المحتوى

مـــقـــدمة

بسـم اللّه الرحمن الرحيم، الحمد للّه رب العـالمين، والصلاة والسلام على رسـول اللّه محمد و آله و صحبه أجمعين ومن تبعهم بإحسان إلى يوم الدين. أما بعد:

إن الكتاب الذي بين يديك يهدف إلى زيادة الوعي حول كيفية تأمين المعلومات والتعريف بالخدمات والوسائل المتاحة لتحقيق هذا الهدف، بالإضافة إلى معرفة كيفية حماية معلومات المؤسسات والمعلومات الخاصة بالأفراد.

إن المعلومات مصطلح واسع، وهي في مفهوم الحاسب الآلي تحوي: الملفات الإلكترونية ومنها ملفات البرامج وملفات البيانات، وتحوي المعلومات: الوثائق الورقية، المطبوعة منها والمكتوبة باليد وكذلك الصور، كما تحوي: التسجيلات أكانت تسجيلات الفيديو أو الصوت، وتحوي كذلك الاتصالات، وهي إما أن تكون محادثات صوتية وجها لوجه أو بالهاتف الثابت أو المحمول، أو تكون المحادثات بالرسائل بتعدد أشكالها كذلك كالرسائل الإلكترونية (الإيميل) أو رسائل الفاكس أو رسائل الفيديو أو رسائل الهاتف القصيرة أو الرسائل العادية.

هذه المعلومات لها قيمة في نظر المؤسسات لذا تعدها من أصول ممتلكاتها، وعليه يجب حمايتها مثلها مثل بقية الأشياء الثمينة، ولأنه يجب حماية المعلومات فإن البنية التحتية التي تساندها يجب حمايتها كذلك. حيث تحوي هذه البنية: الشبكات، والأنظمة، والوظائف التي تهيئ للمؤسسة إدارة معلوماتها والسيطرة عليها، وهنا يأتي أثر هذا الكتاب إذ يشرح لك ما يمكنك فعله لحماية معلومات مؤسستك، وذلك في اثني عشر درساً كما هو مبين في الفهرس، مغطياً كل نواحي أمن المعلومات بداية من التعريف بالمعلومة إلى تفاصيل طرق حمايتها، هذا و نسأل اللّه أن يكون سهل المأخذ عظيم الفائدة، وهو سبحانه من وراء القصد...

الوقاية من الإختراقات الإلكترونية وكيفية التعامل معها

مقدمة

في عالمنا المعقد والمعتمد بشدة على الانترنت، تتزايد وبشكل مذهل احتمالات الهجمات الإلكترونية وحوادث التسلل والاختراقات الأمنية. ولذا فإن أمن الأنظمة والتطبيقات سيبقى تحديا مستمرا لإدارات تقنية المعلومات والأعمال التجارية.

ان العديد من الهجمات ومحاولات الاختراق هي ببساطة مبرمجة وتستهدف دون تمييز الثغرات و نقاط الضعف المتواجدة في الأجهزة والبرامج بغض النظر عن المؤسسة التي تقوم باستخدامها. وتجدر الاشارة هنا الى ان الثغرات و نقاط الضعف هذه تتواجد وبشكل أكبر في البرامج التي لا يتم تحديثها بشكل دوري، بالإضافة الى البرامج مجهولة المصدر والبرامج المحمية بكلمة مرور ضعيفة.

تنبيهات

البرمجة الآمنة

برمجتك للتطبيقات والشبكات بشكل آمن يعتبر أمر أساسي لعملية الدفاع وحماية التطبيقات والشبكات، حيث يساعد ذلك على تقليل مخاطر التسلل إليها أو التلاعب بها.

وبشكل عام، فإنه من الأسهل وأقل كلفة بناء برمجيات آمنة تنطبق عليها المعايير الأمنية الدولية، عوضاً عن تصحيح الثغرات الأمنية بعد اكتمال البرنامج، ناهيك عن التكاليف التي قد ترتبط بالاختراقات الأمنية و الأثار المترتبة على ذلك.

لقد أضحى تأمين موارد البرمجيات الحرجة أكثر أهمية عن ذي قبل، حيث يستهدف المخترقين في يومنا الحالي التطبيقات ومواقع الانترنت و ذلك بناءاً على أحدث الهجمات التي تعرضت لها المؤسسات بالسلطنة.

