الإنترنت: الأمن ... والوقاية

ان حماية شبكة لمؤسسة ما، ضد أخطار التشبيك بين حواسيبها ومع شبكة الإنترنت يجب ان يشمل تطبيق للأمن بطبقات متتابعة تتوالى (دفاع يتعمق) وهذا يعني تركيب لحواجز وعوائق أمنية داخل منظومة الشبكة. ان هذا التتابع الدفاعي يعرقل الاختراق المهدد لأمن الشبكة حيث ان أي اختراق غير مصرح به لحاجز دفاعي في الشبكة لا ينتج عنه وصول مصدر الخطر الى بقية المنظومة الشبكية. وفي العموم، ان منع الأخطار يجب ان يأخذ في الاعتبار إدارة عملية ملموسة وهاجس أمني محسوس بالإضافة الى تطبيقات متعددة التشكيل (Configurations) ووسائل أمن مادية وبرمجية (Hardware & Software Security Tools). في ما يلي وصف لأساليب أمنية يمكن تطبيقها للوصول الى درجة عالية من الأمان ضد الأخطار.

ضبط الدخول (Access Control):

ان ضبط الدخول والتحكم به هو عملية تحديد لامتيازات استخدام المصادر المتوفرة على شبكة المنظومة. وأساليب التحكم إدارية (Administrative) أولا وهذا يستند الى سياسات المؤسسة في التشغيل والإدارة للأفراد العاملين والتيقظ لأهمية أمن الشبكة، وفيزيائية (Physical) ثانيا في منع العبث بأسلاك الشبكة وعقديات ترابطاتها، ومنطقية (Logical) ثالثا بتحديد الوصول الإلكتروني الى برتوكولات التراسل ووسائل التشفير. وبهذا يكون ضبط الدخول بطرق عديدة منها:

١- ليس حقا للمستخدمين الوصول الى ملفات ومصادر شبكية ليسوا في حاجة لها.
٢- الوصول الى معلومات حساسة يجب ان يكون مقيدا لعدد محدود من المستخدمين وخلال فترة وأزمان محددة مسبقا.
٣- الوصول الى خادم الشبكة (Network Server) يجب ان يكون مقيدا في أعلى درجاته.
٤- حافظات الطاقة (Unbreakable Power Supply) لأجهزة البيانات الحساسة ضرورة لازمة.
٥- استخدام برمجيات الكشف للاختراقات غير المصرح بها (Intrusion Detection Software) أينما كان ذلك ممكنا.
٦- التطبيق المنضم والممنهج لسياسات الخزن الدوري للبيانات واستخدام أساليب تشفير البيانات ذات الطبيعة الهامة، ومراقبة استخدامات مصادر الشبكة وساعات التشغيل لحسابات المستخدمين أمر يوفر لأدارة الشبكة ومشغليها الكثير من الهم الممكن تجنبه.
٧- استخدام الأساليب التقنية الحديثة في التحقق من شخصية المستخدم المصرح له باستخدام الشبكة ومصادرها وليس الاعتماد فقط على الأساليب التقليدية التي تعتمد كلمات المرور النصية (Textual Password) والأساليب الحديثة عديدة منها نذكر المنظومات الحيوية (Biometric systems) التي تستند في التعرف على صفات حيوية للمستخدم كطبعة من أصابعه أو عينة لصورة من شبكة عينه أو وجهه أو صوته.. الخ.

مكافحة ومنع الفيروسات (Anti Viruses Control):

لتقليل إمكانية الإصابة بالفيروسات التي قد تهاجم الشبكة هناك محاذير يفضل اتباعها وينصح باتخاذها:

١. بدء تسلسل استنهاض (Booting) الجهاز من القرص الذي تستقر عليه منظومة التشغيل (System Disk).
٢. إلغاء قابلية التشغيل الذاتي لبعض برمجيات نظام التشغيل التي تحتاجها فيروسات البرامج الملحقة بالبريد الإلكتروني.
٣. جعل جميع الملفات بحالة الظهور (Unhidden) ليتسنى ملاحظة أي ملف غريب.
٤. عدم قراءة الملفات الملحقة (Attached Files) بالبريد الإلكتروني الا بعد فحصها (Anti Virus Scanned).

