إلى مقطع الشبكة.

وتسفر عملية وضع طبقات الأمن عن القدرة على تقديم أمنٍ متغير العمق. فكل مستوى إضافي للأمن يعتمد على مقدرات الطبقة دونه. ويوفر كل مستوى إضافي أمناً أكثر دقة وإحكاماً.

وعلى سبيل المثال، توفر الشبكات المحلية الافتراضية إمكانية تقسيم الشبكة الأساسية إلى مكونات ومقاطع. ويتيح ذلك حصر مختلف وظائف الأعمال وتقطيعها إلى شبكاتها المحلية الخاصة وحدوث حركة متقاطعة من مقاطع أخرى في الشبكة المحلية الافتراضية مشروطة أو ممنوعة. وثمة منافع عديدة من نشر هذه الشبكات في شتى مواقع الشركة. إذ يتيح استخدام "واسمات" الشبكة المحلية مثلاً فرز الحركة إلى فئات معينة مثل الشؤون المالية والموارد البشرية والهندسة. ومن العناصر الهامة في مجال الأمن فصل البيانات دون أي "تسرب" بين الشبكات المحلية.

ويمكن إقامة طبقة ثانية من الأمن من خلال ترشيح جدران الحماية في محيط الشبكة وتلك الموزعة عند نقاط استراتيجية داخل الشبكة. فطبقة جدران الحماية تمكّن من زيادة تقسيم الشبكة إلى مجالات أصغر ومن ضمان توصيلات آمنة إلى الشبكة العمومية. وتحد جدران الحماية نفاذ الحركة الداخلة والخارجة لتلك البروتوكولات التي يتم تشكيلها صراحة داخل جدران الحماية. وعلاوة على ذلك، يمكن توفير مقدرة استيقان المستخدمين الداخلين أو الخارجين. وتمكّن جدران الحماية التي تدعم ترجمة عناوين الشبكة من ترشيد عناوين بروتوكول الإنترنت داخل الشبكة على النحو المحدد في RFC 1918 (توزيع العناوين لشبكات الإنترنت الخاصة).

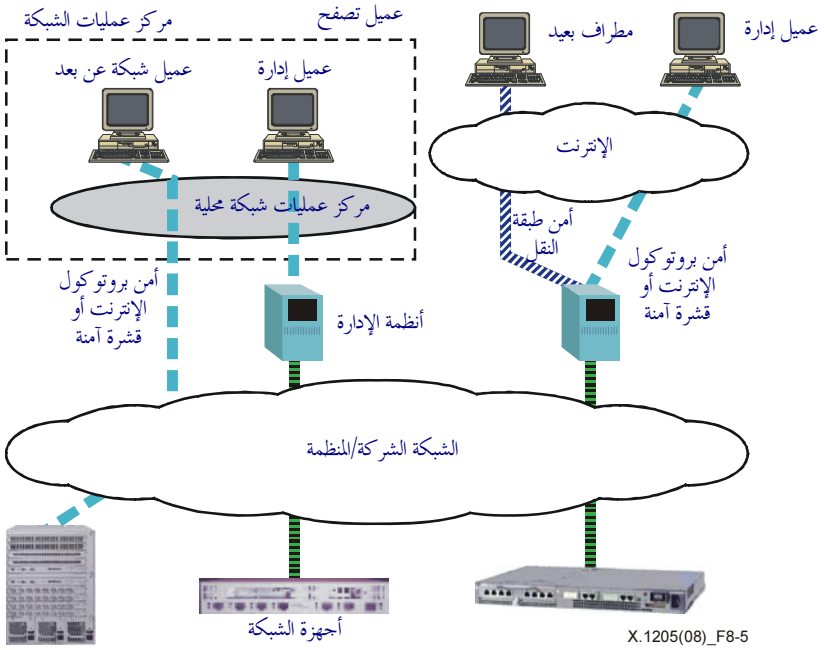
ويوفر استخدام جدران الحماية طبقة إضافية من الحماية مفيدة للتحكم في النفاذ. ويتيح تطبيق النفاذ القائم على أساس السياسات تكييف النفاذ استناداً إلى احتياجات المؤسسة. كذلك فإن استخدام أسلوب جدران الحماية الموزعة يوفر منافع إضافية من حيث قابلية التوسع بتطور احتياجات المؤسسة. ويمكن نشر جدران الحماية الشخصية على الأنظمة الطرفية لضمان سلامة التطبيقات.

ويمكن إضافة الشبكات الخاصة الافتراضية (VPN) من الطبقة 3 باعتبارها الطبقة الثالثة للأمن المعزز. وتوفر هذه الشبكات قدراً أكبر من الدقة في التحكم في نفاذ المستعمل وتمييزه شخصياً. وتوفر هذه الشبكات أيضاً مزيداً من الأمن حتى مستوى المستعمل الفرد وتمكن من تأمين النفاذ عن بعد للمواقع البعيدة وشركاء المؤسسة. ولا حاجة في هذه الشبكات إلى استخدام الخطوط المكرسة. ويوفر استخدام التسيير الديناميي في أنفاق آمنة عبر الإنترنت حلاً على درجة عالية من الأمن يعتمد عليه وقابل للتوسيع. ويتيح استخدام الشبكات الخاصة الافتراضية بالاقتران مع استخدام شبكات المنطقة المحلية الافتراضية وجدران الحماية لمدير الشبكة فرصة قصر نفاذ أي مستعمل أو مجموعة مستعملين استناداً إلى معايير السياسات واحتياجات المؤسسة. وتوفر الشبكة الخاصة الافتراضية ضمانات أقوى لسلامة البيانات وسريتها. ويمكن القيام بتجفير قوي للبيانات في هذه الطبقة لتوفير السرية وسلامة البيانات.

والحلول الأمنية المعتمدة على أسلوب الطبقات حلول مرنة وقابلة للاتساع. والحل قابل للتكيف بحسب الاحتياجات الأمنية للمؤسسة.

## 5.8 ضمان أمن الإدارة

إن قناة أو مستوي الإدارة المأمون، سواء أكانت تمثل "أفضل ممارسة" أم جزءاً أساسياً من معمارية الأمن في منظمة أو مؤسسة ما، تشكل الأساس لجميع العناصر الأخرى في إدارة الشبكة وأدائها وبقائها. ويبين الشكل 5.8 نموذجاً مرجعياً ممكناً لضمان أمن إدارة الشبكة فيما يتعلق بمركز عمليات الشبكة (NOC).




**الشكل 5-8 – نموذج مرجعي لضمان أمن الإدارة**

وأمن الإدارة أسلوب شامل وليس مجرد عنصر معين من عناصر الشبكة. ولذلك، فإن الأسلوب الموصى به في هذه التوصية يغطي المجالات الأساسية في البنية التحتية للشبكة ويوفر إجراءات معينة للتخفيف من الأحداث التي تهدد الشبكة. ويمثل كل من المجالات الواردة أدناه مكوناً حرجاً يتطلب اهتماماً أمنياً لضمان توافر نسيج متماسك من الحماية يحيط بالشبكة.

وهناك تسعة مجالات رئيسية لإدارة الشبكة يتعين معالجتها من جانب الأمن قبل اعتبار مستوي إدارة الشبكة مأموناً وهي:

- تسجيلات نشاط الأمن

- استيقان مشغل الشبكة
- التحكم في النفاذ لمشغلي الشبكة
- تجفير حركة إدارة الشبكة
- أمن نفاذ المشغلين عن بعد
- جدران الحماية
- كشف الاقتحام
- تحصين نظام التشغيل
- البرمجية الخالية من الفيروسات

### 1.5.8 إدارة السياسات

يمكن استخدام السجلات المأمونة في الحفاظ على تتبّع تدقيق أنشطة المستعمل أو مدير الشبكة والأحداث الناشئة عن الجهاز ذاته، وذلك عنصر أساسي في استكمال إدارة السياسات. وتدعى البيانات الخام المجمعة "سجل التدقيق" ويشار إلى مسير الأحداث القابل للتحقق من خلال سجلات التدقيق بأنه "تتبّع التدقيق". ولكي تكون سجلات تدقيق الأمن فعالة، يتعين أن تتضمن معلومات كافية لإجراء التحريات بعد الحدث أو تحليل حوادث الأمن. وتوفر سجلات التدقيق هذه وسيلة لإنجاز الأهداف العديدة ذات الصلة بالأمن، بما في ذلك المساءلة الفردية وإعادة تشكيل الأحداث السابقة وكشف الاقتحام وتحليل المشكلات. كما يمكن استخدام السجلات في إجراء تحليل الاتجاهات طويلة الأجل. فالمعلومات المتضمنة في سجلات التدقيق تساعد في تحديد أصل سبب المشكلة الأمنية ومنع وقوع الحوادث في المستقبل؛ وينبغي حفظ هذه المعلومات بصورة مأمونة. إذ يمكن، على سبيل المثال، أن تساعد سجلات التدقيق في إعادة تصور تسلسل الأحداث الذي أدى إلى المشكلة، مثل نفاذ أحد المقتحمين غير المرخص له إلى موارد النظام أو حدوث عطب في النظام نتيجة لتشكيل غير صحيح أو تنفيذ خاطئ.

### 2.5.8 إدارة النفاذ المأمون

ينبغي أن يستند استيقان مشغل الشبكة إلى استيقان مركزي قوي لمشغلي الشبكات ومديريها. وتمكن الإدارة المركزية لكلمات السر من تعزيز كلمات السر والاستغناء عن التخزين المحلي لكلمات السر على عناصر الشبكة وأنظمة إدارة العناصر. وخدمة الاستيقان عن بعد من مستعمل بالمراقمة (RADIUS) هي الآلية الأساسية المفضلة لأتمتة الاستيقان المركزي.

وينبغي استخدام الممارسات الجيدة للتحكم في النفاذ بالنسبة لمشغلي الشبكات. إذ يمكن لتحديد مستوى الترخيص مثلاً استخدام التقنيات المعتمدة على مخدمات الاستيقان RADIUS لتوفير مستوى أساسي من التحكم في النفاذ؛ وينبغي إضافة مخدم بروتوكول النفاذ LDAP لتوفير قدر أدق من التحكم في النفاذ إذا كان ذلك ضرورياً.

### 3.5.8 تجفير حركة إدارة الشبكة

يوصى بالتجفير في حركة كل البيانات المستخدمة في إدارة الشبكة وذلك لضمان سرية البيانات وسلامتها. ويتزايد استخدام المؤسسات لإدارة الشبكات داخل النطاق ومن ثم يتعين فصل حركة الإدارة باستخدام التجفير. ويكفل تجفير حركة الإدارة درجة عالية من الحماية من العناصر داخل المؤسسة باستثناء المجموعة الصغيرة منها المخولة بالنفاذ المشروع إلى مفاتيح التجفير. وينبغي توفير التجفير فيما بين عملاء مركز عمليات الشبكة (NOC) ومخدمات نظام إدارة العناصر و/أو عناصر الشبكة. ويتضمن ذلك حركة بروتوكول SNMP حيث إن هناك مواطن ضعف معروفة فيما يتعلق بكل من الصيغتين 1 و2 من بروتوكول SNMP، وتمت معالجة هذه المواطن في الصيغة الثالثة من هذا البروتوكول SNMP. وبروتوكولات الأمن التي يتعين استخدامها في هذه الوصلات، تبعاً لنوع الحركة، هي بروتوكول TLS وIPSec والقشرة الآمنة (SSH) (انظر [b-IETF RFC 4252]). والقشرة الآمنة عبارة عن بروتوكول على مستوى التطبيق يحل مباشرة مكان Telnet (انظر [b-IETF RFC 854]) وFTP (انظر [b-IETF RFC 959]) إلا أنه لا يمكن استخدامه عادة لحماية أنواع أخرى من الحركة. ومن ناحية أخرى فإن أمن بروتوكول الإنترنت (IPSec) لا يعمل إلا فيما بين طبقة الشبكة (الطبقة 3) وطبقة النقل (الطبقة 4) ويمكن استخدامه لحماية أي نوع من حركة البيانات بصرف النظر عن التطبيقات

والبروتوكولات المستخدمة. وأمن بروتوكول الإنترنت (IPSec) هو الطريقة المفضلة إلا أنه يمكن استخدام القشرة الآمنة (SSH) إذا كانت الحركة تتألف من شبكة Telnet وبروتوكول FTP فقط. ويمكن لتكنولوجيا TLS أن تحمي حركة HTTP عندما تستخدم في إدارة الشبكة بين عملاء مركز عمليات الشبكة (NOC) ونظام إدارة العناصر (EMS) و/أو عناصر الشبكة. ويمكن استخدام جهاز خارجي للشبكة الخاصة الافتراضية لأمن بروتوكول الإنترنت في مختلف أجزاء الشبكة لضمان أمن حركة الإدارة.

### 4.5.8 النفاذ البعيد المأمون للمشغلين

ينبغي توفير الأمن للمشغلين والمديرين الذين يديرون الشبكة من موقع بعيد عبر شبكة عمومية. وتوفير شبكة خاصة افتراضية مأمونة باستخدام أمن بروتوكول الإنترنت (IPSec) هو الحل المفضل حيث إن ذلك يوفر تخفيراً قوياً ويمكّن من استيقان جميع المشغلين عن بعد. إذ يمكن مثلاً وضع شبكة خاصة افتراضية عند السطح البيني لنظام الإدارة وينبغي تزويد جميع المشغلين بعملاء نفاذ خارجي لحواسيبهم المحمولة أو محطات عملهم.

### 5.5.8 جدران الحماية

من الممارسات الجيدة لتطبيق مبادئ الأمن متغير العمق لتقسيم بيئة إدارة الشبكة من خلال استخدام شبكات المنطقة المحلية الافتراضية وجدران الحماية. فهذه الجدران تتحكم في نوع الحركة (بروتوكول، رقم منفذ، عنوان مصدر أو مقصد) المستخدم لعبور الحدود بين ميادين مجالات الأمن. ويمكن، بحسب نوع جدار الحماية (ترشيح التطبيق إزاء ترشيح الرزم) توسيع ذلك ليشمل ترشيح محتوى التطبيقات من تدفق البيانات. ويتوقف وضع جدار الحماية ونوعها وقواعد الترشيح على التنفيذ الخاص بكل شبكة.

### 6.5.8 كشف الاقتحام

يمكن إدماج أنظمة كشف الاقتحام لدى المضيف في مخدمات الإدارة لتوفير لدرء عمليات اقتحام الشبكة. ويمكن استخدام أنظمة كشف الاقتحام لتحذير مديري الشبكة من احتمال وقوع حادث أمني مثل تهديد مخدم بالضرر أو هجمات رفض الخدمة.

### 7.5.8 طبقة أمن التطبيقات

يوصى بتحصين جميع أنظمة التشغيل المستخدمة في إدارة الشبكة. ولهذه الغاية ينبغي تحصين جميع أنظمة التشغيل المستخدمة في إدارة الشبكة سواء أكانت أنظمة تشغيل لأغراض عامة أم أنظمة تشغيل كامنة تعمل في الوقت الفعلي. وبالنسبة للأنظمة التي لا يتوافر لها دليل تحصين معين، ينبغي الاتصال بصانع نظام التشغيل للحصول على أحدث ترقيعات وإجراءات التحصين.

### 8.5.8 البرمجية الخالية من الفيروسات

لا بد من فحص جميع البرمجيات، سواء أعدت داخل المؤسسة أم حصل عليها من طرف ثالث، والتأكد من خلوها من الفيروسات إلى أقصى حد معقول ممكن. ويتعين تطوير عملية للتحقق من عدم وجود فيروسات تشتمل على مسح لجميع البرمجيات بأداة محددة لكشف الفيروسات قبل إدراج البرمجية في أي منتج.

## 6.8 الأمن متعدد الطبقات عبر التطبيقات والشبكات وإدارة الشبكات

لكل منظمة أو مؤسسة عتبة أمن مختلفة وبنية تحتية تكنولوجية مختلفة. وتمثل التطبيقات العاملة انطلاقاً من الإنترنت مزيداً من المخاطر والتهديدات من زاوية المؤسسة. وقد يكون لتطبيقات الإنترنت أمناً متأصلاً على مستوى التطبيقات. غير أن استخدام وظيفة الأمن التي يمكن أن توفرها الطبقات الدنيا من الشبكة من شأنه أن يعزز أمن هذه التطبيقات.

ويتعين على المؤسسات التي لديها موقعاً في الإنترنت أن تلتزم جانب الحرص الشديد لدى تصميم مواقعها. وتوفر المجموعة [b-IETF RFC 2196] (دليل أمن المواقع) مرجعاً جيداً يناقش أمن المواقع. ويوصى على مستوى التطبيقات باستخدام السياسات الأمنية دقيقة التفاصيل. وينبغي، حيثما أمكن، أن تكون المواضيع قابلة للمعالجة على مستوى معرّفات الموارد الموحدة (URI). ويتعين تعطيل الوظيفة غير المطلوبة. وينبغي، حيثما أمكن، استخدام بروتوكول أمن طبقة النقل (TLS). ويوصى باستخدام بوابات على مستوى التطبيقات والتركيز على توفير درجة قوية من الاستيقان والترخيص. وإذا مكّنت البنية التحتية للأمن ذلك ينبغي ضمان أمن

خدمات البريد الإلكتروني باستخدام تمديدات بريد الإنترنت متعددة الأغراض الآمنة S/MIME (انظر [b-IETF RFC 2311]) أو تقنيات مثل الخصوصية بدرجة معقولة PGP (انظر [b-IETF RFC 1991]).

ويوصى على مستوى طبقة الشبكة، باستخدام التقنيات المشار إليها في الفقرة 7.8 لضمان قدر مقبول من الأمن للمؤسسة. ويتحقق الأمن باستخدام معمارية من طبقات يمكن تكييفها بحسب المتطلبات الأمنية لكل نوع من أنواع المؤسسات. وضمان أمن حركة إدارة الشبكات مطلب أساسي لضمان أمن الشبكة. ويمكن أن يتحقق ذلك بالعمل أولاً على تحصين نظام التشغيل في مواجهة التهديدات المعروفة. وينبغي الاتصال بصانع نظام التشغيل للحصول على أحدث ترقيعات لإجراءات التحصين. وينبغي اتخاذ خطوات للتحقق من أن جميع البرمجيات المركبة خالية من الفيروسات المعروفة. ويفضل تجفير جميع بيانات حركة الإدارة طوال الوقت باستخدام أمن بروتوكول الإنترنت أو بروتوكول أمن طبقة النقل (TLS) لحماية حركة بروتوكول نقل النصوص المترابطة (HTTP). والتجفير ممارسة جيدة يوصى بها إذا كانت الحركة تنتقل إلى خارج شبكة المنطقة المحلية. ويوصى باستخدام بروتوكول SNMPv3 وخدمة RADIUS في التحكم في النفاذ عن بعد لمشغلي الشبكات من خلال آليات التحكم متعددة المستويات التي تشمل استخدام كلمات سر قوية ويفضل إدارة نظام التحكم في النفاذ مركزياً. والسجلات المأمونة عنصر ضروري للتسجيل في حركة إدارة الشبكة.

### 7.8 استمرارية عمل الشبكة حتى أثناء الهجوم

تدعم شبكة المؤسسة، في بيئة اليوم، عمليات حرجة لنجاح المهمة التي تضطلع بها وهي عنصر أساسي في ممارسة الأعمال. ويفترض أن تكون الشبكة مأمونة ويعتمد عليها ومتاحة لشركاء الأعمال في جميع الأوقات.

وهناك العديد من التقنيات التي يمكن أن تستخدم لضمان موثوقية الشبكة. وتضمن الموثوقية التشغيل الصحيح للشبكة عندما يتعطل بعض البرمجيات و/أو المعدات. ولكن عندما يكون أمن الشبكة مهدداً فإن نمط التفكير هو مفهوم الشبكات القادرة على البقاء. فالشبكة القادرة على البقاء هي الشبكة التي تواصل القيام بالقدر الأدنى من الوظائف الأساسية في حينها، حتى أثناء الهجمات. وتتألف الوظائف الأساسية من توفير الخدمات الأساسية في حينها حتى إذا تعذر الوصول إلى أجزاء من الشبكة أو تعطلت نتيجة تعرضها لهجوم.

وينبغي أن يبدأ تصميم الشبكات القابلة للبقاء بتنظيم خدمات الشبكة في فئتين هما الخدمات الأساسية والخدمات غير الأساسية. وتعني قابلية البقاء أن تكون الشبكة قادرة على مقاومة الهجمات. ولا بد من توافر استراتيجية واضحة بشأن كيفية التعامل مع هذه الهجمات والتغلب عليها. وقد يكون هناك، بحسب نوع الهجوم، العديد من استراتيجيات المقاومة والتعرف على الهجمات والتغلب عليها التي ينبغي أن يدرسها مدير الشبكة. والقدرة على التكيف هي إحدى خصائص الشبكة القابلة للبقاء. فعلى سبيل المثال، تستطيع الشبكة أن تعيد تسيير الحركة من مخدم لآخر إذا اكتشف اقتحام أو هجوم على المخدم الأول.

ويتعين، في مرحلة تصميم السياسة الأمنية، تحديد الخدمات الأساسية التي ينبغي أن توفرها الشبكة، حتى أثناء الهجوم. وتحدد هذه المرحلة كيف تقاوم الشبكة أي هجوم وكيف تتغلب عليه وأفضل أسلوب لعودة الأمور إلى نصابها. وينبغي في هذا التحليل مراعاة أنظمة الإدارة والجهات المضيفة والتطبيقات والمسيرات والبدالات، وكلها عناصر نموذجية.

وتتزايد مقاومة الشبكة للهجمات باستخدام آليات التحكم في النفاذ وتعزيز الاستيقان والتجفير. كذلك فإن استخدام ترشيح الرسالة والرزمة وتقطيع الشبكة والمخدم عوامل تعزز من مقاومة الشبكة للهجمات. ويساعد استخدام التقنيات الملائمة لكشف الاقتحام في تحديد الهجوم، كما يمكن استعمال تقنيات التخزين الاحتياطي الملائمة لاستعادة نشاط النظام والشبكة.

# التذييـــل I

# تقنيات المهاجمين

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يستعرض هذا التذييل بإيجاز بعض الهجمات التي تثير قلقاً خاصاً في بيئة تجهيز البيانات وتوصيلها.

## 1.I تصنيف التهديدات الأمنية

يتعين على خبراء تكنولوجيا المعلومات اعتبار شبكتهم بمثابة مورد ينفذ إليه مستعملون لا يمكن، بصفة عامة، الثقة بهم. وهناك العديد من الأدوات والتقنيات والمنهجيات المتوافرة لدى المهاجمين للإضرار بشبكة ما. وبوسع المقتحمين استخدام هذه الأدوات لإطلاق هجمات متعددة المستويات للنفاذ إلى الشبكة. وفي بعض الحالات، يستغل المهاجم موطن ضعف في الأمن ثم يشن هجمات أخرى لاستغلال أجزاء أخرى من الشبكة.