ولذا فعلى فريق التطوير البرمجي ان يتمتع بمستوى عال من الخبرات والوعي الأمني وذلك أجل تطبيق أفضل الممارسات وتقييم المستوى الأمني للتطبيقات والبرامج. كما ينبغي عليهم ايضا ان يتحلوا بالمسؤولية و يسعوا للحصول على التدريب الكافي والأدوات والموارد اللازمة لضمان توفير الحماية والامان للأأنظمةة والبرامج .

يعد كلاً من معهد سانس ومجلس المفوضية الأوروبية رائدا في هذا المجال، وبإمكانهما أن يزودا مطوري البرامج بالأدوات والمهارات المطلوبة للحصول على مستوى مقبول من البرمجة الآمنة.

قائمة البرمجة الآمنة:

- التأكد من صحة البيانات
- ترميز المُخرجات
- إدارة كلمات المرور والتثبت من الهوية
- إدارة الجلسات
- التحكم في الوصول
- ممارسات التشفير والحماية
- التعامل مع الاعطال والتوثيق
- حماية البيانات والمعطيات
- أمن الاتصال
- تهيئة النظام
- أمن قواعد البيانات
- إدارة الملفات
- إدارة الذاكرة

تأمين الخوادم

تأمين الخوادم هي عملية تحسين مستوى أمن الخوادم من خلال العديد من الوسائل والسبل التي تنتج عنها بيئة تشغيلية أكثر أمانا. ويعزى ذلك إلى الإجراءات الأمنية المتقدمة التي يتم اتخاذها خلال هذه العملية .

إن التهيئة الإفتراضية لمعظم أنظمة التشغيل تم تصميمها بشكل عام دون التركيز على الأمن كعامل أساسي، حيث تأتي الأولوية لسهولة الاستخدام، وسهولة التواصل، والوظائف التي يقوم بها النظام. ولذا ، لحماية الخوادم فإنه يجب أن توضع سياسات وإجراءات معقدة لتأمين جميع الخوادم في المؤسسة. ولربما تتمثل اول خطوة لرفع مستوى أمن الخوادم والشبكات لديك في إنشاء قائمة ضبط لتأمين الخوادم لتسهيل عملية التنفيذ والمتابعة. كما عليك أن تتأكد من أن هذا القائمة تتضمن اساسيات الممارسات الأمنية التي تتوقع من الموظفين اتباعها. وإذا ما توجهت إلى استشاري فبإمكانك تقديم قائمة الضبط هذه لاستخدامها كقاعدة للقياس والتطوير.

وتتفاوت قوائم الضبط بحسب نظام التشغيل، إلا أن القائمة المعدة أدناه تضم المهام العامة التي ينبغي اتباعها مع أي نظام تشغيل:

- ضع سياسة داخلية لأمن الخوادم ونظام التشغيل
- عطل أو تخلص من الحسابات أو المنافذ أو الخدمات غير الضرورية
- أزِل أي تطبيقات غير ضرورية
- اضبط اعدادات الجدار الناري لنظام التشغيل.

- اضبط التدقيق
- عطل المشاركات الغير الضرورية
- اضبط التشفير
- التحديثات الدورية والإصلاحات العاجلة
- ثبت برنامجا مضادا للفيروسات والبرمجيات الضارة
- قلل من الصلاحيات
- عطل الرسالة التعريفية بالخوادم
- قم بتفعيل هاتين الطريقتين: POST أو GET وإلغاء باقي الطرق المتوفرة
- عطّل بروتوكول الانترنت إلإصدار السادس (IPv٦) ما لم يكن مطلوبا.
- راجع سجل الدخول وسجلات أعطال النظام

هناك عدد من الأدوات التي يمكنها برمجة عملية تامين الخوادم بشكل تلقائي، ومن أفضل المنتجات: نيسوس (Nessus)، يو أر إل سكان (URL scan)، برنامج إدارة الالتزام الأمني من مايكروسوفت (Microsoft security compliance management toolkit (SCM)، و برنامج تحليل السمات الأمنية الدنيا من مايكروسوفت (Microsoft baseline security analyzer (MBS).