التشفير والترميز (Cryptography & Encryption):

التشفير والترميز هو استخدام شفرة مفتاحيه (Cipher or keyed Code) لتحويل رسالة ما الى ان تقرأ كشيء آخر، وكي نستطيع استرجاع الرسالة الى محتواها الأصلي لابد من استخدام المفتاح (الرقمي بطبيعة الحال) الذي أستخدم في تحويلها. والتقنية الحديثة لنوعية المفتاح المتبعة في الوقت الحاضر تكون اما باستخدام مفتاح متماثل (Symmetric Key) واحد أو مفتاحين غير متماثلين (Asymmetric Keys). واستخدام مفتاح واحد كذلك المستخدم في تقنية تشفير البيانات القياسية (Data Encryption Standard: DES) المعروفة والتقنيات المماثلة فيه شيء من الخطورة في ان يقع رمز المفتاح بيد من يسيء استخدامه وبالتالي يلغي أهميته الأمنية. في حالة استخدام مفتاحين غير متماثلين مربوطين بعلاقة رياضية بحيث يستخدم أحدهما للتشفير ويكون خاصا وسريا ويستخدم الآخر لذوي العلاقة بالمفتاح الأول بحيث يكون غير سري ومعلوما من جميع الأطراف التي تتعامل مع المفتاح السري الأول والخاص بكل جهة، كما هي الحال في تقنية خوارزمية التوقيع الرقمي (Data Signature Algorithm) وتقنيات مشابهة أخرى. كما ان جمع أسلوبي التقنيتين المارة الذكر (ذات المفتاح الواحد والمفتاحين) ممكن أيضا كما هي الحال في تقنية كيربروس (Kerberos) التي تستخدم خادم خاص للتعريف (Authentication Server) يعرف بالخادم المانح لبطاقة التعريف (Ticket Granting Server). وفي حالة تخاطب الحواسيب فأن تقنية عدم إنكار الإرسال من مستخدم ما تتطلب وضع توقيعه الرقمي الذي يكون في العادة مجموعة من الرموز الرقمية المشفرة، التي يعني استلامها وقراءتها أشبه بإيصال من المرسل يتعذر عليه إنكار إرسالها.

الشبكات الخاصة الافتراضية (Virtual private Networks: VPN):

هذا النوع من الشبكات هو غير متحقق فيزيائيا بل هو تشبيك افتراضي هدفه الأمني خلق مجموعة من المستخدمين الذين يتشاركون بالمصادر والتراسل وعدم السماح لغيرهم بقراءة ما يتراسلوه. والشبكات الافتراضية هذه على نوعين داخلي يكون فيه المستخدمين على نفس شبكة المؤسسة، وخارجي يكون فيه المستخدمين متواصلين عبر شبكة الإنترنت. وفي هذا النوع من الشبكات تستخدم تقنية التنفيق (tunneling)، أي خلق نفق

افتراضي للتواصل تكون البيانات المرسلة عبره مكبسلة (encapsulated) مع مقدمة رمزية (header) لا تمكن قراءتها الا من قبل أعضاء الشبكة الافتراضية الشرعيين.

الجيل القادم من بروتوكول الإنترنت (Next Generation IP):

ان البروتوكول الحالي (IP_{v4}) بالإضافة الى محدودية قابليته في العنونة (Addressing) التي لا تتجاوز الأربعة مليارعنوان انترنتي الا بقليل، هناك مشاكل وثغرات أمنية عديدة لا تحمي الخصوصية وآلية التعرف. ومن أجل هذا يتصدى الجيل القادم من بروتوكول الإنترنت (والتحويرات في البروتوكول الحالي) لهذه المشاكل باستخدام مقدمة التعرف (Authentication Header) ومقدمة الأمن المكبسلة (Encapsulating Security Header) من أجل التكامل في منظومة التراسل الآمن التي تحمي أمنية الشبكة من الداخل وأمنيتها من الخارج عند التوصيل مع الإنترنت.