ويصف هذا الفرع التقنيات والأدوات والمنهجيات التي يستخدمها المهاجمون والمقتحمون للإضرار بشبكة ما.

### 1.1.I تهديدات الترخيص

ينتج النفاذ غير المرخص به إلى موارد شبكة عادة عن تشكيل غير صحيح للنظام وعن أخطاء في الاستخدام. ويمكن للمهاجمين النفاذ دون ترخيص من خلال استغلال عدم كفاية استيقان وترخيص المستعملين والمهام المدرجة في أنظمة المؤسسة أو باستغلال ممارسات إهمال من جانب الموظفين (مثل وضع كلمات السر على الشبكة عندما يضطر المستعمل إلى تذكر عدة كلمات سر).

وتشكل بعض الممارسات، مثل سوء تخصيص الحيز المحجوب وتقاسم المزايا بين التطبيقات، مصادر خطيرة لمواطن ضعف الشبكة. ويمكن استخدام هجمات "باب المصيدة" للنفاذ غير المرخص به. فعلى سبيل المثال، يستطيع المهاجمون النفاذ غير المرخص به من خلال تخمين أسماء المستعملين وكلمات السر باستخدام قاموس متواليات شائعة. ويمكن أن يستخلص المهاجمون كلمات السر بوسائل خوارزمية. ويمكن التقاط كلمات السر أثناء العبور إذا أرسلت دون تجفير.

وبعد تخمين اسم المستعمل وكلمة السر المتصلة به، يستطيع المهاجم النفاذ إلى موارد المنظمة. ويعتمد مستوى النفاذ على الامتيازات التي يتمتع بها الحساب الذي تعرض للضرر. كما أن حجم الضرر الذي يمكن أن يلحقه المهاجم بالمنظمة يعتمد على ما يكنّه من نوايا. وفي معظم الحالات، يستخدم المقتحمون الحساب المكشوف في تركيب مدخل خلفي إلى المؤسسة.

وتستخدم بروتوكولات النفاذ عن بعد للبريد الإلكتروني مثل MAP وPOP3 وPOP2 أسماء مستعملين بسيطة وتقنيات استيقان لكلمة السر. ولذا يمكن للمهاجمين استخدام هذه البروتوكولات في الهجمات الكاسحة. وثمة طرائق منشورة تتيح للمهاجمين استغلال خدمات هذه البروتوكولات عن بعد.

وهناك وسائل أكثر تعقيداً للنفاذ غير المرخص به. فيمكن استخدام الديدان (worms) للقيام بهجمات احتيال على النظام حيث يتنكر أحد مكونات النظام في هيئة مكون آخر. فعلى سبيل المثال، بوسع هذه الديدان أن تستغل التدفقات في خيار إزالة أخطاء الرسائل المرسلة، وفي ملفات الاستضافة (مثل المستخدمة في UNIX) نتيجة لضعف الاستيقان. ويمكن إبطال خيار إزالة الأخطاء من الرسائل المرسلة. ويعتبر ترك هذا الخيار ناشطاً مثالاً على موطن ضعف في الاستعمال.

### 2.1.I الاحتيال على بروتوكول الإنترنت

يعتبر الاحتيال على بروتوكول الإنترنت هجوماً معقداً يستغل علاقات الثقة. إذ ينتحل المهاجم، باستعمال تقنيات التنكر، خصائص هوية مضيف لتعطيل أمن المضيف المستهدف الذي يظن أنه يجري محادثة مع مضيف موثوق به.

وفي هذا الهجوم يحدد المهاجم أولاً المضيف الموثوق به الذي سينتحل هويته. ويمكن تحقيق ذلك أولاً من خلال تحديد أنماط الثقة للمضيف. ويتناول ذلك عادة تحديد طائفة عناوين بروتوكول الإنترنت التي يثق فيها المضيف. وتكون الخطوة التالية تعطيل المضيف، حيث إن المهاجم سوف ينتحل خصائص هويته. ويمكن تحقيق ذلك باستخدام بعض التقنيات مثل تزامن هجمات بروتوكول التحكم في الإرسال TCP العارمة.

وقد تنجح هجمات الاحتيال على بروتوكول الإنترنت لأن من السهل تزييف عناوين البروتوكول ولأن تقنيات استيقان العناوين المعتمدة على الشبكة تخضع لقيود. وهجمات الاحتيال على بروتوكول الإنترنت هجمات طائشة لأن المهاجم قد لا ينفذ إلى ردود المضيف المستهدف. غير أن بوسع المهاجم أن يحصل على اتصالات ثنائية الاتجاه إذا تم التلاعب بجداول التسيير لاستخدام عنوان بروتوكول الإنترنت الخاص بالمصدر الذي تعرض للاحتيال. وتستخدم هجمات الاحتيال على بروتوكول الإنترنت في كثير من الأحيان كخطوة أولى نحو شن هجمات أخرى مثل هجمات منع الخدمة والهجمات العارمة.

وجدير بالملاحظة أن معظم موردي خدمة الإنترنت (ولكن ليس جميعهم بالتأكيد) والكثير من شبكات المؤسسات المسؤولة يقومون حالياً بترشيح العناوين المرسلة مما يستبعد حصول هجمات احتيال على بروتوكول الإنترنت المباشرة. ورداً على ذلك، يعكف المهاجمون على تجميع "شبكات الانتحال" (bot nets) للاحتفاظ بسرية هوياتهم.

### 3.1.I كاشف الشبكات

صمم كاشف الشبكات في الأصل كأداة تمكّن مديري الشبكات من تشخيص المشاكل أو أداء عمليات التحليل أو تحسين أداء شبكاتهم. وتعمل كاشفات الشبكات في مقطع من الشبكة غير محوّل مثل المقاطع الموصولة من خلال مركز محوري. وبهذه الطريقة يمكن للكاشف أن يرى كل الحركة التي تمر في ذلك المقطع.

وكانت الكاشفات القديمة تقرأ رأسيات الرزم الخاصة بحركة الشبكة وتركز على تحديد خصائص الرزم منخفضة المستوى مثل عنوان المصدر والمقصد. غير أن بوسع الكاشفات الحالية أن تفك شفرة البيانات من الرزم عبر جميع طبقات نموذج التوصيل ما بين الأنظمة المفتوحة (OSI).

ويمكن للمهاجمين استخدام الكاشفات لرؤية معلومات المستخدم وكلمات السر الخاصة به من رزم تمر عبر شبكات عامة أو خاصة. وبوسع المهاجمين، باستخدام الكاشفات، الحصول على معلومات قيمة عن أسماء المستعملين وكلمات سرهم، على وجه الخصوص من بعض التطبيقات مثل بروتوكول نقل الملفات (FTP)، وشبكة الاتصالات وغير ذلك من الشبكات التي ترسل كلمات السر دون تجفير. وتستخدم البروتوكولات الخاصة بالنفاذ عن بعد للبريد الإلكتروني مثل IMAP وPOP3 وPOP2 أسماء مستعملين وتقنيات استيقان لكلمات السر تتسم بالبساطة كما أنها عرضة لهجمات الكاشفات.

ونظراً لأن المستعملين يميلون إلى إعادة استخدام كلمات السر عبر تطبيقات ومنصات متعددة، يستطيع المهاجمون استخدام هذه المعلومات للنفاذ إلى مختلف الموارد المتوافرة على الشبكة حيث يمكن النيل من سريتها. وعلاوة على ذلك، يمكن أيضاً استخدام هذه الموارد بمثابة منصات لإطلاق هجمات أخرى.

ويستطيع المهاجمون عموماً استخدام كاشفات الشبكات من خلال اختراق الأمن المادي للمؤسسة، كما لو تمكن أحد من دخول المؤسسة فعلاً وتوصيل جهازه المتنقل في الشبكة. وتنطبق نفس هذه المخاطر على الشبكات اللاسلكية حيث يستطيع شخص يقف في موقف السيارات أن يحصل على النفاذ إلى الشبكة المحلية للمؤسسة. ويتيح النفاذ إلى شبكة الرزم الأساسية للمهاجم أن يعرف تشكيلات وطرائق التشغيل لمواصلة الاستغلال.

### 4.1.I منع الخدمة

تركز هجمات منع الخدمة على حرمان المستعملين الشرعيين من القدرة على استخدام الخدمة. ومن السهل شن هجمات منع الخدمة التي يمكن أن تحدث أضراراً بالغة. فبوسع هذه الهجمات أن توقف عمل المؤسسة وتفصلها فعلياً عن بقية العالم. وتستخدم هجمات منع الخدمة الموزعة موارد أكثر من آلة لإطلاق هجمات منع الخدمة المتزامنة على مورد ما.

ويمكن أن تتخذ هجمات منع الخدمة أشكالاً مختلفة وأن تستهدف طائفة من الخدمات. وتركز هذه الهجمات على إنهاك موارد الشبكة والمخدمات والمضيف والتطبيقات. وتركز بعض هذه الهجمات على وقف توصيلية الشبكة. إذ يستخدم الهجوم العارم المتزامن مثلاً طلبات توصيل زائفة ببروتوكول TCP نصف المفتوح تنهك سعة ذاكرة مورد المستهدف. ويمكن أن تحرم هذه الأنماط من الهجمات المستعملين الشرعيين من النفاذ إلى موارد المضيفين وتطبيقات الويب وغير ذلك من موارد الشبكة. ويمكن أن تتمثل هذه الهجمات في:

- منع توصيلية الشبكة إلى الإنترنت
- منع توفر عناصر الشبكة للمستعملين الشرعيين
- منع توفر التطبيقات للمستعملين الشرعيين

وتستغل هجمات منع الخدمة جوانب الضعف في معمارية النظام الذي يتعرض للهجوم. وفي بعض الحالات، تستغل ضعف الكثير من بروتوكولات الإنترنت المشتركة مثل بروتوكول رسالة التحكم في الإنترنت (ICMP). فعلى سبيل المثال ترسل بعض الهجمات عدداً كبيراً من رزم صدى بروتوكول رسالة التحكم في الإنترنت إلى عنوان بث في بروتوكول الإنترنت. وتستخدم الرزم عنواناً مزيفاً في هذا البروتوكول لهدف محتمل. ويمكن أن تسبب الردود العائدة إلى الهدف في إصابته بالشلل. ويطلق على هذا النوع من الهجمات اسم "SMURF". ويستخدم شكل آخر من الهجمات رزم بروتوكول بيانات المستعمل UDP إلا أنه يعمل على أساس نفس المفهوم.

### 5.1.I هجمات الاعتراض الوسيط

تعرف هجمات الاعتراض الوسيط أيضاً باسم هجمات الوسيط. وفي هذا النوع من الهجمات، يعترض المهاجم الرسائل عند تبادل المفاتيح العمومية بين المخدم والعميل. ويقوم المهاجم بإعادة إرسال الرسائل مستبدلاً مفتاحه العمومي بالمفتاح المطلوب. وعندئذ يظن الطرفان الأصليان أنهما يتصلان بعضهما بالآخر. وقد ينفذ المهاجم فقط إلى الرسائل أو قد يعدلها. ويمكن استخدام كاشفات الشبكات لإطلاق هذه الهجمات.

### 6.1.I شراك الأبواب الخلفية

الأبواب الخلفية من الطرائق السريعة للنفاذ إلى موارد الشبكة في الأحوال التالية:

- توضع عن قصد بواسطة مطوري النظام لإتاحة النفاذ السريع أثناء عملية التطوير، إلا أنها لم تبطل لدى التسليم
- يضعها الموظفون لتيسير أدائهم لوظائفهم
- تكون جزءاً من تركيبات نظام تشغيل معياري لم يتم إلغاؤها بالتحصين، مثل هوية تسجيل المستخدم بالتغيب وتوليفات كلمات السر
- يضعها موظفون ساخطون لإتاحة النفاذ بعد انتهاء خدمتهم
- استحدثت باستعمال شفرة مؤذية، مثل الفيروسات

### 7.1.I التنكر

ينطوي ذلك على إدعاء المهاجم بأنه موظف صيانة أو هندسة حقاً لكي ينفذ إلى الشبكة، وهو فاتحة طائفة من التهديدات التي تستغل ثغرات الأمن المادي ومواطن الضعف البشري. فعلى سبيل المثال، يستطيع المقتحم أن يعدل البيانات ذات الصلة بإدارة التشكيل وطبقات التشوير في الشبكة فضلاً عن بيانات الفوترة والاستخدام.

### 8.1.I هجمات التكرار

تقع هذه الهجمات عندما يتم تكرار رسالة أو جزء من رسالة لإحداث تأثير غير مرخص به. فعلى سبيل المثال، يرد أحد الكيانات برسالة صحيحة تتضمن معلومات لتمكين الاستيقان منه.

### 9.1.I تعديل الرسائل

يحدث تعديل الرسائل عندما يتم خلسة تغيير محتوى بيانات مرسلة ويسفر هذا التعديل عن تأثير غير مرخص به.

### 10.1.I الهجمات الداخلية

تقع الهجمات الداخلية عندما يتصرف المستعملون الشرعيون للنظام بطريقة غير مقصودة أو غير مرخص بها. ويقع الكثير من الجرائم الحاسوبية المعروفة على يد عناصر داخلية تعرض للخطر أمن النظام. ولذا فإن المسح الدقيق للموظفين والفحص المستمر للمعدات والبرمجيات والسياسات الأمنية عوامل تساعد في الحد من مخاطر الهجمات الداخلية. كذلك فإن سجلات التدقيق الجيدة لزيادة احتمال الكشف عن هذه الهجمات تعتبر من الممارسات الجيدة التي ينبغي اتباعها.

## 2.I تهديدات الأمن

تواجه جميع أنماط المنظمات ومنها المؤسسات التجارية طائفة عريضة من التهديدات. وتعتبر الاحتياجات الأمنية والاستراتيجية الأمنية الموصى بها لكل منظمة ذات طابع فريد ومختلف. والمؤسسة المفتوحة هي أكثر البيئات احتياجاً من زاوية الأمن. وفي هذه الحالة، يتعين معالجة الاحتياجات الأمنية عبر المؤسسة للتحكم في نفاذ الموظفين والشركاء بل وحتى العملاء إلى قواعد البيانات والتطبيقات ذات الصلة بالمؤسسة.

### 1.2.I الهجمات على طبقة التطبيقات

يمكن أن تتخذ الهجمات على طبقة التطبيقات أشكالاً مختلفة وتستخدم طرائق عديدة. ونظراً لأن الجهات المضيفة للويب قابلة للنفاذ من جانب الجمهور عموماً عند عناوين منافذ معروفة، على النحو المحدد في بروتوكولات مثل HTTP (المنفذ 80) يمكن للمقتحمين استخدام هذه المعرفة في إطلاق هجمات قادرة على تجاوز جدران الحماية.

وتستغل الهجمات على طبقة التطبيقات مواطن الضعف في نظام التشغيل والتطبيقات للنفاذ إلى الموارد. ويمكن أن يؤدي التشكيل والاستيقان غير السليمين إلى حدوث ثغرات أمنية. فعلى سبيل المثال قد يكون المضيف مخدم ويب، وينبغي أن يزود كل فرد بصفحات الويب المطلوبة. وقد تملي السياسة الأمنية أن على الجهات المضيفة أن تقصر أوامر النفاذ عبر القشرة على المديرين المرخص لهم بذلك.

ويستهدف جمع أسماء الحسابات عملية الاستيقان عندما يطلب أحد التطبيقات هوية تسجيل المستعمل وكلمة السر الخاصة به. والتطبيقات التي تسفر عن رسائل خطأ مختلفة عندما تجد هوية تسجيل المستعمل خاطئة وكلمة السر خاطئة معرضة لهذا النمط من الهجوم. واستناداً إلى نمط رسالة الخطأ، يمكن أن يكيف المقتحم هجوماً يحدد أولاً هوية تسجيل صحيحة لمستعمل ما ثم يستخدم أشكالاً أخرى من تقنيات اقتحام كلمة السر للحصول على كلمة السر المطلوبة.

ويمكن أن تستند الهجمات في طبقة التطبيقات إلى الفيروسات والديدان وإغراق حيز التخزين المؤقت وتجميع كلمات السر من بين تقنيات أخرى. ولم يؤد استحداث خدمات الويب وتكنولوجيات التسجيل وحيدة المرة إلا إلى تفاقم المشكلة حيث إنها تميل إلى تمكين التطبيقات التقليدية في شبكة الويب. وعندما صممت هذه التطبيقات لم تأخذ توصيلية الويب والأمن في الحسبان.

وتستهدف بعض الهجمات في طبقة التطبيقات مجرد تفكيك موقع الويب. ويستهدف البعض الآخر منها تسميم ملفات زوار موقع الويب للحصول بصورة غير مشروعة على معلومات عن مخدم معين. ولا تتحقق التطبيقات عموماً من سلامة ملفات الزوار، وقد تصبح ضحية لتنفيذ شفرة مؤذية مخبأة في ملفات الزوار. وهناك مواطن ضعف معروفة في المتصفحات الحالية التي تمكن من الهجمات المعتمدة على هذه الملفات.

كذلك يمكن للمهاجم أن يستخدم تقنيات كتابة البيانات عبر المواقع لإدراج شفرة مؤذية في شكل واسمة بيانات مكتوبة تضاف إلى محدد موقع الموارد المشترك (URL). وسوف تنفذ الشفرة عندما ينقر مستعمل غير مشتبه به على المحدّد URL. ويمكن أن يحل استخدام بروتوكول TLS بعض المشاكل المتعلقة بالأمن في طبقة التطبيقات. غير أن طبقة المقبس الآمن (SSL)

لا تحمي تطبيقات الويب بالكامل. ويظل في الإمكان شن هجمات مثل جمع أسماء الحسابات وكسر كلمات السر حتى في حالة استخدام طبقة SSL.

ويُوصى، للحد من الهجمات التي تهدد طبقة التطبيقات، تحصين جميع أنظمة التشغيل المستخدمة في إدارة شبكة سواء أكانت أنظمة تشغيل للأغراض العامة أم أنظمة تشغيل مبيّتة تعمل في الوقت الفعلي. وينبغي اتباع أدلة تحصين محددة ومحدّثة متوفرة لدى الصانع. وبالنسبة لبعض الأنظمة الموروثة التي تستخدم أنظمة تشغيل قديمة، قد لا تتوفر أي ترقيعات أمنية من الصانع. كما يوصى باستخدام بريد إلكتروني مأمون، وجدران حماية لطبقة التطبيقات، وأنظمة للوقاية من اقتحام المضيف والكشف عن هذا الاقتحام، وتقنيات استيقان قوية وكلمات سر قوية وتحكم ملائم في الخروج في مواقع الويب للحيلولة دون عرض تعديلات من محتوى الويب غير مرخص بها.

### 2.2.I التهديدات التي تتعرض لها طبقة الشبكة

قد يستخدم المهاجم أدوات المهنة لشن هجمات على طبقة الشبكة على درجات مختلفة من الشدة. والمؤسسة الموسعة والمفتوحة معرضة بصورة خاصة للهجمات في طبقة الشبكة، وثمة عدد من التهديدات الأمنية الجسيمة ترتبط عادة بالبنية التحتية للشبكة. وتشمل هذه التهديدات التعطيل والتخريب والعبث بتشكيل الأنظمة ومنع الخدمة والاحتيال والتجسس الصناعي وسرقة الخدمة. ويمكن شن هجمات من داخل الشبكة على يد أفراد في المؤسسة ومن مصادر خارجية مثل المقتحمين.

وتبين التطورات الحديثة في مجال تكنولوجيا الاقتحام، مثل ماسحات المنافذ المعتمدة على المطاريف المتنقلة، أن من الممكن أن تنشأ الهجمات على البنية التحتية للشبكة من مطراف متنقل كذلك. ولذلك يوصى بوضع سياسة أمنية جيدة وعملية أمنية حسنة الفهم لحماية البنية التحتية للشبكة. ومن الأصول التي تستحق الحماية: البدالات والمسيّرات ونقاط النفاذ ومخدمات النفاذ عن بعد ونقاط النفاذ اللاسلكية والجهات المضيفة والموارد الأخرى.

وفيما يلي التهديدات ومواطن الضعف في البنية التحتية للشبكة والتي تتسم بها عادة شبكات رزم بروتوكول الإنترنت:

1) انتشار بروتوكولات غير آمنة: ما زالت بعض الشبكات تستخدم بروتوكولات من المعروف أنها تعاني مواطن ضعف من ناحية الأمن. وتشمل هذه البروتوكولات: ICMP وTELNET وSNMPv1&2 وDHCP وTFTP وRIPv1 وNTP وDNS وHTTP.

2) استخدام كلمات سر ساكنة وضعيفة تدار محلياً: ما زالت بعض الشبكات تسمح باستخدام كلمات سر ضعيفة تستند إلى كلمات قصيرة شائعة في القواميس يمكن تخمينها بسهولة. وقد يستخدم بعض مديري الشبكات كلمة سر واحدة عبر عناصر الشبكة والتي يمكن تقاسمها وتكون معروفة لجميع مديري الشبكة.

3) معلومات أمن غير محمية: في بعض الشبكات لا يجري تجفير المعلومات الحرجة مثل ملفات كلمات السر. ويجري إرسال معلومات أخرى مثل كلمات السر دون تجفير عبر الشبكة. وقد وضعت مجموعة قواعد جدران الحماية بصورة غير ملائمة واستخدمت مفاتيح تجفير ضعيفة.

4) تحميل برمجيات وملفات تشكيل غير مستيقنة: يمكن أن تأتي التهديدات التي تتعرض لها الشبكة من تحميل برمجيات أو ملفات تشكيل غير صحيحة أو مؤذية يمكن أن تتسبب في فقدان الخدمة، وقد تؤدي إلى سوء الأداء. وتؤدي هذه الممارسة إلى فتح ثغرات أمنية مثل إدخال "أحصنة طروادة" أو غير ذلك من الشفرات المؤذية بواسطة عناصر داخلية أو خارجية. كما تؤدي الممارسة إلى تشكيلات غير صحيحة في الأجهزة.

5) عناصر شبكة وأنظمة تشغيل غير محصنة: يمكن أن تنشأ التهديدات من تحميل أنظمة تشغيل بالتغيب من المصنع غير محصنة ضد الهجمات الشائعة. ويشمل ذلك تشغيل خدمات غير ضرورية وترك حسابات وكلمات السر بالتغيب ممكّنة.

6) منافذ وسطوح بينية للإدارة معرضة دون داع للشبكة العمومية: يمكن أن تنشأ التهديدات التي تتعرض لها الشبكات من السطوح البينية للإدارة داخل النطاق التي تبقى قابلة للنفاذ من الإنترنت العمومية. ويمكن أن تنشأ تهديدات

إضافية من سوء استخدام آلية الدعم مثل النفاذ إلى الشبكة الأساسية بأسلوب الدعم عن طريق المراقمة أو الشبكة ISDN أو توصيلات أخرى.