اختبار النفاذ الأمني الدوري

أفضل طريقة لحماية بياناتك ومعلوماتك هي التعرف على نقاط الضعف المحتمل وجودها ، ومعالجتها قبل أن تتعرض للهجمات الالكترونية. وذلك ومن خلال إجراء سلسلة من الاختبارات الدقيقة من قبل خبراء مختصين وذوي مهارات عالية والذين بإمكانهم اكتشاف هذه الثغرات ونقاط الضعف،والافادة بالحلول التي تمكنك من معالجة هذه الثغرات بشكل سريع، مما سيعزز من الحماية الأمنية.

إن اختبارات النفاذ الأمني هي مصممة لإختبار الحماية الأمنية للشبكات، الخوادم ، التطبيقات، برمجيات الهواتف المتنقلة، الحواسيب الشخصية المحمولة، الأنظمة اللاسلكية، الطابعات ، أو أي من المكونات المادية الصلبة أو الأنظمة التي بإمكانها أن تخزن معلومات أو تعالجها، إزاء محاولات أياً من المخترقين لاستغلال الأنظمة أو التحكم بها.

انواع اختبارات النفاذ الامني

الاختراق الخارجي، وهي اختبارات تقليدية، والأكثر شيوعاً في اختبار النفاذ الأمني. حيث يتم من خلالها معرفة مدى قدرة أي مخترق خارجي على اختراق الشبكات الداخلية والوصول اليها. وتهدف هذه الاختبارات إلى الوصول إلى خوادم معينة أو مكونات ذات أهمية قصوى ضمن الشبكات الداخلية، وذلك من خلال استغلال نقاط الضعف المكتشفة عن طريق تطبيقات الانترنت ، أو من خلال استدراج مستخدم للتصريح بكلمة المرور الخاصة به عبر الهاتف، أو الوصول إلى الشبكة الافتراضية (VPN)، فإن الهدف الأساسي هنا هو القدرة على النفاذ من الخارج إلى الداخل.

الاختراق الداخلي، يتمثل في ما يمكن للمخترق تحقيقه من داخل المؤسسة بحيث يتمتع بالصلاحيات التي تسمح له بالدخول أو أنه يبدا هجومه من موقع ضمن الشبكة الداخلية. والهجمات الداخلية يمكن أن تسبب ضررا أشد وقعا من الهجمات الخارجية، لأن المخترق من الداخل يدرك مسبقا الأجزاء الهامة من الشبكة ومواقعها، وهذا ما لايعرفه عادة المخترقين من الخارج عند بدء هجماتهم.

ومع التطور السريع في مجال تقنية المعلومات والبرمجيات الحرة فقد أصبح بإمكان المخترقين استغلال اي بيئة تعد «آمنة» بعد فترة من الزمن والتلاعب بها اذا لم يتم إجراء اختبارات دورية للنفاذ الآمني للتعرف على أي مخاطر أو تهديدات جديدة قد تتعرض لها الأنظمة المستخدمة

خدمة اختبار النفاذ الأمني من المركز الوطني للسلامة المعلوماتية

يوفر المركز الوطني للسلامة المعلوماتية خدمة اختبار النفاذ الأمني إلى جميع المؤسسات الحكومية والقطاع الحيوي بالسلطنة، هذا وبالإمكان طلب هذه الخدمة عن طريق موقع المركز www.cert.gov.om

وبعد القيام باجراء اختبار فإن المركز سيقوم بتسليمك تقريرا مفصلا عن جميع نقاط الضعف التي تم اكتشافها، وتصنيفها بحسب مستوى خطورتها والمخاطر المصاحبة لها ، كما يضم التقرير أيضا مقترحات بالحلول والاجراءات الواجب اتباعها لمعالجة الثغرات.

سياسة أمن المواقع لدى هيئة تقنية المعلومات

قامت هيئة تقنية المعلومات بصياغة (سياسة أمن المواقع الإلكترونية) بالتعاون مع عدد من المختصين في أمن المعلومات، والتي بإمكانك من خلالها تطبيق الإجراءات الأمنية المثلى.