شهادات المفتاح العام (Public Key Certificates: PKCs):

وهي بيانات مهيكلة (Data Structured) فيها شفرة أو توقيع صلاحية (Certificate Authority: CA) تربط هوية مستخدم ما لمفتاح عام. وشهادات المفتاح العام هذه تستخدم من أجل دعم التعرف والسرية الأمنية لعمليات الشبكة العنكبوتية (Web) وتبادليات البريد الإلكتروني (Email Exchange) وأمن بروتوكول الإنترنت بشكل عام. ان بنية هذه الشهادات تستند الى ما يعرف بتقنية (Public Key Infrastructure: PKI) التي تجهز آلية توليد المفاتيح وضمان أمنها وادارة الشهادات.

الجدران النارية (Firewalls):

عند إحاطتنا بالأخطار نستخدم النار لمنع الأعداء من الوصول الى حواضرنا ولمنع أطفالنا من الخروج الى بيداء الخطر. كذلك هي فكرة الجدران النارية في الشبكات. ان خواديم الجدران النارية هي مصدات وسطية (Buffers) بين الخواديم والحواسيب الأخرى على الشبكة لفصلها عن العالم الخارجي من أجل منع الدخلاء وجعل الشبكة أمينة قدر الإمكان. والاستخدام العادي للجدران النارية يستند على وضعية السماح لكل الخدمات بالمرور ما لم تكون قد تم منعها بأمر مسبق، أو عدم السماح لكل الخدمات بالمرور ما لم تكون قد تم السماح لها بأمر مسبق. وفي العموم تستخدم الجدران النارية واحدة من التقنيات التالية:

١. تفحص الحزمة (Packet Filtering): بالتأكد من الصلاحية الأمنية للحزمة المارة عبر الجدار الناري.
٢. تفحص الدائرة (Circuit Level): وذلك بالتأكد من أن الأطراف المتراسلة قد تم وصلها بشكل أصولي وليس بشكل استثنائي كما يحدث في حالة الدخلاء الطارئين.

٣. تفحص التطبيق (Application Level): باستخدام الوكيل المساعد والفاحص (Proxy) الذي يمكنه أيضا إخفاء حواسيب الشبكة باستخدام تقنية تشفير العنوان (Network Address Translation).
٤. ترشيح الحزمة الديناميكي (Dynamic Packet Filter): باستخدام كلا الأسلوبين ١ و٣ المارة الذكر.
٥. الوكيل الذاتي (Kernel Proxy): المطبق على مستوى نظام التشغيل المستخدم.

وما يجب الانتباه اليه ان الجدران النارية قد تعاني اختناق يؤخر التراسل عند تحميلها بأعباء التدقيق بكل البيانات الداخلة وكل البيانات الخارجة رغم إنها تضمن بذلك الأمن والسرية. وقد تستخدم الجدران النارية هذه بعدة طبقات أمنية وبأشكال هيكلية مختلفة. وفي العادة تكون المنطقة السابقة للجدار الناري منطقة يسمح للآخرين الدخول إليها بدون محاذير أو مخاطر أمنية، وتعرف هذه المنطقة الغير محروسة بالمنطقة غير المسلحة (De Militarized Zone: DMZ) ويكون فيها خدمات يسمح لكل الداخلين على الشبكة من الخارج بالدخول إليها. وفي العموم، فأن الجدران النارية تستخدم أجهزة أو برامجيات أو كلا ذلك، مكرسة لعمل الجدار الناري. وتتولى الجدران إدارة بروتوكول الإنترنت المستخدم (IP)، و ترجمة العناوين أو تغييرها، حفظ تقارير للأعمال التي تجري عبر الشبكة، إمكانية التشبيك الافتراضي الخاص، وترتيب أوليات الاتصال.