### 3.2.I النفاذ دون ترخيص

النفاذ دون ترخيص تعبير يشير إلى عدد من مختلف أشكال الهجمات. والهدف النهائي للمهاجم هو الحصول على النفاذ إلى بعض الموارد بصورة غير مشروعة. ويمثل ذلك مشكلة أمنية لجميع أنماط المؤسسات. فأي مؤسسة تمكّن النفاذ إلى الإنترنت أو النفاذ عن بعد إلى شبكة المنطقة المحلية معرضة لهجمات النفاذ دون ترخيص.

فيمكن لخدمات النفاذ عن بعد التي تمكّن الموظفين المسافرين من المراقمة للنفاذ إلى البريد الإلكتروني، والمكاتب البعيدة الموصولة من خلال خطوط المراقمة، وشبكات الإنترانت وشبكات الإكسترانت التي تربط الأطراف الخارجية بشبكة المؤسسة، أن تتسبب جميعها في تعريض الشبكة للمقتحمين والفيروسات وغير ذلك من الهجمات. ويمكن أن يستخدم المقتحمون أدوات المهنة في النفاذ إلى شبكة المؤسسة حيث قد تتعرض المعلومات الحساسة للخطر أو تستخدم في شن هجمات ضد شبكات أخرى.

وقد تساعد حماية الشبكة على مختلف المستويات في منع النفاذ غير المرخص به. ويمكن على مستوى طبقة الشبكة أن يضيف استخدام جدران الحماية والمخدمات بالتفويض والترشيح "من المستخدم إلى الدورة" حماية إضافية، إلا أنه يبدو أن المقتحمين يزدادون دهاءً طيلة الوقت. كما يمكن أن يقلل استخدام التحكم في نفاذ المستخدم على مستوى الشبكة والتطبيقات مع الاستيقان والترخيص الملائمين إلى أدنى حد ممكن من مخاطر النفاذ غير المرخص به.

### 4.2.I التنصت

التنصت تهديد يصعب اكتشافه. فهدف المهاجم هنا هو ترصد البيانات الخام في شبكة المنطقة المحلية للمؤسسة وتسجيلها بدقة. ويستخدم التنصت "أسلوب الاختلاط" لمكيفات الإثرنت الجاهزة التي تباع في الأسواق. وتتيح هذه الطريقة للمهاجم الاستيلاء على كل رزمة على الشبكة. وهناك اليوم الكثير من كاشفات الشبكات المجانية على الويب التي يمكن أن يستخدمها المهاجم في التنصت.

وأي نمط من المؤسسات يسمح بالنفاذ عن بعد معرض لهذا الهجوم. وتتعرض المؤسسات المفتوحة والموسعة لأعلى مستويات المخاطر. وتنتفي فعالية بدالة الإثرنت بالكامل أمام أخطار التنصت، حيث إن من الممكن أن يؤدي الاحتيال على ARP إلى إفساد آلية البدالة. ولن يتم عرقلة سوى "التنصت البطيء" بواسطة بدالة الإثرنت. ويمكن أن يقلل استخدام تقنيات إدارة النفاذ القوية والتجفير إلى أدنى حد ممكن من أخطار هذه الهجمات.

# التذييـــل II

# مجالات تكنولوجيا الأمن السيبراني

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

إن درجة تطور وفعالية تكنولوجيا الهجوم تتزايد دائماً. إذ يستطيع المقتحمون هذه الأيام إعداد هجمات بسرعة لاستغلال جوانب ضعف تكتشف في المنتجات. وبوسع المهاجمين أتمتة هذه الهجمات وتيسيرها لاستخدامات الجمهور العريض.

وترد أمثلة على مجالات التكنولوجيات المتيسرة لمكافحة المخاطر السيبرانية في الجدول 1.II.

**الجدول 1.II – تكنولوجيات الأمن السيبراني**

| التقنيات | الفئة | التكنولوجيا | الغرض |
|---|---|---|---|
| التجفير | معمارية الشهادة والمفتاح العام | توقيعات رقمية | تستخدم للتمكين من إصدار وحفظ الشهادات التي تستخدم رقمياً |
| | | التجفير | تستخدم التجفير البيانات خلال الإرسال أو الحفظ |
| | | مبادلة المفتاح | تحدد إما مفتاح الدورة أو مفتاح المعاملة الذي يستخدم لضمان أمن توصيلية ما |
| | الضمان | التجفير | ضمان أصالة البيانات |
| التحكم في النفاذ | حماية المحيط | جدران الحماية | التحكم في النفاذ إلى الشبكة ومنها |
| | | إدارة المحتوى | رصد الحركة بالنسبة للمعلومات غير المتطابقة |
| | الاستيقان | المقاييس البيولوجية | تستخدم الخصائص البشرية مثل بصمة اليد في التحقق من هوية المستخدم |
| | | عامل وحيد | نظام يستخدم هوية المستخدم/كلمة السر للتحقق من معرف الهوية |
| | | عاملان | نظام يتطلب توافر مكونين لمنح المستخدم النفاذ إلى النظام مثل امتلاك علامة مادية بالإضافة إلى معرفة أحد الأسرار. |
| | | ثلاثة عوامل | يضيف عامل تعريف آخر مثل مقياس بيولوجي أو مقياس خصائص في الجسم البشري |
| | | العلامات الذكية | تحدد معرفات هوية موثوقة للمستخدمين من خلال دائرة محددة في الجهاز مثل بطاقة ذكية |
| | الترخيص | اعتماداً على الدور | آليات ترخيص تتحكم في نفاذ المستخدم إلى موارد نظام ملائمة استناداً إلى الدور المسند له |
| | | اعتماداً على القاعدة | آليات ترخيص تتحكم في نفاذ المستخدم إلى موارد النظام الملائمة استناداً إلى قواعد محددة مصاحبة لكل مستخدم بصورة مستقلة عن دورها داخل المنظمة |
| سلامة النظام | مضاد للفيروسات | طرائق التوقيع | الحماية من شفرة الحاسوب الخبيثة مثل الفيروسات والفيروسات المتسللة والفيروسات المتخفية باستخدام توقيعاتها الشفرية |
| | | طرائق السلوك | التحقق من البرامج الدائرة بحثاً عن سلوك غير مرخص به |
| | السلامة | رصد الاقتحام | يمكن استخدامه لتحذير مديري الشبكات من احتمال وجود حوادث أمنية مثل حدوث أضرار بملفات على المخدم |

**الجدول 1.II – تكنولوجيات الأمن السيبراني**

| التقنيات | الفئة | التكنولوجيا | الغرض |
|---|---|---|---|
| التدقيق والرصد | الكشف | كشف الاقتحام | مقارنة حركة الشبكة ومداخل تسجيل المضيف لمقارنة توقيعات البيانات التي تشير إلى المبرمجين العابثين |
| | المنع | منع الاقتحام | رصد الهجمات على الشبكة واتخاذ إجراءات على النحو الذي تحدده المنظمة للتخفيف من الهجمات. وتطلق الأنشطة المشبوهة إنذارات المدير وغير ذلك من الاستجابات القابلة للتشكيل |
| | التسجيل | أدوات التسجيل | رصد ومقارنة حركة الشبكة ومداخل تسجيل المضيف لمضاهاة توقيعات البيانات وملامح عنوان المضيف مما يشير إلى المبرمجين المقتحمين |
| الإدارة | إدارة الشبكة | إدارة التشكيل | تتيح التحكم في الشبكات وتشكيلها والإدارة بالتغيب |
| | | إدارة الرقعة | تركيب آخر المحدثات والروابط مع أجهزة الشبكة |
| | السياسة | الإنفاذ | تتيح للمديرين رصد وإنفاذ السياسات الأمنية |

## 1.II التجفير

التجفير هو عملية تطبيق التحويلات على البيانات الواضحة لتجفيرها إلى شفرة سرية. ويمكن أن يؤدي فك شفرة البيانات السرية إلى استرجاع النص الواضح الأصلي. ويمكن استخدام تقنيات التجفير المتيسرة حالياً لتشفير وفك شفرة البيانات. كما يمكن استخدامها للاستيقان من منشأ رسالة وعدم الإنكار.

ويضطلع التجفير بدور هام في حماية المعلومات أثناء حفظها داخل الجهاز أو وسيط تخزين وخلال إرسالها عبر وصلة اتصالات.

وتعرف مهمة تشفير البيانات في شفرة سرية من خلال استخدام خوارزميات رياضية في التجفير بأنها تجفير البيانات. ومن ناحية أخرى فإن فك تجفير البيانات يؤدي مهمة عكسية مثل تلك التي تحدث عندما تطبق على بيانات مجفرة حيث تعيد إنتاج البيانات الأصلية. ويستخدم التفجير مفاتيح سرية لأداء التجفير وعمليات فك التجفير.

ويمكن تقسيم تقنيات التجفير إلى نمطين أساسيين: مفتاح تناظري ومفتاح لا تناظري.

1) يستخدم تجفير المفتاح التناظري خوارزميات يتماثل فيها مفتاح التشفير ومفتاح فك التشفير. ويعتمد أمن النموذج على صعوبة تخمين المفتاح. ولا بد لأطراف الاتصال من الاتفاق على مفتاح والاحتفاظ بهذا المفتاح بصورة سرية بعيداً عن الآخرين. وتشمل الأمثلة على خوارزمية المفتاح التناظري معيار التجفير الثلاثي (3DES) ومعيار التجفير المتقدم (AES).

2) ويستخدم تجفير المفتاح اللاتناظري خوارزميات تستخدم مفتاحاً لتجفير البيانات ومفتاحاً آخر لفك تجفير النص المشفر. وفي هذا النمط من التجفير، يكون للمستخدم مفتاح خاص لا يعرفه إلا المستخدم ومفتاح عام يمكن أن يعرفه الآخرون. ويستخدم المفتاح العام بواسطة الآخرين لتشفير النص الواضح. ولن يتمكن سوى الحائز على المفتاح الخاص المقابل من فك تجفير النص المشفر.

وتقنيات تجفير المفتاح التناظري أسرع، عموماً، في الحساب من التقنيات اللاتناظرية. غير أن التعقيد الرئيسي في تجفير المفتاح التناظري يكمن في مشكلة توزيع المفتاح. ولذا فإنها لا تناسب عادة التوزيعات الكبيرة. ومن ناحية أخرى فإن تجفير المفتاح اللاتناظري (المعروف أيضاً بتجفير المفتاح العام) يحل بعض قيود إدارة المفتاح الموجودة في تجفير المفتاح التناظري. ويعتمد تجفير المفتاح العام على استخدام الشهادات الرقمية لحل مشاكل إدارة المفاتيح العامة وإزالتها. وسعياً إلى تحسين السرعة الحاسوبية، يمكن استخدام تقنيات تجفير المفتاح العام كوسيلة للمبادلة بطريقة مأمونة المفتاح التناظري للاستخدام في دورة أو في معاملة.

وتعتبر التوقيعات الرقمية مثالاً على التنفيذ العملي لتكنولوجيا تجفير المفتاح العام. وتوفر شهادة رقمية ضماناً بالربط بين المفتاح العام والحائز على الشهادة. ويمكن أن توفر التوقيعات الرقمية الاستيقان، وسلامة البيانات، وعدم الإنكار للمعاملات. ويمكن استخدام هذه التوقيعات في تثبيت معرف الهوية المزعومة راسل إحدى الرسائل. كما تستخدم هذه التوقيعات في كثير

من الأحيان بالاقتران مع الشهادات الرقمية. وتستخدم هذه الشهادات كوسيلة لحمل المعلومات اللازمة لتجفير المفتاح العام والتوقيعات الرقمية. ويمكن إصدار الشهادات الرقمية للمستخدمين من خلال هيئة معتمدة أو موثوق بها.

وتشكل شفرة استيقان الرسائل (MAC) وسيلة تدقيق للاستيقان تشتق من خلال تطبيق مخطط استيقان جنباً إلى جنب مع مفتاح سري على رسالة. وعلى العكس من تقنيات التوقيعات الرقمية، تحسب شفرة استيقان الرسائل ويجري تدقيقها باستخدام نفس المفتاح. وبهذه الطريقة لا يمكن التحقق من هذه الشفرة إلا بواسطة المستقبل المقصود. وفي شفرة استيقان الرسائل المعتمدة على دالة الفرم (HMAC) (انظر [b-IETF RFC 2104])، يستخدم المفتاح أو (المفاتيح) بالاقتران مع دالة الفرم للخروج بقائمة تدقيق ترفق بالرسالة.

## 2.II تكنولوجيات التحكم في النفاذ

يركز التحكم في النفاذ على ضمان عدم نفاذ سوى المستخدمين المرخصين إلى جهاز الشبكة أو نظام مصاحب. وعلى ذلك فإن التحكم في النفاذ يمكّن خبراء تكنولوجيا المعلومات من الارتقاء بتحليل وفهم نمط وطبيعة الهجمات التي تحدث على شبكتهم. وهناك الكثير من التقنيات التي يمكن استخدامها لتنفيذ التحكم في النفاذ. وتناقش هذه الطرائق في الفقرات الفرعية التالية.

### 1.2.II حماية المحيط الخارجي

تحول تكنولوجيا حماية المحيط الخارجي دون النفاذ إلى الشبكة أو الحاسوب من جانب المستخدمين الخارجيين غير الموثوق بهم أو المرخص لهم. وتقيم تكنولوجيات حماية المحيط حدوداً منطقية أو مادية بين المناطق المحمية والمناطق المفتوحة للجمهور والمستخدمين الخارجيين غير الموثوق بهم (ولا يشمل ذلك العناصر الداخلية غير الموثوق بها). ويمكن تطبيق تكنولوجيا حماية المحيط على حماية الشبكة أو جهاز مفرد. وتشمل الأمثلة على تكنولوجيات حماية المحيط ما يلي:

1) برمجيات ترشيح المحتويات أو إدارة المحتويات تقيد نمط البيانات التي يمكن النفاذ إليها أو توزيعها في إحدى الشبكات (انظر [b-ISO/IEC 10828-3]) وتقيد قدرة المستخدمين على النفاذ إلى المحتويات الواقعة خارج حدودهم. ويقلل ذلك إلى أدنى حد ممكن من فرص تحميل الفيروسات وغير ذلك من الشفرات الضارة من مواقع غير موثوق بها. ويمكن أن يتخذ ترشيح المحتويات شكل مرشاحات (URI) (انظر [IETF RFC 2396]) حيث يمكن أن تمنع المستخدمين من النفاذ إلى صفحات الويب التي تتضمن محتوى مشكوكاً فيه. ويمكن استخدام ترشيح المحتويات في مسح رسائل التطبيقات مثل البريد الإلكتروني للبحث عن فيروسات الرسائل الاقتحامية أو المحتويات غير المعتمدة.

2) جدران الحماية: يمكن تقسيم هذه التكنولوجيا (انظر [b-ISO/IEC 10828-3]) إلى أربع فئات عريضة هي: مرشاحات الرزم والبوابات على مستوى الدارة والبوابات على مستوى التطبيقات وجدران الحماية للتفتيش متعدد الطبقات الشاملة.

- جدران الحماية بترشيح الرزم تعمل عند طبقة بروتوكول الإنترنت. وتعتبر دائماً جزءاً من جدران حماية المسير. وتقوم بإجراء مقارنة كل رزمة في بروتوكول الإنترنت مقابل قاعدة معرفة حددت قبل تقديمها إلى المسير التالي أو مقصدها النهائي. واعتماداً على نتائج المقارنة، تقوم جدران الحماية إما بإسقاط الرزمة أو تقديمها أو إرسال رسالة إلى مصدر الرزمة. ويمكن أن تتضمن القواعد المصدر والمقصد في عنوان بروتوكول الإنترنت، ورقم منفذ المصدر والمقصد والبروتوكول المستخدم. ويوفر مسيرات تحويل عنوان الشبكة (NAT) مزايا عناوين الأجهزة العاملة ببروتوكول الإنترنت خلف جدران الحماية. ولن يكون لجدران حماية ترشيح الرزم تأثير كبير على أداء الشبكة ويوفر بعض مستويات الأمن لطبقة الشبكة.
- البوابات على مستوى الدارة تعمل عند طبقة TCP في TCP/IP لرصد تنظيم الاتصالات TCP بين الرزم لاكتشاف ما إذا كانت الدورة المطلوبة قانونية من عدمه. وعلاوة على ذلك، سوف تظهر للمستقبل الطلبات الصادرة لحاسوب بعيد، من خلال بوابة على مستوى الدارة، كما لو كانت هذه الطلبات صادرة عن البوابة. وتساعد التقنية في حجب المعلومات المستقلة بالشبكة المحمية. ولا تقوم البوابات على مستوى الدارة بترشيح الرزم المفردة.

- التفويضات أو البوابات على مستوى التطبيقات يمكن أن ترشح الرزم عند طبقة التطبيقات في نموذج ترابط الأنظمة المفتوحة (OSI). ولا يمكن للطلبات الوافدة والخارجة أن تنفذ إلى الخدمات التي لا يوجد لها تفويض. وتفحص التعويضات الرزم عند طبقة التطبيقات لترشيح الأوامر النوعية المعنية بالتطبيقات مثل HTTP POST (انظر [b-IETF RFC 2616]). ولا يسمح التفويض للحركة غير المستقلة أن تصل إلى التطبيقات. كما يمكن استخدام التفويضات لتسجيل نشاط المستخدم وزيارته. وقد توفر التفويضات مستوى مرتفعاً من الأمن بتأثير كبير على أداء الشبكة.
- جدران الحماية للتفتيش متعدد الطبقات الشامل تجمع جوانب أنماط جدران الحماية المشار إليها أعلاه. وتقوم جدران الحماية متعددة الطبقات بترشيح الرزم عند طبقة الشبكة، وتترشح إذا كانت رزم الدورة صالحة وترشيح محتويات الرزم عند طبقة التطبيقات. وجدران الحماية متعددة الطبقات تتسم بالشفافية إزاء التوصيلات بين الراسل والمستقبل.

3) تحويل عنوان الشبكة (NAT): توفر هذه التكنولوجيا القدرة على إخفاء مخطط عنونة الشبكة خلف بيئة من جدران الحماية. وفي هذا التحويل (NAT)، يجري تقابل عنوان بروتوكول الإنترنت لأحد الأنظمة على الشبكة الداخلية على مختلف عناوين بروتوكول الإنترنت الخارجية والقابلة للتسيير المتوافقة. ويمكن في إطار (NAT) للكثير من الأنظمة المتخفية وراء جدار حماية تقاسم نفس العنوان الخارجي ببروتوكول الإنترنت. وتظل الموارد الموجودة وراء جدار الحماية قابلة للنفاذ للمستخدمين الخارجيين من خلال تقديم توصيلات غير مقيدة على أرقام منفذ معين. ويمكن تنفيذ NAT على معظم أجهزة الشبكات مثل البدالات والمسيرات وجدران الحماية.

4) البوابات على مستوى التطبيقات. تتألف هذه الأنظمة (انظر [b-ISO/IEC 10828-3]) من المعدات والبرمجيات استناداً إلى جهاز أو مجموعة من الأجهزة. وقد صممت لتقييد النفاذ فيما بين شبكتين منفصلتين. وتستخدم هذه الأنظمة تقنيات تفتيش الرزم الشامل وتفويض التطبيقات لتقييد النفاذ فيما بين الشبكات. ويمكن أيضاً استخدام تجميعات وتباينات (مثل جدران الحماية على مستوى الدارة) هذه التقنيات. وعلاوة على ذلك، يمكن أداء تحويلات عنوان الشبكة (NAT) من خلال البوابات على مستوى التطبيقات.

5) تفويض التطبيقات: توفر هذه الأنظمة (انظر [b-ISO/IEC 10828-3]) المعرفة على مستوى التطبيقات بمحاولات التوصيلات من خلال فحص الرزم على أعلى طبقة في مجموعة البروتوكول. ويتوافر لتفويضات التطبيقات الرؤية الكاملة لمبادلات البيانات على طبقة التطبيقات. وتتيح لها هذه القدرة أن ترى بسهولة التفاصيل المبلورة لكل محاولة توصيل أمامية وتنفيذ السياسات الأمنية بناءً على ذلك. ويمكن أن تتحلى تفويضات التطبيقات بالقدرة على إنهاء توصيلات العميل ويمد توصيلة جديدة إلى الشبكة الداخلية المحمية. وتوفر هذه القدرة أمناً إضافياً حيث إنها تفضل الأنظمة الخارجية عن تلك الداخلية.

### 2.2.II الشبكة الخاصة الافتراضية (VPN)

يقدم المعيار [b-ISO/IEC 18028-5] عرضاً عاماً شاملاً لاستخدام الشبكة الخاصة التقديرية في حماية الاتصالات عبر الشبكات.

وتستخدم هذه الشبكات (VPN) الآن في مهمة الربط البيني للشبكات وكطريقة لربط المستخدمين في المناطق النائية بالشبكات وتوفر شبكات VPN في أبسط صورها آلية لإقامة شبكة أو شبكات بيانات مأمونة على شبكة قائمة أو توصيلة من نقطة إلى نقطة. ويمكن إقامة هذه الشبكات VPN وإزالتها بصورة دينامية. وقد تكون الشبكة المضيفة خاصة أو عامة.

وينفّذ النفاذ عن بعد باستخدام شبكة خاصة افتراضية (VPN) على قمة توصيلة عادية من نقطة إلى نقطة تقوم منشأة بالمثل بين المستخدم المحلي والموقع البعيد (انظر [b-ISO/IEC 18028-5]). ويمكن توفير شبكات VPN كخدمة مدارة حيث تتوفر توصيلية آمنة موثوقة وإدارة وعنونة، مكافئة لما يحدث في شبكة خاصة، وذلك في بنية تحتية متقاسمة.

وهناك عدة طرق لبيان أشكال شبكات VPN (انظر [b-ISO/IEC 18028-5]). فقد تكون هذه الشبكات (VPN) من حيث المبدأ ما يلي:

– توصيلة واحدة من نقطة إلى نقطة (مثل جهاز عمل ينفذ عن بعد إلى شبكة مؤسسة على بوابة موقع)؛ أو

– توصيلة من نقطة إلى نقطة (باستخدام تقنيات مبادلة الواسمة متعددة البروتوكولات (MPLS).

وثمة ثلاثة أنماط رئيسية للشبكات الخاصة الافتراضية (انظر [b-ISO/IEC 18028-5]) هي:

– الشبكات الخاصة الافتراضية (VPN) من الطبقة 2 تحاكي تسهيلات شبكة المنطقة المحلية باستخدام توصيلات شبكة VPN العاملة على شبكة مضيفة، للربط بين مواقع مؤسسة أو لتوفير توصيلة بعيدة لمنطقة. وتشمل عروض الموردين المعتادة خدمة سلكية خاصة تقديرية (VPWS) توفر توصيلة لأسلاك زائفة فقط أو خدمة شبكة منطقة محلية خاصة افتراضية توفر خدمة شبكة منطقة محلية تمت محاكاتها بصورة أكمل.