للإطلاع على سياسية أمن المواقع يرجى زيارة الموقع التالي:
http://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=12

التخزين الاحتياطي

مما لا شك فيه أن التخزين الاحتياطي مهم في كل مؤسسة، ويعد أحد أهم الإجراءات الاستباقية الواجب اتباعها لضمان توافر البيانات والمعطيات . غير أنه من المهم ايضا التعرف على المخاطر المحيطة بالتخزين الاحتياطي وكيفية الحد منها.

ينبغي حفظ النسخ الاحتياطية على خادم احتياطي وأقراص صلبة على نحو يومي / أسبوعي/ شهري تبعا لحساسية البيانات المخزنة وأهميتها. كما يجب أن يكون محل حفظ النسخ الاحتياطية مؤمنا. إضافة الى ذلك فإنه ينبغي التحكم في مدى الوصول إليها، وذلك لضمان عدم دخول الغير المخولين أو المصرح لهم بذلك. علاوة على ذلك، ينبغي تشفير النسخ الاحتياطية الهامة والتي تضم معلومات حساسة،لاسيما خلال مرحلة النقل أو الحفظ الخارجي، تجنبا لوقوعها في أيد العابثين.

وكذلك بالنسبة لخوادم النسخ الإحتياطية ، فإنه يجب تأمينها وسد نقاط الضعف بها وتعريضها لإختبار النفاذ الآمني وذلك بهدف ضمان عدم تعرضها للحوادث الأمنية مستقبلا. كما يجب

التحكم في مكان حفظ هذه الخوادم، وضبط عملية الوصول إليها. وفي حالة نقل هذه الخوادم إلى موقع خارج المؤسسة أو موقع آخر غير موقعها الحالي، فإنه يجب نقلها في حاويات مغلقة ومؤمنة، كما يجب التأكد من سمعة و موثوقية الشركة التي تقوم بعملية النقل وموظفيها لا سيما الذين سيقومون بالنقل.

وكإجراء تنظيمي، يجب تسجيل جميع عمليات النسخ الاحتياطي، وذلك لتسهيل عملية تتبعها إلى مصادرها الأصلية.

وفي وقتنا الحالي ، أصبح التخزين الاحتياطي التلقائي امر شائعا، حيث يوفر حلا مناسبا للقيام بعملية التخزين الاحتياطي بشكل متكرر. ومن المهم ان يتم اختيار حلول برمجية تراعي تطبيق الإجراءات الاحترازية، وتوفر سجلات ومعلومات تسهل متابعة عمليات التخزين الاحتياطي و وضعها الحالي. كما يجب تحديث هذه الحلول البرمجية ومعالجتها من أية ثغرات قد تشوبها بانتظام.

تجدر الاشارة ايضا الى أهمية اختبار ملفات التخزين الاحتياطي بانتظام وبشكل دوري، وذلك لضمان دقة البيانات ونجاح عملية تخزينها وحفظها واسترجاعها.

المراقبة الآمنية

تساعد المراقبة بشكل كبير في فحص أداء الخوادم، والشبكات، وسجلات الدخول، والكشف عن أية ممارسات أو أنشطة ضارة على مستوى الخوادم. وعلاوة على ذلك، فإن المراقبة خلال مرحلة الاختبار تساعد على كشف المخاطر المحتمل وقوعها لاحقا و التي يمكن في حينها التعامل معها ومعالجتها قبل التدشين. كما تساعد المراقبة في كشف المخاطر الجديدة من خلال التعرف وتحديد السلوكيات المشكوك فيها والمريبة والتي تحتاج إلى مزيد من التحقيق.

مزايا المراقبة

- الحماية من المخاطر الداخلية والخارجية
- الاستفادة القصوى من الاستثمار القائم والمستقبلي في الأمن الإلكتروني
- تقوية الجانب الأمني من خلال البحث والتطوير
- الحصول على صورة واضحة وشاملة للعمليات والأنشطة الأمنية في شبكة المؤسسة
- اتباع المتطلبات التنظيمية لمراقبة السجلات

من المهم ايضا اتباع المعايير العالمية عند مراقبة سجلات الدخول، مثل معايير PCI–DSS و معايير ISO ٢٧٠٠١. كما يجب على بعض المؤسسات الالتزام بهذه المعايير للحصول على تراخيص تشغيلية مثل مؤسسات البني الأساسية الوطنية كالبنوك، وإدارات المرور، ومؤسسات قطاع النفط والغاز...إلخ

وهناك أيضا عدد من أطر العمل المتبعة للمراقبة التشغيلية التي بالإمكان اتباعها، بما في ذلك أطر مايكروسوف التشغيلية (Microsoft Operations Framework)، ويمكن لمثل هذه الأطر المساعدة فيما يلي:

- قياس مدى تعرض الأعمال التجارية وتحديد ما يجب تأمينه.