التغيير في البروتوكولات (Protocol Switching):

ويكون في تغيير البروتوكولات المستخدمة بعد الجدران النارية الى بروتوكولات أخرى مما يصّعب أو يمنع الدخلاء والغرباء في الاستمرار في حالة النجاح من عبور تلك الجدران دون اكتشاف التغير في البروتوكول المستخدم والتواءم مع التغيير فيه.

التسلل الفاحص (Penetration Test):

يعتقد بعض المسؤولين عن أمن الشبكة ان استخدام واحد أو أكثر من الأساليب المارة الذكر يكفي للاطمئنان على أمنية الشبكة. الا ان الواقع أثبت ان المتطفلين والدخلاء يجدون في أغلب الأحيان طرق ووسائل وثغرات منسية للوصول. وهنا يأتي دور أدارة الشبكة في استخدام مهندسيها الجيدين وأصحاب الخبرة منهم بتقمص سلوك الدخلاء في التسلل للتعرف على نقاط الضعف في منظومة أمن الشبكة. ان هذا الفحص المتسلل هو تطفل نافع وأخلاقي (Ethical Hacking). وقد يستغرب الآخرين عن كيف يكون التطفل أخلاقيا!. الا ان الكثير من أساليب الأمن والتعرف على ثغرات الأمن يتأتى من هذا النوع من التطفل. وهو جزء من اختبار دفاعات الشبكة لسدها أو ردمها قبل ان يكتشفها الدخلاء الضارين. وللتطفل الأخلاقي هذا أسس وقواعد يجب مراعاتها:

١. استحصال الأذن المسبق وعدم مخالفة القوانين المرعية.

٢. تجميع أكبر قدر من المعلومات عن الهدف المنوي مهاجمته (والهدف هنا قد يكون حساب لشخص أو حاسوب في الشبكة أو جهاز خادم رئيسي) دون اتخاذ فعل. وتعرف هذه المرحلة بجمع المعلومات السلبي (Passive Information Gathering).
٣. البدء بتجميع المعلومات نحو الانطلاق ببدء الاختراق (Active Information Gathering). مثل ذلك البحث عن ثغرة غير مغلقة (open port) يمكن استخدامها للوصول الى الهدف. وتحوي شبكة الإنترنت عن مواقع عديدة للمساعدة في ذلك!. وواحد من الأساليب المعروفة يكون بإرسال بريد إلكتروني الى خادم بريد الشبكة مع خطأ مقصود. ان الرد يحوي الكثير من المعلومات التي تساعد المتطفل.
٤. وضع خريطة عن مواضع الضعف (Vulnerability Mapping) المتوفرة عن الهدف.
٥. تقييم انجازية التسلل (Performing the Exploit): ان الدخلاء الضارين لا يهتمون بما يسببه تطفلهم من ضرر على الهدف المقصود. الا ان ذلك ليس مقبولا مع الدخلاء الفاحصين الذين يتطلب عملهم تقييم الأضرار التي يسببها التطفل الضار.
٦. تقوية المنظومة (Hardening the System): ويكون بتوثيق نقاط الضعف لتقويتها والاستمرار في البحث عن نقاط الضعف الأخرى.

ان التسلل الفاحص أو التطفل النافع هذا يمكنه ان يزود ادارة الشبكة برؤية تقيمية ونظرة داخلية عن كيفية جعل الشبكة عصية على الدخلاء. وعمل هذا النوع من الدخلاء لا يكتمل الا بعد وضع تدرج تفاضلي لنقاط الضعف وعن تطبيقات التحكم بها.