– الشبكات الخاصة الافتراضية (VPN) من الطبقة 3 تحاكي تسهيلات شبكة المنطقة الواسعة باستخدام شبكات خاصة افتراضية تعمل على بنية تحتية لإحدى الشبكات. وتوفر القدرة على استخدام مخططات العناوين الخاصة على بروتوكول الإنترنت على بنية تحتية عامة، وهي ممارسة لن يسمح بها على توصيلات بروتوكول الإنترنت العامة. غير أن استخدام العناوين الخاصة على شبكات عامة عن طريق تحويل عناوين الشبكة قد تتسبب في تعقيد أمن بروتوكول الإنترنت (انظر [b-IETF RFC 2411]) وإنشاء الشبكة الخاصة الافتراضية واستخدامها.

– الشبكات الخاصة الافتراضية من الطبقة 4 تستخدم في ضمان أمن المعاملات على الشبكات العامة. وفي هذا النمط من الشبكات الخاصة الافتراضية تقام التوصيلات عادة على TCP الذي يكون بروتوكول من الطبقة 4. ويوفر هذا النمط من الشبكات الخاصة الافتراضية قناة مأمونة لتوصيل التطبيقات لضمان سرية البيانات وسلامتها طوال فترة المعاملة.

ويمكن تنفيذ الشبكات VPN داخل شبكة خاصة تحت رقابة المنشأة المالكة أو يمكن تنفيذها عبر الشبكات في مجال عام. كما يمكن إجراء التنفيذ باستخدام تجميع لهذين المخططين. ومن ناحية أخرى، يمكن إقامة القنوات من خلال استخدام القنوات المأمونة عن طريق استخدام الأنفاق التي تمر عبر شبكات مقدم خدمة الإنترنت. وفي هذا الصدد فإن الإنترنت العام هو، من الناحية الفعلية، نظام النقل الأساسي. وعلى ذلك فإن هناك مخاطر أكبر على سرية البيانات التي تحملها الشبكة الخاصة الافتراضية.

والنفق عبارة عن مسير بيانات بين الأجهزة المترابطة شبكياً المنشأة عبر البنية التحتية الشبكية القائمة. والنفق يتسم بالشفافية إزاء عمليات الشبكة. والشبكة الخاصة الافتراضية التي تنشأ بأنفاق تعتبر عموماً أكثر مرونة من الشبكة التي تعتمد على الوصلات المادية. ويمكن إنشاء الأنفاق من خلال استخدام الدارات الافتراضية أو تبديل الواسمات أو كبسلة البروتوكول.

ويتضمن الجدول 2.2.II الجوانب الأمنية لمختلف أنماط الشبكات الخاصة الافتراضية (انظر [b-ISO/IEC 18028-5]).

**الجدول 2.2.II – الجوانب الأمنية للشبكات الخاصة الافتراضية (VPN)**

| الشبكة الخاصة الافتراضية | التكنولوجيا | استيقان المستخدم | تجفير البيانات | إدارة المفتاح | التحقق من السلامة |
|---|---|---|---|---|---|
| **الشبكة VPN من الطبقة 2** | مرحل رتل، ATM، MPLS، PPP، L2F | لا تنطبق | لا تنطبق | لا تنطبق | لا تنطبق |
| | L2TP (انظر [b-IETF RFC 2661]) | مثل CHAP | لا تنطبق | لا تنطبق | لا تنطبق |
| **الشبكة VPN من الطبقة 2** | أمن بروتوكول الإنترنت (IPSec) | مفاتيح سرية تعتمد على الشهادات (الرزم) سبق تبادلها | خوارزميات (رزم) عديدة قابلة للتفاوض | مبادلة مفتاح الإنترنت | قابلة للتفاوض |
| | أمن IPSec على L2TP | مفاتيح سرية تعتمد على الشهادات (الرزم) سبق تبادلها | خوارزميات (رزم) عديدة قابلة للتفاوض | مبادلة مفتاح الإنترنت | قابلة للتفاوض |
| | MPLS | لا تنطبق | لا تنطبق | لا تنطبق | لا تنطبق |
| **الشبكة VPN من الطبقة 4** | TLS | استناداً إلى الشهادة | قابلة للتفاوض | قابلة للتفاوض | قابلة للتفاوض |
| | قشرة آمنة | زوج مفاتيح مولدة من النظام (غير معتمدة) | قابلة للتفاوض | مبادلة المفاتيح العامة لمرسل البيانات | قابلة للتفاوض |

**الملاحظة 1** – يمكن استخدام SSL بدلاً من TLS.

**الملاحظة 2** – توفر [b-IETF RFC 3031] عرضاً عاماً لمعمارية مبادلة الواسمة المتعددة البروتوكولات (MPLS). وتصف[b-IETF RFC 1661] بروتوكولاً من نقطة إلى نقطة (PPP) وتناقش [b-IETF RFC 2427] الربط البيني المتعدد البروتوكولات عن مدخل رتل.

### 3.2.II الاستيقان

يمكن استخدام طرائق عديدة للاستيقان من مستخدم. وتشمل التقنيات: كلمات السر، وبطاقة المرور لمرة واحدة، وتقنيات القياس البيولوجي، والبطاقات الذكية [b-ISO/IEC 7816-x]] والشهادات. ويتعين أن يستخدم الاستيقان المعتمد على كلمات السر كلمات سر قوية (مثل أن تتكون من ثمان سمات على الأقل من حيث الطول مع أبجدية واحدة على الأقل وسمة عددية واحدة وسمة خاصة على الأقل). وقد لا تكفي عملية الاستيقان باستخدام كلمات السر. وقد يكون من الضروري، اعتماداً على تقييم جوانب الصنف، الجمع بين الاستيقان باستخدام كلمات السر وعمليات الاستيقان والترخيص الأخرى مثل الشهادات والبروتوكول سريع النفاذ للدليل (LDAP) (انظر [b-IETF RFC 3377]) وخدمة المستخدم لمراقمة الاستيقان عن بعد (انظر [b-IETF RFC 2869] و[b-IETF RFC 3579] و[b-IETF RFC 3580]) وآلية Kerberos (انظر [b-IETF RFC 1510]) والبنية التحتية للمفتاح العام (انظر [b-IETF RFC 2459]).

ويمكن تصنيف أنظمة الاستيقان وفقاً لعدد عوامل التعريف اللازم لإثبات الهوية. فيشير الاستيقان ذو العامل الواحد إلى نظام يستخدم عنصراً واحداً (مثال: توليفة من هوية المستخدم/كلمة السر). ويصف الاستيقان على أساس عاملين عملية تتطلب مكونين للحصول على النفاذ إلى النظام، مثل امتلاك رمز مادي بالإضافة إلى معرفة بأحد الأسرار (مثل كلمة السر). ويضيف النظام المكون من ثلاثة عوامل عامل تعريف آخر مثل مقياس بيولوجي أو مقياس لخصائص في الجسم البشري. ويؤدي استخدام المزيد من عوامل الاستيقان إلى زيادة أمن الاستيقان، إلا أن تضمين عدد أكبر من العوامل يضاعف من التعقيد والتكاليف ومصروفات الإدارة. ولذا فإن إيجاد التوازن الأمثل بين البساطة والأمن تمثل تحدياً يواجه أي نظام للاستيقان.

والاستيقان بعامل واحد من هوية المستخدم وكلمة السر هو الآن النظام الأكثر شيوعاً في الاستخدام. فأنظمة الاستيقان بكلمة السر بسيطة وسهلة على الإدارة ومألوفة تماماً للمستخدمين. وفي حالة استخدام كلمات السر القوية، قد توفر أنظمة الاستيقان بالعامل الواحد مستوى عالياً من الأمن. غير أن أنظمة كلمات السر التقليدية كانت تنطوي على بعض التحديات نظراً لأن كلمات السر القوية المتعددة تتسبب في صعوبة شديدة في التذكر لدى المستخدمين. ويمكن التقليل من هذه العيوب إلى أدنى حد ممكن، كما سيرد تفصيله في التوصيات أدناه، لتوفير حل أمثل بنظام "كلمة سر قوية واحدة".

وتضاف بعض العلامات (الأمارة) مثل البطاقات الذكية كعامل ثان في كثير من أنظمة الاستيقان. فالعلامات توفر أمناً إضافياً للاستيقان حيث يتعين على المستخدم أن يثبت الامتلاك المادي لهذه العلامات لكي يستيقن منه. كما يتعين أن يكون لدى المهاجم العلامة التي لدى المستخدم لكي يحصل على النفاذ إلى النظام. غير أن تحقيق المستوى الأعلى من الاستيقان يتم بتكاليف إضافية على النظام نتيجة للعلامات الضرورية، وأجهزة قراءة هذه العلامات. وعلاوة على ذلك، يمكن فقد هذه العلامات بسهولة مما يتسبب في تكاليف إدارية كبيرة لإعادة إصدارها.

ويمكن توفير الاستيقان المعتمد على التجفير الشديد من خلال استخدام الشهادات الرقمية التي تصدر للمستخدمين وتحتفظ في علاقات أو داخل ذاكرة حاسوب المستخدم. وتستخدم خوارزمية التجفير لضمان إصدار شهادة معينة بطريقة قانونية للمستخدم. وتستخدم البنية التحتية للمفتاح العام للتمكين من إصدار الشهادات الرقمية والمحافظة عليها. وتوفر الأنظمة المعتمدة على التجفير القوي استيقاناً شديد القوة إلاّ أن هذه الأنظمة باهظة التكلفة وتتسبب في تكبد مصاريف إدارية، ولذا فإنها لا تعتمد حالياً إلاّ في إطار البيئات التي تحظى بالأمن الشديد.

### 4.2.II الترخيص

تقوم آليات الترخيص، بعد أن يتم الاستيقان، بالتحكم في النفاذ إلى موارد النظام الملائمة. ويمكن تصنيف الترخيص وفقاً لمدى التحكم، أي وفقاً لمدى تفصيل التقسيم بين موارد النظام. ويشير الترخيص الدقيق، بصورة عامة، إلى النظام الذي يخضع فيه النفاذ للتحكم إلى أدنى زيادات متوافرة مثل التطبيقات أو الخدمات الفردية.

وكثيراً ما يعتمد الترخيص على "الدور" حيث يعتمد النفاذ إلى موارد النظام على الدور المسند لشخص ما في المنظمة. وقد يكون لدور القائم على الشؤون الإدارية للنظام نفاذ شديد التمييز إلى جميع موارد النظام في حين يقتصر النفاذ بالنسبة لدور المستخدم العام على مجموعة فرعية من هذه الموارد. وفي حالة تطبيق الترخيص الدقيق، قد يكون لدور مديري الموارد البشرية نفاذ حصري لقواعد بيانات الموارد البشرية شديدة السرية وقد يكون لدور المحاسبة نفاذ حصري إلى قواعد بيانات نظام المحاسبة.

كما يمكن أن يعتمد الترخيص على "القواعد" حيث يستند النفاذ إلى موارد النظام إلى قواعد محددة تتعلق بكل مستخدم بصورة مستقلة عن الدور الذي يضطلع به أو تضطلع به في المنظمة. فعلى سبيل المثال، يمكن وضع القواعد لإتاحة النفاذ للقراءة فقط أو النفاذ لقراءة وكتابة جميع الموارد أو بعض الملفات داخل النظام.

### 5.2.II بروتوكولات الاستيقان والنفاذ

اعتمد العديد من البروتوكولات بصورة عامة لخدمات الاستيقان. إذ يستخدم بروتوكول RADIUS (الاستيقان عن بعد لمراقمة خدمات المستخدم) (انظر [b-IETF RFC 2865]) على نطاق واسع لوضع خدمات الاستيقان باستخدام كلمة السر على المستوى المركزي. وقد اعتمد بروتوكول RADIUS، الذي كان قد صمم في الأصل لاستيقان مستخدمي المراقمة عن بعد، على الخدمات العامة لاستيقان المستخدمين. كما استخدم بروتوكول LDAP (البروتوكول سريع النفاذ للدليل) على نطاق واسع في أنظمة الاستيقان والترخيص. ويوفر LDAP طريقة تقليدية لحفظ معلومات استيقان المستخدم وشهادات اعتماد التراخيص.

ويجري في غالب الأحيان ربط مخدمات الاستيقان ببروتوكول RADIUS مع محفوظات أوراق الاعتماد في أدلة LDAP لتوفير نظام مركزي للاستيقان والترخيص. وعندما يحاول مستخدم النفاذ تطبيقاً معيناً على هذا النظام، يطلب هذا التطبيق من المستخدم أوراق اعتماد الاستيقان وتقديمها للنظام المركزي. ويقوم مخدم RADIUS بعد ذلك بالتحقق من أوراق الاعتماد والمقدمة مقابل تلك المحفوظة في قواعد بيانات LDAP، ويطلب كذلك من قاعدة بيانات LDAP تقديم معلومات عن قاعدة

الترخيص. وتعاد نتائج الاستيقان (النجاح أو الفشل) إلى التطبيق جنباً إلى جنب مع معلومات قاعدة الترخيص لهذا المستخدم المعين. وسيجري بعد ذلك إنفاذ قواعد الترخيص عند التطبيق للسماح للمستخدم النفاذ إلى بيانات أو خدمات معينة. ويتوقع من زاوية المستخدم النهائي أن تكون أنظمة الاستيقان والترخيص هذه أوتوماتية وسهلة الاستخدام.

### 3.II مكافحة الفيروسات، وسلامة الأنظمة

قد تعدل شفرة الفيروسات المتسللة (Worms)، والشفرات الخبيثة، والفيروسات المتخفية (Trojan horses) نظاماً أو تغير في بياناته. ولذا فإن من المهم استخدام التكنولوجيات التي تقوم بالمسح للبحث عن الفيروسات وضمان المحافظة على سلامة النظام.

والفيروسات المتسللة (Worms) عبارة عن برنامج يتكاثر من خلال تكرار نفسه من نظام لنظام آخر دون حاجة إلى تدخل بشري. وقد ترتبط الفيروسات نفسها بملفات المستخدمين وأن تعود إلى الحياة من خلال تكرار نفسها في ملفات أخرى عندما يقوم مستخدم لا يساوره شك بأحد الأعمال مثل فتح ملف ملوث. أما الفيروسات المتخفية (Trojan horses) من ناحية أخرى، فإنها تقدم نفسها للمستخدم الذي لا يساوره شك على أنها برنامج مفيد يخفي شفرة ضارة.

وتساعد تكنولوجيا مكافحة الفيروسات في حماية الأنظمة من الفيروسات المتسللة والشفرات الخبيثة والفيروسات المتخفية. ويمكن إما تركيب البرمجيات على أجهزة المستخدمين أو تقديمها في شكل خدمة من مورد الشبكة أو خدمة الإنترنت. وتستخدم تقنيات سلامة الأنظمة برمجيات تتحقق من عدم تطبيق إلا عمليات التحديث المرخص بها في ملفات النظام الأساسية.

ويمكن أن تستخدم منتجات البرمجيات المكافحة للفيروسات تقنيات التوقيعات المتسلسلة في التعرف على الفيروسات والشفرات الخبيثة. وتتطلب هذه التقنية معرفة مسبقة بالشفرة الخبيثة مثل أن تتمكن برمجيات مكافحة الفيروسات من اكتشافها. ولذا يتعين أن تكون قاعدة بيانات التوقيعات بها جاهزة للحماية الفعالة.

وتعمل ماسحات الأنشطة بحثاً عن أنشطة غير مرخص بها تكون قد تمت بواسطة شفرة التشغيل. وتبلغ البرمجيات المستخدم بالأنشطة المشبوهة. ولا تحقق ماسحات الأنشطة عادة إلا قدراً محدوداً من النجاح في مواجهة الفيروسات إلا أنها لن تكون أكثر فعالية في مواجهة الفيروسات المتسللة وتلك المتخفية. وتقوم الماسحات الساكنة الكشافة بفحص الشفرة لمحاولة التعرف على الأنشطة التي يمكن ربطها بالسلوك المماثل للفيروسات.

وتستخدم تقنيات سلامة الأنظمة برمجيات ترصد التعديلات التي أجريت على ملفات النظام الأساسية. ويمكن استخدام هذه التقنيات بواسطة مديري تكنولوجيا المعلومات للقيام بعمليات تحقق في النظام لتحديد ما إذا كان مبرمجون مقتحمون قد تغلغلوا بنجاح إلى أحد الأنظمة (يميل المبرمجون المقتحمون إلى ترك شراك خلفية).

### 4.II التدقيق والرصد

تتيح تقنيات التدقيق والرصد للقائمين على الشفرات الإدارية لتكنولوجيا المعلومات تقييم أمن النظام الشامل بما في ذلك برمجيات التعليمات والكشف والمنع. وبوسع القائمين على الشؤون الإدارية لتكنولوجيا المعلومات استخدام هذه التكنولوجيا لإجراء تحليل النظام لتحديد جوانب الضعف فيه بعد الهجوم. ويمكن في بعض الحالات إجراء تحليل النظام خلال هجوم نشط على النظام.

ويمكن استخدام أنظمة كشف الاقتحام (IDS) (انظر [b-ISO/IEC 18043]) لمراقبة الشبكة لضمان عدم نفاذ أي مستخدمين غير مرخصين إلى الشبكة. وتقوم معظم تطبيقات كشف ومنع الاقتحام (IDS) بمقارنة حركة الشبكة بمداخل سجل المضيف لمضاهاة توقيعات البيانات بجوانب عنوان المضيف لتحديد المبرمجين المقتحمين. وتتعرف برمجية كشف الاقتحام أنماط الحركة التي تنم عن وجود مستعملين غير مرخص لهم. وتطلق الأنشطة المشبوهة إنذارات لدى مدير الشبكة وغيرها من الاستجابات القابلة للتشكيل. ويمكن تصنيف أنظمة كشف الاقتحام (IDS)، بصفة عامة، وفقاً للمعايير التالية:

- الإطار الزمني لكشف الحوادث: في الوقت الفعلي أو بصورة غير مباشرة بحسب ما إذا كان هناك تسجيل في النظام وتحليل حركة الشبكة أثناء وقوع الأحداث أو بأسلوب الدفعة في ساعات الراحة؛

- نمط التركيب: اعتماداً على الشبكة أو اعتماداً على المضيف. وتشمل أنظمة الكشف عن الاقتحام المعتمدة على الشبكة عادة على شاشات متعددة (في الغالب عبارة عن أجهزة سابقة التشكيل) تركب عند نقاط الاختناق على الشبكة (حيث يمكن رصد جميع أشكال الحركة فيما بين نقطتين). وتتطلب أجهزة كشف الاقتحام المعتمدة على المضيف تركيب البرمجيات بصورة مباشرة على المخدمات التي ستجري حماتيها ورصد توصيلات الشبكة ونشاط المستخدم على هذه المخدمات؛
- نمط الاستجابة للحوادث: سواء تدخلت أنظمة كشف الاقتحام بنشاط لتجنب الهجمات (مثل تعديل قواعد جدران الحماية أو مرشاحات المسير) أو مجرد إبلاغ الموظفين أو أنظمة الشبكات الأخرى بالمشكلة.

وتوفر معظم أنظمة كشف الاقتحام التجارية توليفة من مقدرات الرصد المعتمدة على الشبكة والمعتمدة على المضيف مع مضيف إدارة مركزي لتلقي التقارير من مختلف الشاشات وتنبيه موظفي دعم الشبكة. ويوصى باستخدام أنظمة كشف الاقتحام المعتمدة على الشبكة لمعظم تركيبات الشبكات بحسب الاحتياجات الخاصة للعميل.

## 5.II الإدارة

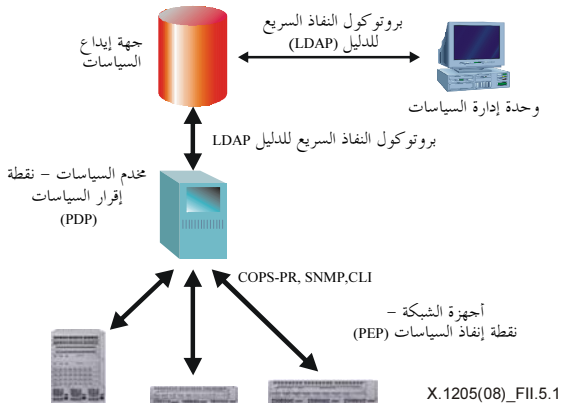
تتيح تقنيات إدارة التشكيل للقائمين على الشؤون الإدارية لتكنولوجيا المعلومات إقامة الأوضاع الآمنة والتحقق منها على الأجهزة في شبكاتهم. وتمكن إدارة السياسات القائمين على الشؤون الإدارية لتكنولوجيا المعلومات من تعريف الأمن الموجه نحو المنشآت التجارية وسياسات نوعية الخدمة (QoS) وإنفاذها عبر المنظمة دون حاجة إلى فهم جميع القواعد والأوضاع الخاصة بالأجهزة اللازمة لإنفاذ هذه السياسات. والسياسات من الناحية التقنية، عبارة عن مجموعة من القواعد اللازمة لتنظيم وإدارة النفاذ إلى موارد تكنولوجيا المعلومات والتحكم فيها، ويتعين أن تكون هذه السياسات مدفوعة من سياسات منشآت الأعمال التي تحددها المنظمة. وتعالج إدارة السياسات، في مجال الأمن، ما تنطوي عليه تعلم المنحنيات ذات الصلة بهذه التكنولوجيا من تقصير وصعوبة (مثل جدران الحماية وأنظمة كشف الاقتحام وقوائم النفاذ والمرشاحات وتقنيات الاستيقان) وانعدام وجهة نظر النظام عبر مختلف أجزاء الشبكة (مركز البيانات، المكتب البعيد، والجامعات).

وفي حين أن هناك العديد من الحلول لمعالجة جوانب من المشكلة، فإن نظام إدارة السياسات النهائية يوفر تشكيلاً لشبكة مركزية بما يضمن وضع معلمات الآن بصورة متسقة عبر العقد المتعددة ويقلل المخاطر الناجمة عن ضعف الشبكة. ولا يعني ذلك أن هناك نظام سياسات واحداً في شبكة كبيرة متعدد فيها المجالات الإدارية، فقد تكون ثمة حاجة إلى أنظمة سياسات متعددة يكون كل منها مسؤولاً عن التحكم في مجموعة فرعية من الأجهزة مع توافر الاتساق فيما بين المجالات.