- معرفة ما يجب اتباعه لتقليل المخاطر المواجهة إلى مستويات مقبولة.
- تصميم خطة للحد من المخاطر الأمنية و آثارها.
- مراقبة كفاءة الآليات الأمنية.
- إعادة تقويم الكفاءة والمتطلبات الأمنية بشكل منتظم.

وكتطبيق للأفضل الممارسات ، فإنه من المهم اتباع حلول المراقبة التي بإمكانها جمع كل سجلات الدخول في موقع مركزي مؤمن وذلك بهدف تسهيل عملية مراجعة هذه السجلات والتعامل معها. وينصح ايضا بتكوين فريق مراقبة مختص لهذا الغرض، حيث يلعب هذا الفريق دورا هاما في القيام بالتحقيقات الأمنية وتحديد الأنشطة التي تمثل مخاطر عالية على المؤسسة.

وسيتناول القسم أدناه، اهم الامور التي يجب مراقبتها والإجراءات والحلول المتبعة للحد من المخاطر:

الدخول غير المصرح (التدقيق الأمني)

هناك نوعان من الأحداث التي يتم تسجيلها في سجل الحوادث الأمنية: العمليات التي تمت بنجاح ، والعمليات التي لم تكتمل أو فشلت. ويضم النوع الأول اية عملية قام بها مستخدم ما بنجاح، أو أية خدمة أو برنامج تم تنفيذه بنجاح. أما النوع الثاني فيوضح العمليات التي لم تكلل بالنجاح.على سبيل المثال، تعد محاولات الدخول الفاشلة نموذج للعمليات التي لم تكتمل أو فشلت، ويتم تسجيلها في سجل الحوادث الأمنية إذا ما تم تفعيل رصد محاولات الدخول.

نظريا، فإن المستخدمين يجب ألا يتمكنوا من القيام بأية مهام غير مرخص لهم الإتيان بها مسبقا من قبل المدير أو المسؤول الأمني، ولذا فاكتشاف القيام بأية مهام غير مرخص بها يستدعي الإبلاغ عنها، والتحقيق بشأنها، وتسجيلها.

وفي معظم الأحوال فإن سجل العمليات التي لم تكتمل أو فشلت يعني أن هجوما ما يُشنُّ حاليا ويجب التعامل معه بأسرع ما يمكن للحد من مخاطر الأختراق الالكتروني. كما يجب إيجاد سياسات لمنع تكرار أي محاولات مستقبلية، مثل سياسات حجب عنوان بروتوكول الانترنت (IP Lockdown) ، وحجب اسم المستخدم، وغير ذلك.

ولقياس سياسات التدقيق الأمني، فمن المهم القيام بالتالي:

- مراجعة الإعدادات الحالية للتدقيق الأمني .
- تقييم دور المشرف وصلاحياته وكذلك باقي المستخدمين.
- مراجعة سياسات وإجراءات العمل.
- التعرف على الأنظمة التي تحتوي على الثغرات
- جرد الأصول والموجودات عالية القيمة.
- التعرف على الحسابات الحساسة أو المشكوك فيها وتحديدها.
- جرد البرامج المرخصة.
- التحقيق في المحاولات القادمة من مواقع جغرافية غير معروفة أو غير معتادة.

مراقبة الأنشطة الضارة

يمكن أن تتراوح الأنشطة الضارة من مسح المنافذ إلى زراعة البرامج الخبيثة والفيروسات، ومثل هذه الأنشطة يمكن التقاطها بسهولة عبر تطبيق الاستراتيجية المذكورة أعلاه ، وتنصيب نظام كشف التسلل / ومنع التسلل.

ومن المهم ايضا الحصول على أكبر قدر من المعلومات بغرض منع مثل هذه الأنشطة والتحقيق فيها. ويمكن للعديد من أنظمة كشف التسلل إخطار الفريق المراقب عن الأنشطة التي تحتاج معالجة بشكل فوري للتقليل من آثارها ، وللسماح للفريق أن يحقق فيها لتفادى أية إخطارات كاذبة مستقبليا.