أخطاء التصميم الشبكي وثغرات الأمن (Design Pitfalls & Security Holes):

ولأن تحقيق الأمن التام والمطلق حالة يستحيل تحقيقها في أي موقف من الحياة، كذلك الأمر في أمن الشبكات. الا ان العمل المنظم والتعاون بين المعنيين بأمر أمنية الشبكة وتواصلاتها الداخلية والخارجية يثمر ويحقق الدرجة الأعلى والموقف الممكن من أجل ذلك. والوصول الى المستوى المرغوب والمطلوب بأعلى درجاته الأمنية يتطلب ما يلي:

أ–تجنب أخطاء التصميم:
١. يجب عدم تواجد الجدار الناري والوكيل (Proxy) على نفس الموزع (Switch or Hub).
٢. يجب وضع خواديم الخدمة العامة (Public Servers) على جزئيات مختلفة (Several Segments) من الشبكة.
٣. تجنب تحميل الجدار الناري بوظائف عديدة تؤخر عملها.
٤. وضع قائمة بنوعية الخدمات المسموح بها الدخول للمناطق غير محروسة (DMZ).
٥. استخدام تشفير البيانات أينما كان ذلك مطلوبا.
٦. تطبيق الحماية المتدرجة على مناطق الشبكة الأمنية. بمعنى آخر استخدام جدار ناري واحد أو وكيل (Proxy) واحد قد يكون غير كاف.

ب- ردم الثغرات الأمنية:

١. كلمات السر النصية (Clear-text Password): كاستخدام كلمات سر نصية تتكون من عدد قليل من الحروف فقط أو استخدام كلمات ذات صلة بالمستخدم من الجوانب الاجتماعية (كأسماء أفراد الأسرة).
٢. سهولة المراقبة(Ease of Monitoring): المتاحة للدخلاء أو الذين يمكنهم الوصول الى توصيلات الشبكة وبالتالي التعرف على ما يجري عبرها.
٣. تزييف العنوان الشبكي (Network Addresses Spoofing): مما يؤدي الى تقمص هوية المستخدمين واستلام نسخ مما يرسل إليهم وما يترتب عن ذلك من مخاطر أمنية.
٤. فقر الإدارة الأمنية في المؤسسة بشكل عام (Poor Quality of Security).
٥. ضعف خبرة المسؤول عن إدارة الشبكة (Network Administrator).
٦. ضعف الحماية الأمنية على خادم الشبكة الرئيسي (Main Server).

الخاتمة:

ان علو الاعتماد على تطبيق ما يجعله ثمينا وتصبح مسألة حمايته واجبا. كما ان اختراق الخصوصية وانتهاك السرية مخالفة غير مقبولة على مختلف الأصعدة وحين يكون ذلك الاختراق وذلك الانتهاك سببا في ضرر على ضحاياه وفائدة لمسببيه يكون حينذاك عملا جرميا. أن الأعمال الجرمية تلك باتت تعرف في عالم التشبيك الحوسبي بأعمال الجريمة الإلكترونية. ان الفراغ القانوني بما يتعلق في كيفية زمان ومكان ومسؤولية إثبات حدوثه في عالم التشبيك الحوسبي مسألة لا تزال مدار بحث من قبل العديد من أخصائي القانون والاجتماع. وفي المقابل يجب ان تكون وسائل الوقاية من أي عبث مسائل بحث وتثبيت من قبل أخصائي الحواسيب وشبكاتها أيضا. والجريمة في عالم تشبيك الحواسيب وتناميه في التجارة والطب والصناعة وغير ذلك عالم لا يعرف حدود الزمان ولا حدود المكان ولا حتى حدود التملك والحيازة. عالم تكون فيه خصوصية البيانات بدرجة أولى هامة على أعلى تقدير وثمينة وفق أي اعتبار. ولما كان تشبيك الحواسيب هو أساس هذا العالم الشبكي، فأن وسائل وأساليب حمايتها ووقايتها جديرة بالاعتبار والأهمية من قبل صناع القرار والإدارة العليا للمؤسسات التي ترى التشبيك لازما في عالم يسلم بأهميته وخطره واستمرار تناميه المولد للتقدم.