وتتمثل المنطقة الرئيسية من نظام إدارة السياسات كامل التنفيذ في سهولة الاستخدام والبنية الأكثر أمناً. وقد يود مديرو الشبكات النموذجية التمكن من تعريف السياسات الخاصة بعمليات الشبكة باستخدام مفردات غير تقنية ثم ترك نظام السياسات تحويل هذه المصطلحات أوتوماتياً إلى آليات أمنية ملائمة تنفذ عبر الشبكة.

### 1.5.II نموذج مرجعي لإدارة السياسات

يبين الشكل 1.5.II الإطار المعماري الذي وضعه فريق مهام هندسة الإنترنت لإدارة السياسات ([b-IETF RFC 2753]). ويستخدم هذا النموذج المرجعي بوصفة المخطط الرئيسي لإدارة السياسات لكل من الأمن وإدارة نوعية الخدمة (QoS). وعلى ذلك عندما ترتكز إدارة السياسات على هذا النموذج وتنفذه عبر الشبكة وفي جميع طبقات المعمارية، وتتيحه لجميع أنماط المستخدمين والتطبيقات بما في ذلك الموظفين وتقنيي الشبكات والشركاء بل وحتى العملاء.




**الشكل II.1.5 – النموذج المرجعي لإدارة السياسات**

وتتضمن مكونات النموذج ما يلي:

- *نقطة إنفاذ السياسات (PEP)*: شبكة أو جهاز أمن يقبل سياسة (قواعد التشكيل) من نقطة إقرار السياسات وإنفاذ تلك السياسة في مواجهة حركة الشبكة التي تقيد هذا الجهاز. ويؤدي هذا الإنفاذ إلى تعزيز الشبكة والآلية الأمنية المعانة حسب مقتضى الحال.
- *نقطة إقرار السياسات (PDP)*: تقوم نقطة إقرار السياسات أو مخدمات السياسة بتحويل سياسات الشبكة إلى رسائل التحكم في جهاز نوعي تُمرّر بعد ذلك إلى نقاط إنفاذ السياسات. وتتمثل مخدمات السياسات هذه في كثير من الأحيان في شكل أنظمة منفصلة تتحكم في جميع البدالات والمسيرات ضمن مجال إداري معين، وتتصل مع الأجهزة الأخرى باستخدام بروتوكول التحكم (مثل COPS وأوامر تدميث SNMP وشبكة Telnet أو السطح البيني لخط الأمر المحدد للجهاز – (CLI)).
- *خدمة السياسات المفتوحة المشتركة (COPS)*: هذه الخدمة هي عبارة عن بروتوكول شامل وبسيط للسؤال والرد يعتمد على TCP ويمكن استخدامها لتبادل معلومات السياسات فيما بين نقطة إقرار السياسات وعملائها من نقاط إنفاذ السياسات. ويحدد هذا البروتوكول في [b-IETF RFC 2748]. وتعتمد هذه الخدمة على نقاط إنفاذ السياسات (PEP) في إقامة توصيلات مع نقطة إقرار السياسات الرئيسية (والثانية عندما يتعذر الوصول إلى الرئيسية) في جميع الأوقات. وبدلاً من ذلك يمكن استخدام تفويض COPS الذي يحول رسائل هذه الخدمة الناشئة عن مخدم سياساته إلى أوامر SNMP أو CLI تفهمها الشبكة وأجهزة الأمن.

  ويدعم بروتوكول COPS نموذجي توسع مختلفين للتحكم في السياسات: نموذج دينامي للتعاقدات الخارجية COPS-RSVP محدد في [b-IETF RFC 2749]، ونموذج تشكيل أو تزويد COPS-PR محدد في [b-IETF RFC 3084]. وتتيح توسعات التزويد لبروتوكول COPS وضع السياسات على الجبهة العالية لـ PEP بواسطة PDP ومن ثم إتاحة الفرصة لـ PEP لوضع قرارات السياسات لرزم البيانات المعتمدة على هذه المعلومات السابقة التزويد. ومن الضروري إقرار اتصالات أخرى بين PEP وPDP لاستمرار توفير السياسات في جهة إيداع البيانات (أي الدليل) في تزامن مع تلك المرسلة إلى PEP.
- *جهة إيداع السياسات*: دليل الشبكة هو جهة إيداع المعلومات المتعلقة بالسياسات حيث يصف مستخدمي الشبكة والتطبيقات والحواسيب والخدمات (مثل المواضيع والنعوت) والعلاقات بين هذه الكيانات. وهناك اندماج وثيق بين عناوين بروتوكول الإنترنت والمستخدم النهائي (عن طريق بروتوكول التحكم في مضيف دينامي – DHCP ونظام اسم الميدان – DNS). وينفذ الدليل عادة على آلة قاعدة بيانات ذات أغراض خاصة. ومن ناحية أخرى فإن البروتوكول سريع النفاذ إلى الدليل هو الآلية التي تستخدمها مخدمات السياسات للنفاذ إلى الدليل.

  وتستخدم جهة إيداع السياسات لحفظ المعلومات الثابتة نسبياً عن الشبكة (مثل تشكيلات الجهاز) في حين أن مخدمات السياسات تحفظ معلومات حالة الشبكة الأكثر دينامية (مثل التوزيع عريض النطاق أو المعلومات عن التوصيلات المنشأة). ويسترجع مخدم السياسات معلومات السياسات من الدليل ويوزعها على عناصر الشبكة الملائمة.

ولا يوجد معيار محدد لوصف بنية قاعدة بيانات الدليل، مثل كيفية تعريف مواضيع الشبكة ونعوتها وتمثيلها. ويتعين وجود مخطط مشترك للدليل إذا كان يتعين أن تتقاسم تطبيقات الموردين المتعددين نفس معلومات الدليل. فعلى سبيل المثال، يتعين على جميع الموردين استخدام وسيلة مشتركة لتفسير وحفظ معلومات التشكيل عن المسيرات. ويعالج معيار التشغيل البيني القادم لتمكين الدليل (DEN) الذي يقوم بوضعه DMTF (فريق مهام إدارة سطح المكتب) هذه الحاجة. وتتضمن DEN نموذج معلومات يوفر تلخيصاً للجوانب والسياسات والأجهزة والبروتوكولات والخدمات. ويوفر ذلك نموذجاً موحداً للربط بين المستخدمين والتطبيقات وخدمات التشغيل الشبكي وإطار قابل للتوسع موجه نحو الخدمة.

- *البروتوكول سريع النفاذ للدليل (LDAP)* (النسخة 3 من LDAP) محدد في [b-IETF RFC 3377]. وهذا البروتوكول عبارة عن بروتوكول مخدم العميل للنفاذ إلى خدمة الدليل. ويستند نموذج معلومات البروتوكول إلى المدخل الذي يتضمن معلومات عن بعض المواضيع (مثل الأشخاص) ويتألف من نعوت لها نمط وقيمة أو أكثر من القيم. ولكل نعت تركيبة لغوية تحدد أنواع القيم المسموح بها في النعت وكيفية تصرف هذه القيم أثناء عمليات الدليل.
- *وحدة تحكم إدارة السياسات:* ويتفاعل البشر مع نظام إدارة السياسات من خلال وحدة تحكم الإدارة التي تعمل عموماً على الحواسيب الشخصية أو محطات العمل. ويمكن بدلاً من ذلك استخدام متصفح الويب في توفير نفاذ المدير من أي مكان تقريباً مصحوباً بالأمن على مستوى مواضيع السياسات الذي يستخدم للحد من السياسات التي يمكن تعديلها بواسطة فرد معين. ويجري من خلال وحدة تحكم الإدارة إدراج السياسات في الدليل. وتوفر وحدة الإدارة سطحاً بينياً بالأشكال البيانية للمستخدم فضلاً عن الأدوات اللازمة للمديرين لتعريف السياسات الشبكية بوصفها قواعد للعمل. كما يمكن أن تمنح المشغلين النفاذ إلى تشكيلات الأمن الأقل مستوى في المبادلات والمسيرات الفردية.

وتعمل عناصر النموذج المرجعي لإدارة السياسات بصورة بينية لتسليم العروة المغلقة لإدارة السياسات. ويتضمن ذلك تشكيل الأجهزة الطرفية، وإنفاذ السياسات في الشبكة والتحقق من وظيفة الشبكة كما يراها تطبيق المستخدم النهائي. وتشمل عملية إنفاذ السياسات على الشبكة ضوابط السماح للتطبيقات أو المستخدمين الذين يتنافسون على النفاذ إلى موارد الشبكة. ويمكن أن تتقدم إدارة السياسات بعض الشيء نحو تبسيط بيئة إدارة التشكيل داخل المؤسسات، والتقليل إلى أدنى حد ممكن من فرص حدوث أخطاء بشرية.

### 2.5.II تشديد أنظمة تشغيل المخدم

يعتبر تشديد أنظمة التشغيل عنصراً رئيسياً في ضمان أمن أنظمة المعلومات داخل طبقة أمن التطبيقات. وقد يكون للمؤسسة النمطية عدة أنظمة تشغيل مختلفة للتطبيقات المختلفة في عالم البيانات (بما في ذلك إدارة الشبكة) بل وكذلك لمخدمات التطبيقات التي تدعم المهاتفة ببروتوكول الإنترنت والتطبيقات كثيفة الاتصالات. ومن الأمور المألوفة وجود نسخ متعددة من نفس نمط أنظمة التشغيل المنتشرة في البنية التحتية لتكنولوجيا المعلومات مما يزيد من تعقيدات مهمة الأمن.

كما تستخدم أكثر أنظمة التشغيل شيوعاً في عالم البيانات بصورة أوسع نطاقاً في مخدمات التطبيقات التي تدعم المهاتفة عن طريق بروتوكول الإنترنت والتطبيقات كثيفة الاتصالات. ويعرض الموردون نسخة متشددة من هذه الأنظمة ببرمجيات أمنية متاحة لبعض الوظائف مثل الحماية من الفيروسات، وكشف الاقتحام، وتدقيقات التسجيل. وتبدأ عملية تشديد أنظمة التشغيل بالمتطلبات التي تقضي بتجنب استنساخ المخدم، وأن تكون الوسائط التي تحمّل منها أنظمة التشغيل موضع ثقة، وتمضي العملية من هذه النقطة. وينبغي فيما يتعلق بأنظمة التشغيل التي لا يتوافر لها دليل متشدد محدد، استشارة المورد للحصول على أحدث معلومات وإجراءات تشديد أنظمة التشغيل.

# التذييـــل III

# مثال على أمن الشبكة

(لا يشكل هذا التذيل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل أمثلة على ضمان أمن مختلف جوانب المنظمة أو المؤسسة الكبيرة باستخدام التقنيات التي نوقشت في هذه التوصية.

وعلى وجه الخصوص، تتحدد مبادئ وضع الحلول الأمنية القائمة على الطبقات لضمان أمن الجامعات بما في ذلك البوابات إلى الإنترنت، ومركز البيانات والمكتب البعيد والنفاذ عن بعد والمهاتفة ببروتوكول الإنترنت. وتستخدم التقنيات التي نوقشت في هذه التوصية لتبين أن أمن المؤسسة لا يقع في نموذج من حجم واحد يصلح للجميع. ويقدم الجدول 1.III مثالاً على الجوانب الأمنية الضرورية ذات الصلة. وتقدم المؤسسة 1 في المثال، وهي مؤسسة من الحجم الصغير تستخدم خطوطاً مادية خاصة محدودة بين المواقع، نفاذاً محدوداً عن بعد إلى الموظفين، ويتحقق وجود الويب من خلال مركز بيانات إنترنت يوفره مورد الخدمة (مسؤول عن إقامة بيئة أمينة). والمؤسسة 2 (في المثال) هي مؤسسة مفتوحة ذات نموذج أعمال يعزز الإنترنت من خلال إعطاء الشريك والمورد والزبون نفاذاً محدوداً إلى تطبيقات إدارة المؤسسة. ويدخل المستعملون الداخليون والخارجيون إلى شبكة المؤسسة في المثال 2 من البيت أو من المكاتب عن بعد أو من شبكات أخرى باستخدام أجهزة سلكية أو متنقلة.

**الجدول 1.III – دليل إلى الجوانب الأمنية ذات الصلة بالمؤسسة**

| مجال الشبكة | مثال مؤسسة 1 | مثال مؤسسة 2 |
|---|---|---|
| **تأمين حرم الجامعة** | نعم | نعم، تمثل أكثر متطلبات الأمن صرامة |
| **تأمين المكتب البعيد** | خيار التجفير على خطوط خاصة تقديرية أو مادية | نعم، بما في ذلك النفاذ إلى المكتب البعيد للإنترنت |
| **تأمين النفاذ عن بعد** | نعم، ولكن لنفاذ المراقمة الخاص فقط | نعم، بما في ذلك الشركاء والعملاء |
| **تأمين مركز البيانات** | نعم لمراكز البيانات الداخلية | نعم بما في ذلك مراكز بيانات الإنترنت |
| **تأمين المهاتفة ببروتوكول الإنترنت** | نعم | نعم بزيادة الشبكات الخاصة التقديرية |

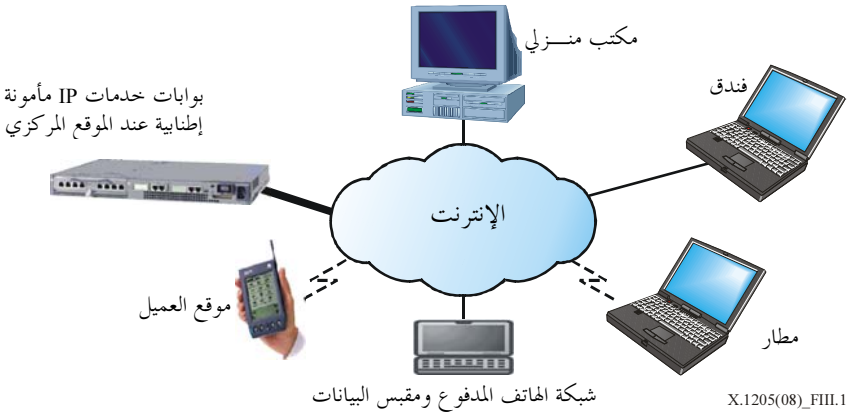
## 1.III تأمين النفاذ عن بعد

تتمكن المؤسسة أو المنظمة بفضل تكنولوجيات النفاذ عن بعد من استخدام الناس والموارد الموجودة في أي مكان. غير أن هذه التكنولوجيات تنطوي أيضاً على إمكانية التسبب في مشاكل أمنية للمؤسسة. ويمثل الموظفون فرادى في مؤسسة الذين يسافرون أو يعملون من منازلهم غالبية مستخدمي النفاذ عن بعد، إلا أن هذه الفئة تشمل أيضاً المكاتب الصغيرة التي تربط، بناءً على طلب، بشبكة المؤسسة. ويتم التصدي للتحديات الرئيسية من خلال أمن الشبكة والإدارة المأمونة للنفاذ. وينفذ أمن إدارة الشبكة في المواقع المركزية. ويفيد أمن التطبيقات من حيث إن الجهاز البعيد يحتاج إلى حماية من خلال برمجيات المسح المضادة للفيروسات، وجدران الحماية الشخصية.

وثمة خطر هام يتعلق بالمستخدمين عن بعد يتمثل في سرقة أجهزة المستعمل. وينبغي ألا تؤدي سرقة هذه الأجهزة إلى حدوث اقتحام في المجالات الأخرى لشبكة المؤسسة أو إلى النفاذ إلى المعلومات التي قد تكون محفوظة في النظام. ومن ناحية أخرى، يريد المستعملون المتنقلون أن يحملوا معهم أجهزتهم أو مطاريفهم من أجل النفاذ إلى الشبكة من أي مكان مما يجعل من الضروري تجفير المعلومات الحساسة المحفوظة في الأنظمة التي تستخدم للنفاذ عن بعد، ويفضل أن يتم ذلك باستخدام نظام يندمج بصورة وثيقة في الاستخدام العادي للتطبيقات. وتتيح أنظمة التجفير المتوافرة حالياً للمستخدم أن يعمل بصورة عادية دون أن يحتاج إلى عمليات تجفير وفك التجفير اليدوية أو الفردية للملفات. فعلى سبيل المثال، يمكن حفظ جميع أنظمة

"الملفات" في شكل مجفر مع دمج عملية فك التجفير في النفاذ العادي لنظام الملفات. وثمة شكل آخر من الأخطار يحدث عندما يعمل مستخدم النفاذ عن بعد على شبكة منطقة محلية لا سلكية، ربما من المنـــزل أو من فندق، ففي هذه الحالة فإن من الضروري أن يكون لديه جدار حافظ شخصي وبرمجيات مضادة للفيروسات.

وأكثر أشكال النفاذ عن بعد شيوعاً للاتصالات المتعلقة بالبيانات هو النفاذ بالمراقمة سواء بصورة مباشرة إلى المؤسسة أو إلى مورد خدمة الإنترنت، والنفاذ المباشر بالاعتماد على الإنترنت باستخدام خط مشترك رقمي أو أجهزة المودم الكبلية، أو شبكة الإثرنت المحلية (مثلما في الفنادق) وشبكات المنطقة المحلية اللاسلكية (مثلما في المطارات). كذلك فإن خدمات البيانات اللاسلكية العامة التي تدعم النفاذ إلى الإنترنت في زيادة كبيرة حيث توفر التنقل المتزايد للحاسوب المتنقل والحواسيب المحمولة يدوياً. وتسهم زيادة تيسر واقتصاديات الإنترنت في نموها السريع للنفاذ عن بعد عبر الشبكات الخاصة التقديرية باستخدام كل من النفاذ بالمراقمة والمباشر. ويقدم الشكل 1.III مثالاً على تأمين النفاذ عن بعد.




**الشكل 1.III – تأمين النفاذ عن بعد**

ويمكن باستخدام التقنيات الواردة في هذه التوصية، اتخاذ الخطوات التالية لتأمين النفاذ عن بعد:

1) *مراقمة النفاذ إلى موقع المؤسسة المركزي*

ينشئ مستخدم النفاذ عن بعد بالمراقمة نداء هاتفياً من مودم متصل بنظام الحاسوب الخاص به إلى أداة مودم (تسمى أيضاً تبديل نفاذ عن بعد) توجد في موقع المؤسسة المركزي أو الإقليمي. وينبغي تشكيل أنظمة النفاذ بالمراقمة بما يتيح استخدام نظام لإدارة النفاذ المأمون يوفر الاستيقان والترخيص للنفاذ على النحو الموصوف سلفاً. ويجري بسرعة الاستعاضة عن النفاذ بالتبديل المباشر، الذي كان يستخدم على نطاق واسع في ثمانينات وتسعينات القرن الماضي، بالشبكات الخاصة التقديرية للنفاذ عن بعد المعتمد على الإنترنت.

2) *الشبكات الخاصة الافتراضية (VPN) للنفاذ عن بعد*

يوفر النفاذ عن بعد المعتمد على الإنترنت مرونة هائلة وعرض نطاق كبير. وهناك أسلوبان: الشبكات الخاصة الافتراضية المعتمدة على أمن بروتوكول الإنترنت باستخدام عملاء الشبكة الخاصة الافتراضية للنفاذ عن بعد أو الشبكات الخاصة الافتراضية بالاعتماد على SSL استناداً إلى مقدرة SSL الخاصة بتصفح المستخدم.

3) *الشبكات الخاصة الافتراضية (VPN) المعتمدة على أمن بروتوكول الإنترنت*

أمن بروتوكول الإنترنت عبارة عن أسلوب طبقة الشبكة الذي يمكن استخدامه عبر التطبيقات (أي في حالة إقامة توصيلة لشبكة خاصة افتراضية تعتمد على أمن بروتوكول الإنترنت، يمكن للمستخدم أن يلجأ إلى البريد الإلكتروني، والتطبيقات ذاتية الخدمة وتصفح شبكة الإنترنت والنفاذ إلى التطبيقات المرخصة). ويحتاج عميل أمن بروتوكول الإنترنت إلى التحميل على حاسوب شخصي للاستخدام في النفاذ عن بعد. ويتوافر العملاء أيضاً للحواسيب المحمولة يدوياً. كما ينبغي تحميل الحاسوب الشخصي برمجيات الكشف عن الفيروسات.

وسواء أكان يعتمد على النفاذ بالمراقمة إلى مورد خدمة الإنترنت POP أو على النفاذ المباشر السلكي أو اللاسلكي، يقوم عميل الشبكة الخاصة الافتراضية باستيقان المستخدم ويتحقق من سلامة النظام الحاسوبي للمستخدم، ويقيم وصلة مأمونة (أو نفق) إلى المؤسسة. ويوفر عميل الشبكة VPN مقدرات (جدران وقاية مثلاً) لضمان أمن النظام البعيد بالذات لا سيما أثناء إقامة التوصيل بالمؤسسة. وتستعمل مرحلة إقامة الجلسة حركة مجفرة ومستيقنة إلى المؤسسة.

ويفترض أن تكون الشبكات الخاصة الافتراضية (VPN) للنفاذ عن بعد قادرة على كشف، وإن أمكن، تجاوز عقبات الإنترنت المشتركة مثل تحويل عنوان الشبكة NAT، وجدران الحماية غير المقيدة (أي إقامة وصلة إلى شبكة المؤسسة من داخل شبكة أخرى محمية بجدار حماية) أو على الأقل تزويد المستخدم عن بعد بالمعلومات عن طبيعة العقبات التي تقابل.

وعلى مستوى حافة المؤسسة، تتم مناولة التوصيلات الخاصة بالنفاذ عن بعد من الإنترنت بواسطة نظام بوابة أمن بروتوكول الإنترنت. وينبغي أن توفر حافة المؤسسة الحماية من نقطة فشل واحدة من خلال استخدام بوابات متعددة بمسيرات متعددة إلى الإنترنت. وبحسب نطاق المؤسسة، يوصى أيضاً بالفصل الجغرافي بين البوابات. وينبغي أن توفر البوابة عدداً من الجوانب اللازمة لدعم النفاذ الفعال عن بعد على نطاق المؤسسة. وتشمل الجوانب الموصى بها: التشكيل البسيط للعميل، ومقدرة تمرير التوصيلات إلى شبكة المؤسسة الداخلية وليس انتهائية الدورة وأن تكون قادرة على توفير وظيفية شاملة لجدار الحماية لتلافي الحاجة إلى جدار حماية منفصل. وعلاوة على ذلك، أن تتضمن البوابة طائفة من آليات الاستيقان مثل RADIUS وPKI وLDAP لزيادة المرونة لدى اختيار المستخدم مستوى الاستيقان. وينبغي أن تتيح البوابة للمؤسسة المرونة في إدراج مخططات أخرى مثل RADIUS، وهوية المستخدم/كلمات السر المعتمدة على الدليل أو حتى الاستيقان بالبطاقة الذكية أو الرمز على الحاسوب المتنقل الخاص بالمستخدم الذي قد يكون مستخدماً بالفعل. ويعتبر تقديم الدعم لكل من L2TP وPPTP مفيداً.