ويمكن للضرر الذي يحدثه خطر داخلي أن يأخذ أشكالا عدة، بما في ذلك زرع الفيروسات، الديدان، أو أحصنة طروادة؛ أو يمكن أن يأخذ شكل اخر كسرقة معلومات أو أسرار تجارية، أو سرقة أموال، أو فساد، أو مسح بيانات ومعطيات، أو تغييرها، أو تشكيل مضايقة أو دليل جنائي كاذب ، أو سرقة هوية أشخاص بأعينهم في المؤسسة.

للحماية من المخاطر الداخلية يمكن اتباع إجراءات شبيهة بتلك المقترحة لمستخدمي الانترنت، مثل استخدام برامج للكشف عن برامج التجسس، وبرامج مضادة للفيروسات، والجدران النارية، واتباع نظام وروتيني ودقيق للتخزين الاحتياطي والأرشفة.

الكشف عن التسلل

يقوم نظام الكشف عن التسلل بفحص جميع أنشطة الشبكة سواء الداخلة أو الخارجة، والتعرف على الأنماط المشبوهة من التعاملات التي قد تشير إلى أن هنالك هجوما على الشبكة أو النظام .

ويلعب نظام الكشف عن التسلل دورا محوريا في الكشف المبكر عن أية مخاطر أمنية للشبكات، الخوادم، والمواقع على الانترنت. ويمكن تهيئة نظام الكشف عن التسلل للكشف عن أنشطة ضارة بعينها ، وإخطار الفريق المراقب بشأنهم.

أنواع أنظمة الكشف عن التسلل

الكشف عن سوء الاستعمال مقابل الكشف عن الاستعمال غير الطبيعي: في الأنظمة التي تنتهج الكشف عن سوء الاستعمال، تقوم هذه الأنظمة بتحليل البيانات التي تجمعها وتقارنها مع قاعدة بيانات كبيرة تضم تواقيع وهويات الهجمات المختلفة. بمعنى آخر فإن هذا النوع من الأنظمة يبحث عن نوع معين من الهجمات التي تم توثيقها. ومثل أنظمة الكشف عن الفيروسات، فإن جودة برامج الكشف عن سوء الاستعمال رهينة بجودة قاعدة بيانات الهجمات التي تستخدمها لمقارنة الهجمات المرصودة. أما في أنظمة الكشف عن الاستعمال غير الطبيعي ، فإن مدير النظام يقوم بتعريف الحدود الطبيعية لأداء النظام ، والحجم الطبيعي للبيانات المتبادلة عبر الشبكة، وكذلك حالات الفشل ، وبروتوكول الشبكة، و وحدة نقل البيانات ، ويقوم هذا النوع من أنظمة الكشف بمراقبة قطاعات الشبكة لمقارنة أدائها وحالتها مع الحدود الطبيعية المحددة مسبقا، وتبحث عن أي مؤشرات غير طبيعية.

الشبكة مقابل المضيف: في برامج الكشف عن التسلل المرتكزة على الشبكة، يتم

تحليل الحزمة التي تمر عبر الشبكة، ويمكن لهذا النوع من الأنظمة الكشف عن الحزم الضارة المصممة لتمر تحت نظر أنظمة الفلترة البسيطة في الجدر النارية دون أن تلاحظها. أما أنظمة الكشف المرتكزة على المضيف، فإنها تقوم بفحص الأنشطة في الحاسوب الذي يستضيفها.

النظام الإستباقي مقابل النظام التفاعلي: في النظام الإستباقي، فإن المجسات تكتشف الاختراقات الأمنية الممكنة، تسجل المعلومات، وتطلق تحذيرا. أما في الأنظمة التفاعلية، فإن مجسات الكشف تتفاعل مع أي نشاط مشبوه أو مشكوك فيه من خلال إخراج المستخدم أو من خلال إعادة برمجة الجدار الناري لحجب أية بيانات صادرة من مصدر ضار او مشبوه من أن تمر عبر الشبكة.