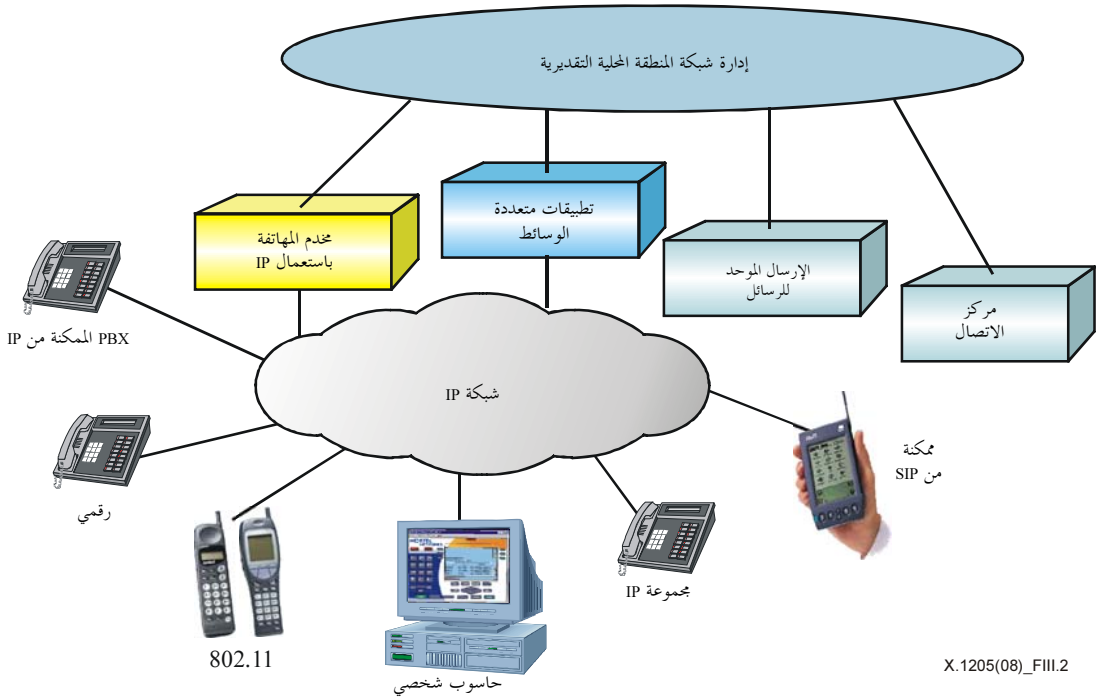
## 2.III تأمين المهاتفة ببروتوكول الإنترنت

بدأت المنظمات والمؤسسات في تطبيق الحلول المعتمدة على المهاتفة على بروتوكول الإنترنت على أمل جني منافع الاندماج في شبكة المنطقة المحلية وشبكة المنطقة الواسعة والتطبيقات المندمجة. ويمثل كل نظام لنقل الصوت باستعمال بروتوكول الإنترنت حلاً بواسطة المعدات/البرمجيات يتكون من مجموعة من أربعة أسس منطقية هي:

- المهاتفات ببروتوكول الإنترنت وعملاء الحواسيب الشخصية.
- مخدمات الاتصالات (وكذلك تسمى مخدمات أو حراس بوابات إدارة النداءات).
- بوابات الوسائط التي توفر النفاذ المرن للشبكة. (مثلاً، عن طريق PBXs التقليدية والشبكة الهاتفية العمومية التبديلية (PSTN) والشبكة اللاسلكية العامة وما يتجاوزها).
- مخدمات التطبيقات (مثل التطبيقات الموحدة لإرسال الرسائل وعقد المؤتمرات والتطبيقات التعاونية المعتمدة على SIP).

وهذه الوظائف فضلاً عن مخدمات تطبيقات الاتصالات ذات الصلة مثل تلك التي تدعم مركز الاتصال والتطبيقات الموحدة لإرسال الرسائل موزعة عبر شبكة ببروتوكول الإنترنت تعمل بالمهاتفة أو على مستوى المنشآت التجارية، التي تسلم المستويات المطلوبة من الموثوقية وإدارة نوعية الصوت والازدحام. ويوفر الوصول الموسع والانتقالية عبر شبكات المنطقة المحلية اللاسلكية وعبر الإنترنت عن طريق الشبكات الخاصة التقديرية ببروتوكول الإنترنت.

ويبين الشكل 2.III أسلوب المنظمة التقليدي إزاء تأمين المهاتفة باستعمال بروتوكول الإنترنت.




**الشكل 2.III – تأمين المهاتفة ببروتوكول الإنترنت**

والمهاتفة ببروتوكول الإنترنت عبارة عن تطبيقات تعمل على شبكة عاملة ببروتوكول الإنترنت وتزيد من وظائفية الأمن التي توفرها الشبكة. وعلى العكس من معظم تطبيقات البيانات، تعتبر مهاتفة IP حساسة للوقت وهو ما يعد عنصراً حاسماً لتشغيل المنشأة التجارية. ويمكن لأنظمة المهاتفة ببروتوكول الإنترنت، شأنها شأن تطبيقات البيانات الأخرى، أن تتعرض لعدد من الهجمات مثل:

- هجمات على المسير يمكن أن تعطل كلاً من الخدمات الصوتية والبيانية في المنظمة؛
- يمكن أن يؤدي رفض الخدمة إلى إرهاق مخدم أو عميل الاتصالات بالمهاتفة ببروتوكول الإنترنت؛
- ضربات الموت يمكن أن تعطل عمليات نقل الصوت باستعمال بروتوكول الإنترنت من خلال إرسال ضربات متعددة إلى أجهزة نقل الصوت باستعمال بروتوكول الإنترنت (VoIP)؛
- يمكن أن يؤدي مسح المنافذ إلى اكتشاف نقاط ضعف في عملاء ومخدمات نقل الصوت باستعمال بروتوكول الإنترنت؛
- التجسس على الرزم يمكن أن يسجل و/أو يعترض المحادثة؛
- الاحتيال باستعمال بروتوكول الإنترنت يمكن أن يسيء عرض المصدر أو المقصد للوسائط أو تدفق التشوير؛
- يمكن أن تهاجم الفيروسات والفيروسات المتسللة والفيروسات المتخفية والقنابل الزمنية المخدمات والعملاء.

وقد تتعرض المهاتفة باستعمال بروتوكول الإنترنت لأضرار. فعلى سبيل المثال، كانت هناك حالات استولى فيها بعض المبرمجين المقتحمين على عملاء بروتوكول الإنترنت نتيجة لتباطؤ إدارة كلمات السر في إحدى الحالات ونتيجة لجوانب الضعف المرتبطة بإدارة XML (انظر [b-W3C XML 1.0])، في حالة أخرى. وقد تشكل هذه الهجمات خطراً بالدرجة الأولى لدى تشغيل نقل الصوت باستعمال بروتوكول الإنترنت محلياً عبر الإنترنت، ودرجة أقل من الخطر لدى استخدام مهاتفة بروتوكول الإنترنت بصورة كاملة داخل المؤسسة أو على التوصيلات المحاطة بالنفق عبر الإنترنت.

ويتعين، مثلما الحال في جميع التطبيقات، إجراء تقييم للمخاطر التي تتعرض لها المهاتفة باستعمال بروتوكول الإنترنت، لتقييم قيمتها الذاتية، وانعكاسات الخسارة المدركة داخل المنظمة والسياسة الأمنية الموضوعة. والمهاتفة عبارة عن وظيفة رئيسية في المنشأة التجارية ولذا سوف يتعين حماية نظام المهاتفة بأكمله، مثله مثل الشبكة ذاتها، من الأخطار الأمنية والهجمات.

وعموماً، فإن المطلوب من مستخدمي المهاتفة ألا يتجاوز استيقان أنفسهم بشأن النفاذ بعيداً عن الشبكة باستخدام مجموعة جوانب يطلق عليها اسم النفاذ للنظام الداخلي المباشر (DISA). ومن ناحية أخرى، ليس من غير الشائع أن يطلب من مستخدمي البيانات استخدام هويات وكلمات سر متعددة للنفاذ إلى الشبكة والتطبيقات. ويتعارض هذا التعقيد مع تأمين محيط المؤسسة. وسوف تكون البساطة أكثر أهمية بالنسبة لنقل الصوت باستعمال بروتوكول الإنترنت، حيث إن التوقع هو أن تكون هناك نغمة مراقمة فورية. ولا حاجة للقول بأن آليات أمن خدمات نقل الصوت باستعمال بروتوكول الإنترنت (VoIP) لا تستطيع أن تعوق التوصيلية اللازمة ونوعية الصوت.

وتشمل المبادئ التوجيهية الرئيسية لضمان أمن المهاتفة ببروتوكول الإنترنت ما يلي:

1) تعمل حلول المهاتفة ببروتوكول الإنترنت في المؤسسة، داخل حدود المؤسسة، وبالتشغيل البيني مع شبكة عامة فوق توصيلات تبديل بالدارة.

2) تعتمد أنظمة المهاتفة ببروتوكول الإنترنت في المؤسسة على البنية التحتية للتشغيل البيني ببروتوكول الإنترنت التي يتم تأمينها من زاوية البيانات وهندستها وتصميمها لتحقيق متطلبات الكمون والموثوقية في المهاتفة.

3) مخدمات توصيلات المهاتفة ببروتوكول الإنترنت في المؤسسة عنصر أساسي في المنشآت التجارية وهي مؤمنة مادياً ومحمية من الهجمات الداخلية والخارجية.

4) يتوفر الاستيقان المأمون لعملاء خدمة نقل الصوت باستعمال بروتوكول الإنترنت (VoIP).

5) لا توجد حاجة لتجفير الصوت إلا عندما تعبر وسائط مشتركة شبكة المنطقة المحلية أو عبر الإنترنت.

6) يتوفر أسلوب شامل إزاء الأمن عبر بيئة المهاتفة بأكملها بما في ذلك عملاء ومخدمات نقل الصوت باستعمال بروتوكول الإنترنت ومخدمات التطبيقات (مثل برمجيات الإرسال الموحد للرسائل ومراكز الاتصال) ومبادلات PBX التقليدية.

ويتطلب تأمين حلول المهاتفة ببروتوكول الإنترنت وجود أسلوب منسق عبر جميع طبقات الشبكة. وتضمن إدارة السياسات وإدارة النفاذ المأمون استيقان المستخدم والتحكم في جوانب المهاتفة وقدرات النداءات. وينبغي استخدام تقنيات الإدارة المأمونة لحماية أجهزة الخدمات الصوتية مثل مخدمات الاتصالات وبوابات الوسائط. ويمكن تعزيز آليات الأمن التي وضعت لحماية البيانات لكي تستخدم في نقل الصوت باستعمال بروتوكول الإنترنت وذلك مثلاً من خلال استخدام أمن بروتوكول الإنترنت لتأمين النفاذ عن بعد، وتوصيلية الفرع والنفاذ إلى شبكة المنطقة المحلية اللاسلكية. ويمكن تحقيق أمن إضافي من خلال إدارة السياسات بإضافة التفتيش الشامل للخدمات الصوتية إلى جدران الحماية ووظيفية تحويل عناوين الشبكة. ويمكن تحقيق أمن التطبيقات بعدة رسائل من بينها تشديد نظام التشغيل والحماية من الفيروسات المركبة في أجهزة المستعمل.

### 1.2.III تأمين مخدمات التطبيقات والتوصيلات المتعلقة بالمهاتفة ببروتوكول الإنترنت

يتمثل صلب نظام المهاتفة ببروتوكول الإنترنت، في مخدم الاتصالات الذي قد يكون مخدماً قائماً بذاته أو مدمجاً مع مدير اتصالات الأعمال PBX العاملة ببروتوكول الإنترنت. كذلك فإن مخدمات التطبيقات لا تقل عن ذلك أهمية حيث تقوم بتسليم مركز الاتصال والتطبيقات المتعددة الوسائط وأنظمة الإرسال الموحد للرسائل وأنظمة الرد الصوتي التفاعلي ذاتي الخدمة. وتبدأ عملية تأمين هذه المخدمات بتشديد أنظمة التشغيل على النحو السابق وصفه.

### 2.2.III تأمين عملاء خدمة نقل الصوت باستعمال بروتوكول الإنترنت (VoIP)

تدعم الحلول ذات الصلة بنقل الصوت باستعمال بروتوكول الإنترنت طائفة عريضة من العملاء وتشكيلات النفاذ بما في ذلك الهواتف السلكية واللاسلكية باستخدام بروتوكول الإنترنت IP والعملاء المؤقتين المعتمدين على الحواسيب الشخصية. فعندما توصل بشبكة IP تكون معرضة للهجمات.

وهناك عدد من بروتوكولات تشوير مختلفة للمهاتفة مثل SIP. وتستخدم عملية تشوير الحركة عموماً TCP على مستوى النقل. وسوف تتوافر في المستقبل القدرة على تأمين حركة التشوير عند عملاء نقل الصوت باستعمال بروتوكول الإنترنت بصفه عامة. ويجري في أنظمة المهاتفة باستعمال بروتوكول الإنترنت، ترزيم الإشارة الصوتية باستخدام معيار مثل التوصية [b-ITU-T G.729] (عند 8 kbit/s) وخوارزمية كشف نشاط الكلام وباستخدام بروتوكول في الوقت الحقيقي مع UDP عند مستوى النقل.

وهناك فروق شاسعة بشأن كيفية خفض المخاطر التي تتعرض لها هواتف IP وعملاء الهواتف المؤقتين بالاعتماد على الحاسوب الشخصي، إلى أدنى حد ممكن. وهواتف IP عبارة عن تطبيقات لدى العميل للمهاتفة فقط. ولا يوجد حفظ أو أرصدة على الهاتف ذاته للحماية (باستثناء وجودها على الشبكة بوضعها في جهاز موثوق به). وتحديد القائم بالنداء، والنداء ذاته هما الرصيدان الوحيدان اللذان يجري حمايتهما. وتستخدم أجهزة المهاتفة هذه، في الغالب الشائع، بروتوكول ملكية عميل مؤقت يعتمد على مخدم التوصيلات للجوانب/الوظيفية والأمن. ويتعارض هذا الأسلوب مع حالات التنفيذ التي تعتمد على XML في مجموعة نقل الصوت باستعمال بروتوكول الإنترنت (VoIP) الصوتية لتشغيل الجوانب مما قد يشكل نقطة ضعف.

ويوجد عملاء نقل الصوت باستعمال بروتوكول الإنترنت (VoIP) المؤقتين في أجهزة المستعملين مع التطبيقات والأرصدة الأخرى، ومديرو أنظمة التشغيل المتوافرة على نطاق واسع. وقد يكون الهجوم الناجح باهظ التكلفة حيث يوجد العديد من الأرصدة القليلة على الحاسوب الشخصي بما في ذلك التطبيقات والأعمال والبيانات المالية والشخصية. وتتمثل الممارسة الشائعة في استخدام واحد أو عدد من التطبيقات الأمنية الموجودة في لوحات الحاسوب الشخصي مما يوفر جدران حماية شخصية والكشف عن الفيروسات وعملاء الشبكة الخاصة التقديرية ببروتوكول الإنترنت. ويمكن بالنسبة لعملاء نقل الصوت باستعمال بروتوكول الإنترنت (VoIP) المؤقتين استخدام نفس الآليات المطبقة على البيانات.

### 3.2.III تأمين خدمة نقل الصوت باستعمال بروتوكول الإنترنت في علبة التوزيع وعبر حرم الجامعة

هناك وسيلتان لتسليك أجهزة بروتوكول الإنترنت في شبكة حرم جامعة: وسائط مشتركة وإثرنت مبدلة مخصصة. ويميل الاتجاه العام للصناعة إلى إثرنت المبدل المخصص، ويرجع ذلك إلى تزايد الحركة ومتطلبات القدرة على الإدارة. وعلاوة على ذلك، فإن الأمن والقدرة على الإدارة تدفعان إلى نشر شبكات المنطقة المحلية الافتراضية (انظر [b-ISO/IEC 18028-5]) في شبكات المؤسسات. وتوفر شبكات المنطقة المحلية اللاسلكية بديلاً ثالثاً أخذ في الظهور في بعض البيئات مثل التعليم والرعاية الصحية.

ومع إدخال المهاتفة ببروتوكول الإنترنت، يوصى بشدة بربط عملاء VoIP المؤقتين وتجهيزات هذه الخدمات VoIP ببيئات إثرنت المبدلة حتى سطح المكتب. ويحقق أعلى المتطلبات التالية:

- التقليل إلى أدنى حد ممكن من كمون الخدمة VoIP من خلال إلغاء عملية CDMA من عملية إثرنت للوسائط المشتركة؛
- تعزيز أمن الخدمة VoIP من خلال حظر إمكانية التنصت من السطوح المكتبية الأخرى على نداءات الخدمة VoIP.

وعلاوة على ذلك، قد تختار المؤسسات التجميع المنطقي لهواتف VoIP في شبكات المنطقة المحلية التقديرية الخاصة بها لتيسير عملية الإدارة.

ويمكن أن تعزز المهاتفة ببروتوكول الإنترنت بدرجة كبيرة من إنتاجية المستخدمين باستخدام شبكات المنطقة المحلية اللاسلكية جوانب/وظيفية المهاتفة في المؤسسة التي تمتد من السطح المكتبي إلى، مثلاً، قائمة الاجتماعات أو حجرة الدراسة. ونظراً للطابع العدائي لشبكات المنطقة المحلية اللاسلكية هذه، تتمثل المعمارية الموصى بها في تأمين كل من مستويات الإشارة والخطط الصوتية على المقطع اللاسلكي. ويمكن تحقيق ذلك بتشكيل العملاء المؤقتين الذين يقيمون مع عميل للشبكة الخاصة التقديرية ببروتوكول الإنترنت على سطح مكتبي. ويمكن بدلاً من ذلك إدراج التجفير والاستيقان من خلال بعض هواتف في شبكة المنطقة المحلية اللاسلكية. ويوفر كلا الأسلوبين قدراً وافراً من الاستيقان والتجفير لبيئات شبكة المنطقة المحلية اللاسلكية.

### 4.2.III تأمين الفروع فيما يتعلق بالمهاتفة ببروتوكول الإنترنت

هناك عدد من الأساليب لدعم حلول المكتب البعيد وفرع الخدمة VoIP. وتشمل هذه الأساليب هواتف الخدمة VoIP، والعملاء المؤقتين الذين يدعمون حلول "المكتب في الصندوق". وتعزز الأساليب الأخرى بصورة كاملة من الطابع المنتشر

للخدمة VoIP من خلال نشر العملاء بعيداً عن المخدم المركزي. ويوصى في جميع الحالات، بإقامة حركة الخدمة VoIP في فرع ينفذ بأمان على شبكة خاصة تقديرية تعمل ببروتوكول الإنترنت، للبيانات.

### 5.2.III تأمين النفاذ عن بعد للمهاتفة ببروتوكول الإنترنت

يمكن أن تعزز المهاتفة ببروتوكول الإنترنت بصورة كبيرة من إنتاجية المستخدمين البعيدين سواء أكانون يعملون من منازلهم أم في فندق أم على الطريق حيث يوسعون في جميع الأحوال من جوانب/وظائفية المهاتفة من سطح المكتب إلى الموقع البعيد. وسيقيم عملاء VoIP المؤقتون للشبكة الخاصة التقديرية على جهاز الحاسوب المتنقل لخدمة الموظفين سريعي التنقل. وسوف يستخدم نفس هذا التشكيل للاستفادة من نقاط النفاذ لشبكة المنطقة المحلية اللاسلكية في الفنادق والمطارات ومراكز الاجتماعات. وسوف توفر هواتف الخدمة VoIP اتصالات غنية الجوانب للمحاسبين عن بعد ووكلاء مركز الاتصالات مع توافر الأمن من الشبكة الخاصة التقديرية العاملة ببروتوكول الإنترنت من مكتب منـــزلي.

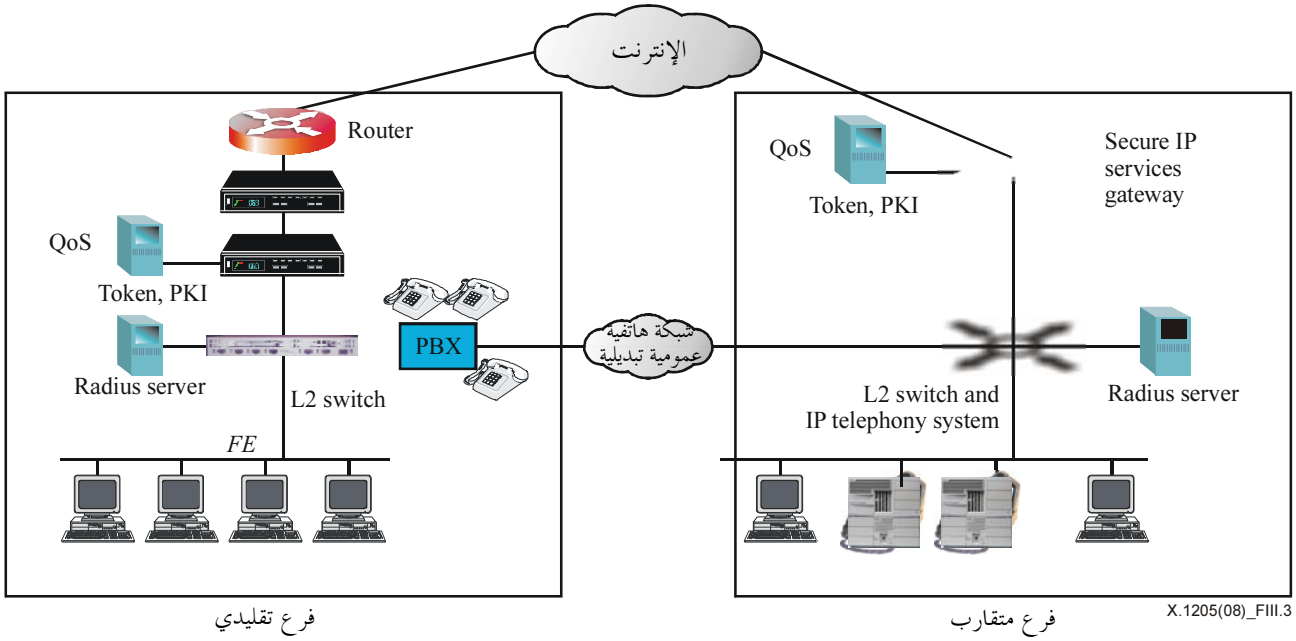
### 6.2.III أمن إدارة الشبكة لأغراض المهاتفة ببروتوكول الإنترنت

ينبغي، من زاوية الإدارة، تشكيل منفذ إثرنت مخصص مادياً. وينبغي أن يكون ذلك جزءاً من إدارة شبكة المنطقة المحلية التقديرية مع وقف جميع أشكال الحركة غير الإدارية على مستوى المسير عن طريق قوائم النفاذ وأمن المحيط. ويمكن توفير النفاذ خارج الشبكة للموردين والقائمين على دمج النظام و/أو VAR عن طريق الشبكات الخاصة التقديرية العاملة ببروتوكول الإنترنت. وينبغي إغلاق المنافذ غير المستخدمة (مثل، لوحدة التحكم أو النفاذ للمودم البعيد). وينبغي ألا تشغل هذه المخدمات سوى برمجيات التطبيقات المرخصة. وينبغي استخدام الأمن متعدد المستويات بمختلف مستويات الميزات (الرصد والتشكيل والتحكم) لاستيقان موظفي التشغيل. وكلمات سر المستخدمين محفوظة بأمان، وإدارة صياغة كلمات السر وتقييدها مضبوطة بصرامة. ويمكن اختيارياً تجفير حركة الإدارة (مثل معلومات الفواتير) حتى لأغراض الإرسال الداخلي من خلال تكنولوجيا الشبكة الخاصة التقديرية.

## 3.III تأمين المكتب البعيد

قد يكون المكتب البعيد من أي حجم ابتداء من سطح مكتب عامل من منـــزله إلى حرم مؤسسة كبير. وعلى الرغم من أن هناك عناصر كثيرة مشتركة بين "المكتب البعيد" "والنفاذ عن بعد"، يمكن التفريق بينهما من خلال استمرارية قدرات الاتصالات ثنائية الاتجاه بين الموقع البعيد وبقية المؤسسة. أي أن المكتب البعيد عبارة عن مكان عمل يربط بصورة مستمرة ببقية المؤسسة، ويستطيع أن يتبادل الرسائل مع بقية المؤسسة خلال ساعات العمل. ومن ناحية أخرى فإن النفاذ عن بعد عبارة عن توصيلة مؤقتة بالمؤسسة تقام بناءً على طلب من مستخدم أو مستخدمي النفاذ عن بعد

ويعبر التشكيل البيني للفرع أكثر وسائل تسليم الخدمات أهمية وكثافة في التكاليف في كثير من الصناعات مثل الخدمات المصرفية بالتجزئة والرعاية الصحية والحكومات. ويستند التشغيل البيني التقليدي للفروع إلى مختلف تكنولوجيات شبكة المنطقة المحلية وإلى مسيرات بروتوكولات متعددة تعمل في شبكات ترحيل للأرتال مع احتياطي مبدل لدارة ISDN. وقد أحدثت أربعة تطورات رئيسية فرصاً رئيسية لتحويل التشغيل البيني للفروع: 1) التقارب على الإثرنت بوصفه معيار الشبكة المنطقة المحلية، 2) القبول العالمي لبروتوكول الإنترنت بوصفه بروتوكول الاختيار، 3) الإنترنت، 4) تزايد قائمة خدمات الشبكة الخاصة التقديرية من الطبقتين 2 و3. غير أن هذه التطورات أظهرت أيضاً طائفة من التحديات الأمنية ولا سيما بالنسبة للمنظمات والمؤسسات الكبيرة. وسيرد ذلك في الشكل 3.III.




**الشكل III.3 – تأمين المكتب البعيد**

تشمل متطلبات حافة شبكة المنطقة الواسعة على مستوى الفرع التسيير فيما بين شبكات المنطقة المحلية التقديرية محلياً وداخل الشبكة، ونوعية الخدمة وإدارة عرض النطاق والسطح البيني القابل لتغيير الحجم في الشبكة المتعلقة بشبكة المنطقة الواسعة ويشمل ذلك دعم مخطط الكبسلة فوق شبكة المنطقة الواسعة وأي مستوى للموثوقية يكون ملائماً. ويعتبر الأمن الذي يحقق مردودية تكاليفه عبر الإنترنت (بل وحتى على موصل الأرتال) مطلباً رئيسياً. لذلك تشكل إدارة التحول من التكنولوجيات التقليدية لشبكة المنطقة الواسعة المأمونة نسبياً إلى الشبكات الخاصة التقديرية العاملة ببروتوكول الإنترنت، تحدياً. فبعض المؤسسات تريد الحصول على نفاذ مباشر للإنترنت من مكتب بعيد مما يبرز الحاجة إلى جدران حماية بعيدة. وتريد مؤسسات أخرى توصيلة مسيرة دينامياً يعتمد عليها بدرجة كبيرة بين الفروع وصلب المؤسسة مع إدراج جدران الحماية المركزية في شبكة الإنترنت على أن يستخدم في بعض الحالات مرحل الأرتال كمسير رئيسي والإنترنت كاحتياطي أو التحرك نحو الشبكات الخاصة التقديرية باستعمال بروتوكول الإنترنت بوصفها التشكيل الرئيسي. ويستخدم التسيير الديناميي لتعزيز القدرة على تغيير الأحجام والموثوقية بواسطة:

- المعرفة الأوتوماتية بطوبوغرافية الشبكة؛
- المعرفة الأوتوماتية بعناوين المستخدمين النهائيين عبر المؤسسة؛
- التكييف الأوتوماتي مع التغييرات في طوبوغرافية الشبكة.

غير أن الأمن في الشبكات المسيرة لا يأتي إلا متأخراً وليس كمطلب من مقتضيات اليوم الأول. فعلى سبيل المثال، لم تكن هناك أية وسيلة فعالة لإدارة التسيير الديناميي على الأنفاق المحفرة للشبكة الخاصة التقديرية، وكانت إدارة هذه الأنفاق في منتهى الصعوبة.

وقد أدى ما أشير إليه أعلاه، عموماً، إلى أن تقوم المؤسسة بشراء وتركيب وصيانة وإدارة أجهزة أمن وتشغيل بيني متعددة للمكتب البعيد وشبكات الفروع مما تسبب في تعقيد هذه العوامل وصعوبة إدارتها.

ويتعين مع الانتقال إلى الشبكات الخاصة الافتراضية باستعمال بروتوكول الإنترنت، تحقيق مجموعة كاملة من المتطلبات الأمنية تحقق مردودية تكاليفها قدر المستطاع. ويشمل ذلك وظائف أمن الشبكة مثل التسيير ببروتوكول الإنترنت على أنفاق مأمونة، والشبكة الخاصة الافتراضية والتجفير وتفتيش جدار الحماية الشاملة عند الطبقة المعاقة من الشبكة واستيقان المكتب البعيد وخدمات الدليل عند طبقة دارة النفاذ المأمون، على أن يوفر جميع ذلك بطريقة عالية التكامل. ويتعين دمج إنفاذ إدارة السياسة الأمنية في هذا الحل مما يتيح تزويد كل مستخدم بملامح أمنية فريدة تظل مع كل مستخدم بصرف النظر عما إذا كان

هو أو هي يسجل من حاسوبه الشخصي في المنـــزل عبر الإنترنت العامة أو يرتبط محلياً داخل مكتب الفرع. كما يتعين توسيع أمن إدارة الشبكات ليشمل المكتب البعيد دون عناصر جانبية قد تضر بأمن الشبكة. وأخيراً يتعين توفير أمن التطبيقات إذا كانت مخدمات البيانات و/أو المهاتفة ببروتوكول الإنترنت قد نشرت عند المكتب البعيد.

### 4.III تأمين شبكة المنطقة المحلية اللاسلكية

تتزايد فرص التواصل فيما بين المقار الرئيسية للمؤسسة والمكاتب الفرعية والموظفين العاملين عن بعد والخبراء الاستشاريين وشركاء في الأعمال التجارية. وأصبح بإمكان الشركات الآن أن تعزز من التكنولوجيات اللاسلكية الجديدة للمعيار IEEE 802.11 (انظر [b-IEEE 802.11]) للقيام بأعمالها في أي وقت وفي أي مكان. غير أن هناك حاجة تتزامن مع هذا الحل تتمثل في إدارة النفاذ للمستخدمين بطريقة مركزية وفعالة مع العمل في نفس الوقت على ضمان أمن موارد المنظمة.

فشبكات المنطقة المحلية اللاسلكية عرضة بوجه خاص للانتهاكات الأمنية. فاعتراض الاتصالات على شبكة منطقة محلية نمطية يتطلب النفاذ الماضي إلى البنية التحتية للتكبيل. ومن ناحية أخرى فإن عمليات الإرسال اللاسلكية تخضع للاعتراض في الهواء وتعرض الشبكة لعمليات اقتحام من أي شخص لديه بطاقة شبكة منطقة محلية لا سلكية نمطية.

وتوسع شبكات المنطقة المحلية اللاسلكية من الشبكات المؤسسية باستخدام أجهزة لا سلكية والبروتوكول المشار إليه في المعيار IEEE 802.11. وتشمل التجهيزات في شبكات المنطقة المحلية اللاسلكية بطاقات السطح البيني للشبكة اللاسلكية للتجهيزات المتنقلة مثل أجهزة الحاسوب المحمولة، وتلك المستخدمة على السطوح المكتبية، والتي يشار إليها جميعاً بأنها الوحدة أو المحطة المتنقلة. وتتيح بطاقات السطح البيني للشبكة اللاسلكية (NIC) حمل إشارات الشبكة من جهاز التوصيل من خلال جهاز وسيط، وهو بوابة شبكة المنطقة المحلية اللاسلكية أو المحور المعروف بنقطة النفاذ اللاسلكي (AP) التي تحول الإشارات اللاسلكية إلى إشارات على خط سلكي يتم حملها على الشبكة السلكية.

ويمكن للشركات باستخدام محور أو مبدل إثرنت، ربط نقاط إلى شبكات المنطقة المحلية اللاسلكية بشبكة منطقة محلية سلكية بنفس السهولة التي تضيف بها مستخدماً سلكياً. وتضمن نقطة النفاذ، من خلال ربط نقاط النفاذ ببدالة، Mbit/s 100/10 مخصصة مما يتيح لجميع نقاط النفاذ المتوافرة التصرف مثل بدالة دون حاجة إلى أن تتنافس للحصول على جزء من عرض نطاق المحور السلكي.

ويتكون المعيار الأصلي [b-IEEE 802.11] من مجموعة من المواصفات التي يتوافر منها الآن 802.11a وIEEE 802.11b وIEEE 802.11g وIEEE 802.11.i والتي تستخدم استناداً إلى بيئة إشارة الشبكة مع مقايضات بين المسافة وعرض النطاق.

#### 1.4.III قضايا أمن الشبكة المحلية اللاسلكية

ما زالت إشارات الشبكة المحلية اللاسلكية، بصرف النظر عن آليات أمن هذه الشبكة، ترسل وتستقبل عبر الهواء عن طريق موجات راديوية ومن ثم لا يوجد لديها أية حواجز مادية أمام المستخدم غير المرخص. غير أن هذه الإشارات تخضع، للأسف، للاعتراض وربما الاقتحام في شبكة المؤسسة. لذا تتضمن إضافة عقدة لا سلكية إلى شبكة المؤسسة احتياطات أمنية ملائمة وممارسات أمنية جيدة من أجل حماية جميع محتويات الشبكة WLAN.

وتتألف طبقة البنية التحتية للشبكات WLAN من جميع مكونات الشبكة والكبلات والتوصيلات البينية ووسائط الإرسال (منطقة التغطية). مثال: نقاط النفاذ والمحطات المتنقلة، البوابات والخدمات المصاحبة للمخدمات المضيفة مثل RADIUS وDNS وغيرها.

وتتألف طبقة الخدمة من خدمات النفاذ إلى الشبكة LAN اللاسلكية والخدمات الأخرى التي تمكن النفاذ اللاسلكي مثل الاستيقان والترخيص والمحاسبة (AAA) وخدمات إدارة المفاتيح وغيرها.

وتشمل الأخطار الأمنية التي تسببها شبكات المنطقة المحلية اللاسلكية ما يلي:

- انتهاكات لسرية وسلامة الحركة اللاسلكية. فقد يمكن لأي مهاجم أن يعترض الاتصالات فيما بين حاسوب متنقل ونقطة نفاذ لا سلكية (AP) ومن ثم الاستيلاء على معلومات حساسة أو سرية ليست موجهة لطرف ثالث. وعلى العكس من ذلك، قد يمكن لأي مهاجم إدراج معلومات في معاملات أصلية دون علم المستخدمين الشرعيين.
- تعرض شبكة المنطقة المحلية للمؤسسة. ما لم تكن المنصات المتنقلة مستيقنة بصورة مأمونة، فإنه يمكن للمهاجم أن يتصل ببساطة بشبكة المنطقة المحلية اللاسلكية باستخدام جهاز متطابق مع المعيار IEEE 802.11، ويصبح محطة "مرخصة" على شبكة المنطقة المحلية اللاسلكية ومن ثم الحصول على النفاذ إلى الشبكة المحلية للمؤسسة.

ويمكن باستعمال نموذج التهديد الوارد في التوصية X.800 تلخيص أنواع الهجوم على النحو التالي:

| **نموذج التهديد حسب التوصية X.800** | **طرائق الهجوم** |
|---|---|
| إتلاف المعلومات و/أو الموارد الأخرى | اقتحام نقطة نفاذ |
| إفساد المعلومات أو تغييرها | كسر مفتاح البروتوكول WEP، هجوم المعترض |
| سرقة المعلومات و/أو الموارد الأخرى أو حذفها أو إضاعتها | اقتحام نقطة نفاذ، كسر مفتاح بروتوكول WEP، هجوم معترض، انتحال عنوان MAC، أجهزة احتيال، اقتناص الشبكة، اختطاف الطبقة 3، شبكات مخصصة |
| إفشاء المعلومات | اقتحام نقطة نفاذ، كسر مفتاح البروتوكول WEP، هجوم معترض، انتحال عنوان MAC، أجهزة احتيال، اقتناص شبكة، اختطاف الطبقة 3، شبكات مخصصة |
| انقطاع الخدمة | تشويش راديوي مقصود، فيضان البيانات، اختطاف الطبقة 2، نقطة نفاذ كاذبة، رتل خادع لزعزعة الاستيقان، هجوم FATA-Jack على نظام DoS |

وتتطلب شبكات المنطقة المحلية اللاسلكية، شأنها شأن الشبكات السلكية، ضوابط تتعلق بالسرية والسلامة والنفاذ. وتتمثل المشكلة الأمنية الرئيسية في الشبكات اللاسلكية في أن باستطاعة الخارجيين الاستقبال أو الإرسال إلى شبكة المنطقة المحلية اللاسلكية ومنها بصرف النظر عما إذا كان هذا العنصر الخارجي يعتبر خارج المدى.

ويتيح ذلك للمهاجمين التنصت وإدراج نقاط نفاذ لا سلكية (AP) (ويشار إليها بنقاط النفاذ اللاسلكية الحمراء)، وإطلاق الهجمات مثل هجمات المعترض واختطاف الدورة، ومهاجمة مستخدمي شبكة المنطقة المحلية السلكية بسهولة من داخل هذه الشبكة. وعلى ذلك يستطيع المهاجم أن يحتال على المستخدم للتوصيل مع نقطة النفاذ اللاسلكية للمهاجم مما يفرض عقدة شرعية على الشبكة ومن ثم يتقاسم هويات المستخدم وكلمات السر وغير ذلك من المعلومات الخاصة بحرية ودون رغبة.

ويمكن استخدام التقنيات التالية لتأمين البيئة اللاسلكية:

- أسماء الشبكات: مجموعة هويات الخدمة (SSID)
- تسجيل البطاقة: قائمة التحكم في النفاذ MAC (ACL).
- تجفير المفتاح المشترك: من خلال استخدام بروتوكولات الأمن (مثل WPA/WPA2).

وعلاوة على ذلك، يمكن استخدام أنماط الاستيقان التالية:

- استيقان النظام المفتوح: يمكن لأي فرد يمتلك مجموعة هويات الخدمة في نقطة النفاذ اللاسلكية من الحصول على النفاذ.
- استيقان المفتاح المشترك: يكون لدى المستخدم سر مشترك حتى يمكن استيقانه.

ويحدث التجوال المأمون، في مواصفات [b-IEEE 802.11] الأصلية، من خلال الاستيقان المسبق للوحدة المتنقلة إلى نقطة النفاذ اللاسلكية المحيطة. ولا توجد رسائل ترحيل فيما بين نقاط النفاذ اللاسلكية حيث إن جميع هذه النقاط والوحدات المتنقلة تستخدم نفس المفتاح المشترك مما يمكّن نقطة النفاذ اللاسلكية الجديدة من افتراض سلامة استيقان الوحدة المتنقلة. وعلى ذلك يكون الترحيل سريعاً إلا أن الاستيقان يكون أقل أمناً نظراً لأن أرتال الإدارة تكون غير مستيقنة.

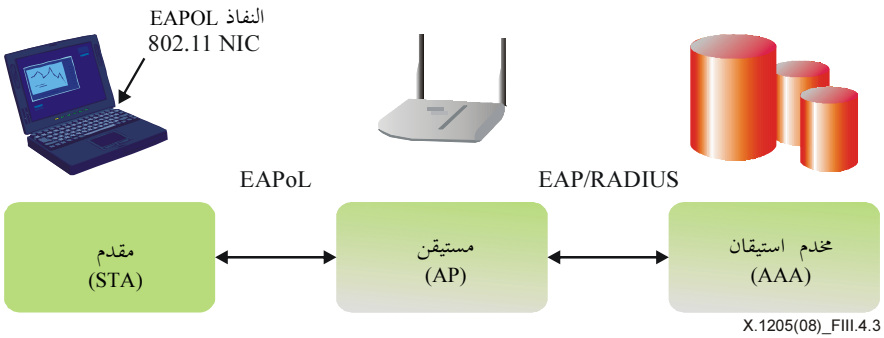
### 2.4.III متطلبات الأمن وآلياته داخل نقطة النفاذ اللاسلكية وأمامها

تتمثل الطريقة الوحيدة لحماية الطابع المفتوح للبيئة اللاسلكية في الحلول التحفيرية وتدابير الاستيقان الملائمة التي تتحقق من المستخدم النهائي. وتحفر الحركة إلى البوابة التي يمكن التحقق من معرف هويتها تحفيرياً.

وثمة شرطان رئيسيان لشبكة المنطقة المحلية اللاسلكية المأمونة هي الحركة المأمونة والتجوال المأمون. فبالنسبة للاتصالات المأمونة. يتمثل الشرط الأساسي في استخدام التحفير للحركة من الجهاز المتنقل إلى نقطة النفاذ اللاسلكية وإلى البوابة الواقعة خلف هذه النقطة (مثل استخدام بوابة أمن بروتوكول الإنترنت) أو إلى مخدم التطبيقات (موقع الويب المأمون). وبالنسبة للتجوال المأمون، ينبغي أن يكون في استطاعة مستخدمي الأجهزة المتنقلة الانتقال من نقطة نفاذ لا سلكية إلى أخرى دون خسارة دوراتهما النشطة ودون حاجة إلى إعادة استيقان لنقطة النفاذ اللاسلكية الجديدة. ويتم التجوال تبعاً لتقييدات زمنية شديدة حتى لا يكون هناك سوى أقل تأثير على تطبيقات المستخدم. ويتوقع المستعملون أن أوراق اعتمادهم محمية بصورة ملائمة فيما بين المجالات ويفترضون ذلك.

### 3.4.III تعزيزات الأمن لمواصفات IEEE 802.11

تؤدي المخاطر الأمنية المشار إليها أعلاه إلى إجراء تعزيزات للمعيار الأصلي [b-IEEE 802.11] لتوفير وسائل أكثر فعالية لأمن شبكات المنطقة المحلية اللاسلكية. وIEEE 802.11i تقدم IEEE 802.1X (انظر [b-IEEE 802.1X]) ضوابط للنفاذ، مراعاة تصميم المفتاح بصورة دينامية، وآليات توزيع مفتاح ما قبل الدورة وخوارزميات تحفير قوية. ويقدم المعيار [b-IEEE 802.1X] المزيد من ضوابط الاستيقان/النفاذ لنقاط النفاذ اللاسلكية من خلال استخدام بروتوكول الاستيقان القابلة للتمديد الذي هو مجموعة من الرسائل الخاصة بمفاوضات الاستيقان، وطريقة نقل الاستيقان فيما بين العميل والمخدم (انظر [b-IETF RFC 2716] و[b-IETF RFC 3748] و[b-IETF RFC 4017]). ويدعم بروتوكول الاستيقان القابل للتمديد العديد من طرق الاستيقان بما في ذلك MD5 وأمن طبقة النقل على أن يكون MD5 هو الأكثر حصولاً على الدعم والأكثر توافراً. وبصرف النظر عن اختيار بروتوكول الاستيقان التوسعي، يتعين أن تدعم المكونات الثلاثة للمعيار IEEE 802.1X (انظر [b-IEEE 802.1X]) نفس الطريقة (انظر الشكل 3.4.III).




**الشكل 3.4.III – مكونات المعيار IEEE 802.1X**

وتتطلب مهمة تأمين تجوال حسب المعيار IEEE 802.1X بأن يقوم المستخدم دائماً بإعادة استيقان نقاط النفاذ اللاسلكية الجديدة التي تقوم بالتجوال إليها. وتتسبب عمليات مفاتيح ما قبل الدورة والبنية التحتية للمفتاح العام في صعوبة إجراء عمليات إعادة الاستيقان السريعة. ولذا ستظهر بعض الصعوبات في خيارات الاستيقان هذه للتحويل ما بين نقاط النفاذ اللاسلكية أثناء التجوال.

وبالنسبة للمعيار [b-IEEE 802.1X] توفر EAP-TTLS وPEAP إعادة الاستيقان السريعة لأغراض التجوال. ويتم ذلك من خلال الاستفادة من توصيل آلية إعادة التمديد التي يوفرها بروتوكول تنظيم الاتصال TLS. وليس من المطلوب إجراء عملية استيقان كاملة على أساس الافتراض بأن معرفة السر الرئيسي التي تثبتها القدرة على استئناف دورة TLS تعد استيقاناً كافياً.

### 4.4.III الأسلوب القائم على الطبقات لتأمين شبكات المنطقة المحلية اللاسلكية

تتطلب المعماريات المأمونة لشبكات المنطقة المحلية اللاسلكية الجيدة توافر أسلوب قائم على الطبقات يطبق تكنولوجيات متعددة مثلما الحال بالنسبة لبيئات شبكات المنطقة المحلية المعتادة. وينبغي أن يكون الحل النهائي هو معمارية أمن مدمجة بين شبكة المنطقة المحلية اللاسلكية وشبكة المنطقة المحلية. وينبغي حيثما يكون ممكناً، توسيع آليات أمن شبكة المنطقة المحلية العاملة لخدمة شبكة المنطقة المحلية اللاسلكية.

#### 1.4.4.III نقطة النفاذ

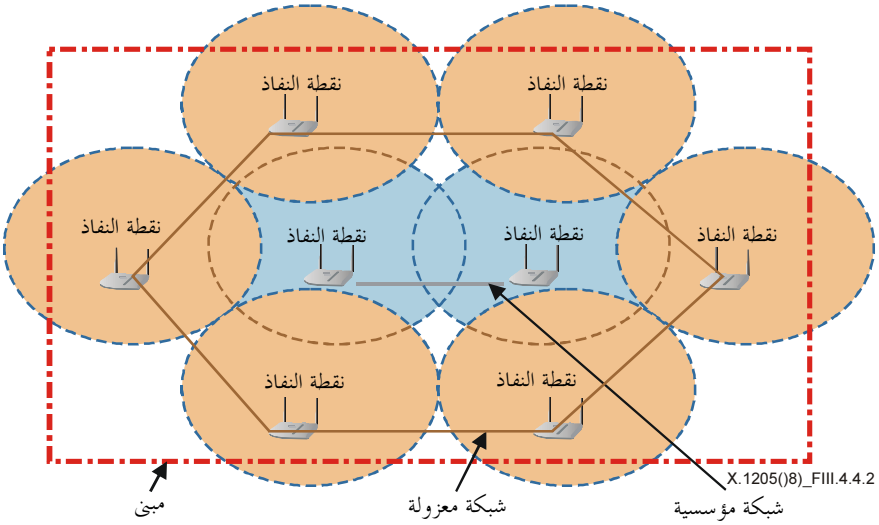
يمكن استخدام ESSID وMAC ACL على الرغم من أنهما يوفران أمناً شديد الضعف. ويمكن لجميع الوحدات المتنقلة ونقاط النفاذ اللاسلكية المشكلة بنفس هوية ESS الارتباط معاً بحرية. ويدعم المعيار [b-IEEE 802.11] "معرف مجموعة الخدمات الموسعة المذاع" (ESSID) التي تسمح لوحدة متنقلة أن ترتبط بنقطة نفاذ لاسلكية دون معرفة معرف مجموعة الخدمة الموسعة (ESSID). ويمكن تعزيز الأمن إذا جرى تعطيل هذا الجانب. إذ إن MAC ACL تحتوي على قائمة بعناوين MAC المسموح بها وقد تحتوي على قائمة بالعناوين المحظورة. وينبغي ألا يغيب عن البال أن ذلك يصبح من الصعب إدارته عندما يتضمن الأمر عدداً كبيراً من الحواسيب.

وفي الوقت الحاضر، يمكن بسهولة تطبيق منتجات نقاط النفاذ اللاسلكية التي تبين آليات الأمن السابقة المعايير والمملوكة التي تتضمن: معيار التجفير المتقدم (AES) لمعادل الخصوصية السلكي الدينامي وللنفاذ WPA والنفاذ WPA2، وبروتوكول سلامة المفتاح المؤقت والتجفير المكون من 128 بتة. ومعادل الخصوصية السلكي الدينامي عبارة عن وسيلة لتغيير مفتاح هذا المعادل بوتيرة كبيرة خلال فترات فاصلة سابقة التحديد. والتجفير AES معيار جديد معتمد من FIPS كي يحل محل خوارزمية تجفير DES. وتعزز (TKIP) خوارزمية تحديد الجدول الزمني للمفتاح للحماية من هجمات استرداد المفتاح لمعادل الخصوصية السلكي التقليدي. ونظراً لما تتسم به من ضعف، يوصي المعيار [b-IEEE 802.11] بعدم استخدام (TKIP) إلا كرقعة مضافة إلى التجهيزات القديمة.

**ملاحظة** – بدأ النفاذ المحمي Wi-Fi (WPA) في شكل مبادرة من الصناعة تحدد التحسينات التي تدخل على أمن التشغيل البيني للمنطقة المحلية اللاسلكية. وWPA-PSK عبارة عن طريقة خاصة للنفاذ المحمي من WPA للمستخدمين من المنازل دون مخدم استيقان المؤسسة ويوفر حماية تجفير قوية. ويجري في WPA-PSK تغيير مفاتيح التجفير أوتوماتياً (إعادة تصميم المفتاح) والاستيقان فيما بين الأجهزة بعد فترة زمنية محددة أو بعد إرسال عدد محدد من الرزم. وتستخدم WPA-PSK سراً مشتركاً يدخل في كل من نقطة النفاذ اللاسلكية وعملاء WPA. ويمكن أن يتكون السر المشترك من 8 إلى 63 سمة من حيث الطول. ويستخدم بروتوكول سلامة المفتاح المؤقت (TKIP) بعد دخول السر المشترك الأول في الأجهزة اللاسلكية، وتناول التجفير وإعادة تصميم المفتاح الأوتوماتي. وقد صمم WPA ليكون وسيلة للارتقاء بالبرمجيات. ويتوقع موردو التجهيزات اللاسلكية وخبراء الأمن المهنيون أن تظل WPA الحالية وWPA-PSK مفيدتان لفترة طويلة جداً قادمة. ويحدد WPA استخدام معيار التجفير المتقدم باعتباره بديلاً اختيارياً إضافياً لتجفير النفاذ المحمي من WEP.

#### 2.4.4.III حيز الهواء

يستطيع أي عنصر خارجي يريد أن يحصل على نفاذ غير مرخص إلى شبكة منطقة محلية سلكية أن يصل، باستخدام هوائي اتجاهي بكسب عال، إلى شبكة المنطقة المحلية السلكية من على مسافة عدة أميال. ومن الأفضل منع العنصر الخارجي من عمل ذلك. وقد تتمثل إحدى الطرق لمنع العناصر الخارجية غير المرخصة من استغلال توافر الإشارة على الهواء المفتوح باستخدام هوائي اتجاهي عالي الكسب في إحاطة محيط أراضي المؤسسة أو شبكة المنطقة المحلية السلكية بنقاط نفاذ لا سلكية غير متصلة بشبكة داخلية (انظر الشكل 2.4.4.III). ويتم منع العنصر الخارجي من رؤية شبكة المنطقة المحلية السلكية الداخلية حيث تعمل نقاط النفاذ اللاسلكية الخارجية في نفس تردد الحمل للشبكة الداخلية. ويمكن تعزيز ذلك من خلال ربط نقاط النفاذ اللاسلكية الخارجية هذه بشبكة منفصلة وإضافة نظام كشف الاقتحام، وشراك حاسوبية لكشف الاقتحام وجمع القرائن.



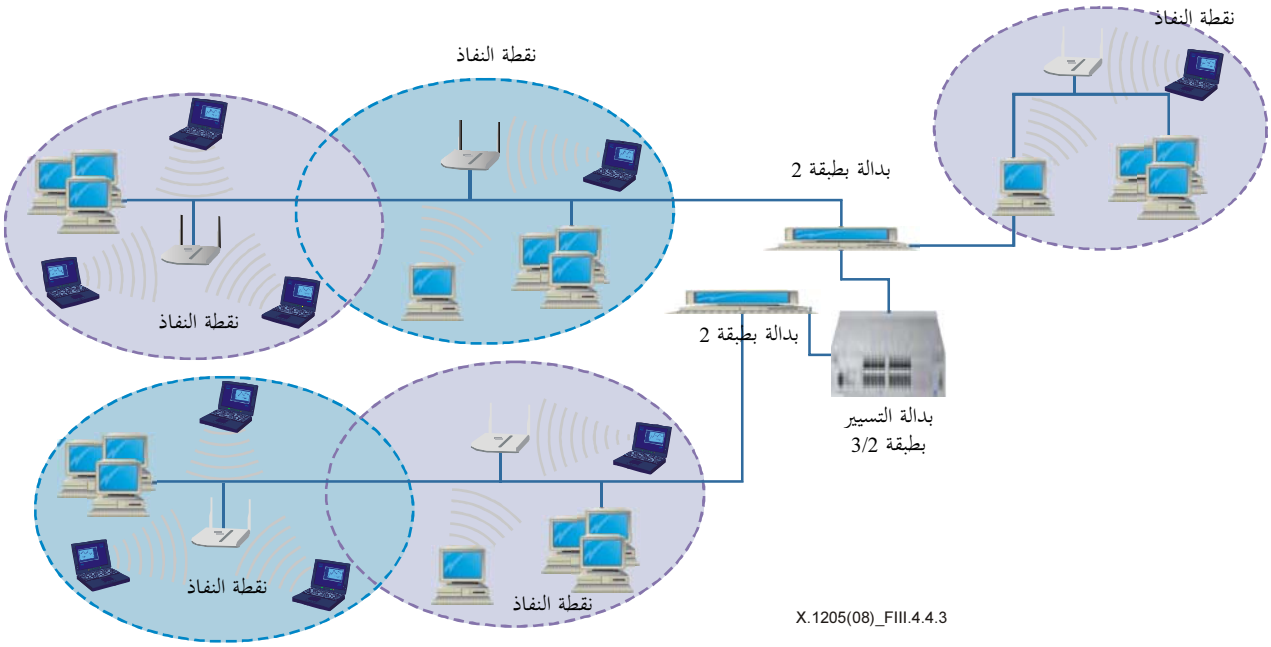

**الشكل 2.4.4.III – نقاط النفاذ اللاسلكية الحارسة لأمن المحيط**

### 3.4.4.III التقسيم إلى مقاطع

ينبغي، حيثما يكون ممكناً، توسيع نطاق آليات أمن شبكة المنطقة المحلية لخدمة شبكة المنطقة المحلية اللاسلكية. وثمة آليات إضافية مثل التجفير من خلال الشبكات الخاصة الافتراضية (VPN) وبروتوكول أمن طبقة النقل TLS، وتقسيم المقاطع اللاسلكية من خلال شبكات المنطقة المحلية الافتراضية والدفاع عن المحيط من خلال جدران الحماية، تعتبر فعالة بصرف النظر عن التعزيزات الإضافية اللازمة للمعيار [b-IEEE 802.1X]. ويبين الشكل 3.4.4.III نقاط نفاذ لا سلكية متنوعة للمعيار IEEE 802.11 لشبكة المنطقة المحلية اللاسلكية مع تعريف مجموعة خدمات أو شبكة فرعية متصلة ببدالة من الطبقة 2. ويمكن أن تمر هذه البدالة بمهارة من الحركة الذاهبة إلى نقاط النفاذ اللاسلكية الأخرى كما أن بعضها قادر على شبكات المنطقة المحلية الافتراضية. ولنقاط النفاذ اللاسلكية هذه القائمة في شبكة فرعية أخرى أو معرف مجموعة خدمات، يمكن إقامة التوصيلة عن طريق مبادلة تسيير من الطبقة 3/2. ولهذه المعمارية اعتبار التوصيلات المأمونة والتجوال والترحيل المأمونين ودفاع المحيط جزء من بنية الشبكة WLAN/LAN المتكاملة والمأمونة.

ويعتبر أمن بروتوكول الإنترنت بروتوكولات مجربة وموثق بها لتأمين الاتصالات. وبالنسبة للبيئات التي يمكن أن تعزز عملاء أمن بروتوكول الإنترنت على الأجهزة المتنقلة أو لديها تطبيقات تتضمن أكثر من طرف أمامي مستند إلى ويب، يعتبر أمن بروتوكول الإنترنت أنسب الوسائل لتأمين الاتصالات. والفائدة الرئيسية من شبكة خاصة افتراضية لأمن بروتوكول الإنترنت متمثل في سيطرة المؤسسة الكاملة على سياسة الأمن الشاملة لدرجة أن الشخص الذي يتم توصيله بشبكة منطقة محلية تكون له جميع ميزات مستخدم شبكة المنطقة المحلية.

وتسري نفس هذه التقنيات على "النقاط الساخنة" في شبكة المنطقة المحلية السلكية. فعلى سبيل المثال، فإن بوسع الموظف البعيد الذي يمكنه النفاذ إلى الشبكة من مورد خدمة إنترنت في فندق أن يوصل عن طريق خدمة الخط الرقمي للمشترك (DSL) باستخدام عميل PPPoE وهوية مستخدم/كلمة سر المقدمة من الفندق للنفاذ إلى مورد خدمة الإنترنت. ويستطيع الموظف عندئذ أن يتصل بشبكة المؤسسة باستخدام عميل أمن بروتوكول الإنترنت.




**الشكل 3.4.4.III – نقاط النفاذ اللاسلكية التنوعية في المعيار IEEE 802.11**
**لشبكة المنطقة المحلية اللاسلكية مع تعريف مجموعة خدمات مشتركة**

### 4.4.4.III طبقة الإدارة

ينبغي أيضاً استخدام التدابير المضادة الإدارية والتشغيلية لتأمين شبكات المنطقة المحلية السلكية. وينبغي توسيع نطاق السياسة الأمنية للمنظمة لتشمل شبكة المنطقة المحلية السلكية. وينبغي، حيثما يكون ممكناً، توسيع آليات أمن شبكة المنطقة المحلية العاملة لخدمة شبكة المنطقة المحلية السلكية. أو يتعين دفع آليات جديدة مع الآليات العامة. فعلى سبيل المثال، يؤدي تقديم حلول أمن بروتوكول الإنترنت إلى تزويد المؤسسة بإدارة مركزية لمستخدمي شبكة المنطقة المحلية السلكية والمستخدمين عن بعد وقواعد جدران الحماية ولا تتطلب أية انعكاسات إضافية للإدارة إذا كانت تستخدم بالفعل في النفاذ للشبكة الخارجية. ويضيف البائعون المعرفة بشبكة المنطقة المحلية السلكية إلى الآليات مثل اكتشاف الشبكة ومسح نقاط الضعف ونظام كشف الاقتحام.

### 5.4.4.III تحليل بروتوكولات النفاذ WLAN

يمكن تحليل نقاط القوة والضعف لمختلف البروتوكولات Wi-Fi التي نوقشت أعلاه، وهي المعيار IEEE 802.11i والبروتوكولات WPA2[2] وWPA وWEP. باستعمال الأبعاد التي تنص عليها التوصية ITU-T X.805. والتحليل موضح في بعدين ويمكن توسيعه ليشمل الأبعاد الثمانية جميعها.

وتصف النتيجة النوعية لكل بعد باستعمال الرموز التالية:

| | |
|---|---|
| √ | مُرض |
| P | جزئي |
| X | لا يتطرق له المعيار |

[2] للبروتوكول WPA2 والمعيار IEEE 802.11i عناصر أمن متماثلة، لكن بما أن البروتوكول WPA2 يعمل مع WPA بمقدار أقل من الأمن، فإن ضَعْف البروتوكول WPA ينعكس على أمن البروتوكول WPA2.

## التحكم في النفاذ

لا تضم المواصفات الأصلية للمعيار [b-IEEE 802.11] بما فيها البروتوكول WEP آليات تحكم في النفاذ مدمجة، ولذا استخدمت عمليات نشر الشبكات WLAN العريضة بوابة WLAN لأغراض التحكم في النفاذ إلى الخدمة. واستناداً إلى هذه الفرضية، اعتبر التحكم في النفاذ في الخدمة WLAN المقدمة إلى المستعملين النهائيين ملائماً جزئياً.

والمعيار [b-IEEE 802.1X] هو آلية التحكم في النفاذ المتوفرة للمستعمل الطرفي في الخدمة Wi-Fi في المعيار IEEE 802.11i والبروتوكولين WPA وWPA2.

**الجدول 2.III – التغطية بالنسبة لبعد التحكم في النفاذ**

| بُعد أمن التحكم في النفاذ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| مستويات الأمن | طبقات الأمن | | | | | | | |
| | البنية التحتية | | | | الخدمات | | | |
| | IEEE 802.11i | WPA2 | WPA | WEP | IEEE 802.11i | WPA2 | WPA | WEP |
| المستعمل النهائي | √ | √ | √ | X | √ | √ | √ | P |
| التحكم | √ | X | X | X | √ | √ | √ | X |
| الإدارة | X | X | X | X | X | X | X | X |

### الاستيقان

يستخدم المعيار IEEE 802.11i والبروتوكولان WPA2 وWPA المعيار IEEE 802.1X/EAP في الاستيقان. وعلى العكس من ذلك، يستخدم البروتوكول WEP إما الاستيقان "المفتوح" أو استيقان "السر المشترك" اللذين يستخدمان نفس المفتاح الساكن المستعمل للتجفير. ولذلك يعتبر استيقان البروتوكول WEP "جزئياً". وقد يكون تقدير الاستيقان في معايير أخرى أيضاً مماثلاً إذا اختير بروتوكول EAP ضعيف مثل MD5 للمعيار [b-IEEE 802.1X].

ولا يعالج استيقان معلومات التحكم في نقاط النفاذ وغيرها من عناصر الشبكة (لدعم خدمة التجول) إلا بالمعيار IEEE 802.11i. وتستخدم عادةً نقاط النفاذ التي تتيح معايير أخرى آليات خاصة من أجل تبادل هذه المعلومات نظراً لأن التجول وضمان أمن هذه التطبيقات لا يقع ضمن نطاق التطبيق.

**الجدول 3.III – التغطية بالنسبة لبعد الاستيقان**

| بُعد أمن الاستيقان | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| مستويات الأمن | طبقات الأمن | | | | | | | |
| | البنية التحتية | | | | الخدمات | | | |
| | IEEE 802.11i | WPA2 | WPA | WEP | IEEE 802.11i | WPA2 | WPA | WEP |
| المستعمل النهائي | √ | √ | √ | P | √ | √ | √ | P |
| التحكم | √ | X | X | X | √ | √ | √ | X |
| الإدارة | X | X | X | X | X | X | X | X |

**التيسر**

هجمات النظام DoS مثل التشويش الراديوي وفيضان البيانات واختطاف جلسة الطبقة 2 هي جميعاً هجمات على التيسر. ولا يستطيع أي من معايير الأمن WLAN منع الهجمات على الطبقة المادية لمجرد أنها تعمل في الطبقة 2 وما فوق. وكذلك لا يستطيع أي من المعايير أن يعالج عطلاً في نقطة للنفاذ

**الجدول 4.III – التغطية بالنسبة لبعد التيسر**

| بُعد أمن التيسر | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| مستويات الأمن | طبقات الأمن | | | | | | | |
| | البنية التحتية | | | | الخدمات | | | |
| | IEEE 802.11i | WPA2 | WPA | WEP | IEEE 802.11i | WPA2 | WPA | WEP |
| المستعمل النهائي | P | P | P | X | P | P | P | X |
| التحكم | P | P | P | X | P | P | P | X |
| الإدارة | X | X | X | X | X | X | X | X |

من الواضح أنه بالإمكان تصميم شبكات WLAN مؤمنة نسبياً وتنفيذها واستخدامها باستعمال المعيار IEEE 802.11i أو البروتوكول WPA2. غير أن مجرد تطبيق هذين المعيارين لن يضمن أمن الشبكات WLAN من طرف إلى طرف. وكما تبين دراسة الحالة هذه، لم يتم تناول أبعاد التيسر.

# بيبليوغرافيا


[b-ITU-T G.729] التوصية ITU-T G.729 (2007)، *تشفير الكلام بمعدل 8 kbit/s بالتنبؤ الخطي مع الإثارة بتتابعات مشفرة ذات هيكل جبري مترافق (CS-ACELP).*

[b-ITU-T X.509] التوصية ITU-T X.509 (2005)، تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر التصديق العمومية الرئيسية وتصديق النعوت.

[b-ITU-T Y.2201] التوصية ITU-T Y.2201 (2007)، *متطلبات الإصدار 1 من شبكات الجيل التالي.*

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification* <http://www.ietf.org/rfc/rfc0854.txt?number=854>.

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)* <http://www.ietf.org/rfc/rfc0959.txt?number=959>.

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm* <http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* <http://www.ietf.org/rfc/rfc1510.txt?number=1510>.

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)* <http://www.ietf.org/rfc/rfc1661.txt?number=1661>.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats* <http://www.ietf.org/rfc/rfc1991.txt?number=1991>.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* <http://www.ietf.org/rfc/rfc2104.txt?number=2104>.

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook* <http://www.ietf.org/rfc/rfc2196.txt?number=2196>.

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification* <http://www.ietf.org/rfc/rfc2311.txt?number=2311>.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap* <http://www.ietf.org/rfc/rfc2411.txt?number=2411>.

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay* <http://www.ietf.org/rfc/rfc2427.txt?number=2427>.

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* <http://www.ietf.org/rfc/rfc2459.txt?number=2459>.

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols* <http://www.ietf.org/rfc/rfc2510.txt?number=2510>.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol -- HTTP/1.1* <http://www.ietf.org/rfc/rfc2616.txt?number=2616>.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* <http://www.ietf.org/rfc/rfc2631.txt?number=2631>.

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"* <http://www.ietf.org/rfc/rfc2661.txt?number=2661>.

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol* <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* <http://www.ietf.org/rfc/rfc2748.txt?number=2748>.

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP* <http://www.ietf.org/rfc/rfc2749.txt?number=2749>.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* <http://www.ietf.org/rfc/rfc2753.txt?number=2753>.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary* <http://www.ietf.org/rfc/rfc2828.txt?number=2828>.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)* <http://www.ietf.org/rfc/rfc2865.txt?number=2865>.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions* <http://www.ietf.org/rfc/rfc2869.txt?number=2869>.

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture* <http://www.ietf.org/rfc/rfc3031.txt?number=3031>.

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* <http://www.ietf.org/rfc/rfc3084.txt?number=3084>.

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)* <http://www.ietf.org/rfc/rfc3174.txt?number=3174>.

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification* <http://www.ietf.org/rfc/rfc3377.txt?number=3377>.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3579.txt?number=3579>.

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* <http://www.ietf.org/rfc/rfc3580.txt?number=3580>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3748.txt?number=3748>.

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol* <http://www.ietf.org/rfc/rfc4252.txt?number=4252>.

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions* <http://www.ietf.org/rfc/rfc4366.txt?number=4366>.

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* <http://www.ietf.org/rfc/rfc4557.txt?number=4557>.

[b-ISO/IEC 7816-x] ISO/IEC 7816-x, *Identification cards – Integrated circuit(s) cards with contacts* <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>.

[b-ISO/IEC 18028-2] ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>

[b-ISO/IEC 18028-3] ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>

[b-ISO/IEC 18028-5] ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>

[b-ISO/IEC 18043] ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control* <http://www.ieee802.org/1/pages/802.1x.html>.

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), <http://www.w3.org/TR/REC-xml/>.

[b-SSL3] The SSL Protocol Version 3.0, <http://wp.netscape.com/eng/ssl3/draft302.txt>

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>

## 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 والأنظمة متعددة الوسائط |
| السلسلة I | الشبكة الرقمية متكاملة الخدمات |
| السلسلة J | الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية 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 ومسائل الأمن** |
| السلسلة Y | البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي |
| السلسلة Z | اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات |

طُبعت في سويسرا
جنيف، 2009