منع التسلل

تستخدم أنظمة منع التسلل في أمن الحواسيب. وهي توفر سياسات وقواعد لتبادل البيانات عبر الشبكة مع نظام للكشف عن التسلل لإخطار مدير الأنظمة أو مدير الشبكة حيال أية بيانات ضارة أو مشبوهة يتم تبادلها، وكذلك تسمح للمدير أن يقوم بالتصرف المناسب عند إخطاره. البعض يرى أن نظام منع التسلل عبارة عن مزيج من نظام للكشف عن التسلل مع جدار ناري كطبقة أمامية للحماية.

يمكن تصنيف أنظمة الحماية من التسلل إلى أربعة أنواع مختلفة، على النحو التالي:

- نظام منع تسلل مرتكز على الشبكة: يراقب الشبكة ككل من أية تبادل ضار أو مشبوه للبيانات من خلال تحليل أنشطة بروتوكول التبادل.
- نظام منع تسلل لاسلكي: يراقب الشبكة اللاسلكية من أية تبادل ضار أو مشبوه للبيانات من خلال تحليل أنشطة بروتوكول التبادل اللاسلكي.
- تحليل السلوك الشبكي: يفحص عملية تبادل البيانات في الشبكة للتعرف على المخاطر التي تحدث نشاطا غير عادي في نقل البيانات وتدفقها، مثل هجمات رفض الخدمة (الحجب) الشاملة (DDoS)، ونوعيات معينة من البرمجيات الضارة أو المخالفات.
- نظام منع تسلل مرتكز على الحاسوب المضيف: برنامج يتم تنصيبه فرديا يراقب فقط الحاسوب الذي يستضيفه من الأنشطة المشبوهة من خلال تحليل الأحداث والعمليات داخل الحاسوب المضيف.

إن وجود نظام لمنع التسلل يساعد في اتخاذ إجراء مبكر يحمي ضد مثل هذه الأنشطة ويعطي مزيدا من الوقت للفريق المراقب لتحليلها والتحقيق بشأنها.

خدمات المراقبة من قبل المركز الوطني للسلامة المعلوماتية

يقدم المركز الوطني للسلامة المعلوماتية خدمات مراقبة على مستويات عدة وفي بيئات مختلفة مثل:

- مراقبة الشبكات
- مراقبة سجلات المواقع
- مراقبة الرمز التعريفي العالمي للمواقع (URL)
- مراقبة الخوادم

لمعرفة المزيد عن خدمات المراقبة التي يقدمها المركز الوطني للسلامة المعلوماتية، يرجى زيارة الرابط التالي:

http://www.cert.gov.om/contact.aspx

التحديثات / المعالجات التصحيحية

مع ازدياد المخاطر الناشئة و تطور الهجمات الأمنية ، أصبح من المهم الحفاظ على الخوادم والتطبيقات وتحديثها وتصحيح أعطالها ، لتفادي أية هجمات مفاجئة. علاوة على ذلك، يوصى بالتسجيل مع مركز استشارات مختص بأمن المعلومات ليتم إخطاركم بالتنبيهات بشكل دوري.

التحديثات التلقائية لنظام التشغيل

وجود التحديثات التلقائية يمكن أن يوفر الوقت الثمين الذي يستغرقه التحديث والإصلاحات التي تستهلك وقتا كثيرا في المؤسسات الكبيرة، وعلاوة على ذلك ومن أجل تسريع هذه العملية وضمان إجرائها في جميع الحواسيب والمعدات المرتبطة بها، فمن الأفضل استخدام نظام مركزي للتحديث السريع والتلقائي، والذي يمكن التحكم به وادارته من قبل المدراء.

التحذيرات والإشعارات الأمنية المحدثة

يقوم المركز الوطني للسلامة المعلوماتية بتقديم خدمة التحذيرات والإشعارات الأمنية إلكترونيا، وذلك بالاشتراك لاستلام هذه التحذيرات والإشعارات بشكل فوري و منتظم عن آخر المخاطر باللغتين العربية والإنجليزية. بالإضافة إلى ذلك، يمكنكم التسجيل عبر موقع www.cert.gov.om لاستلام هذه التحذيرات والإشعارات في بريدكم الإلكتروني.

المسح

إن وجود حلول مضادة للفيروسات والرسائل الإلكترونية الضارة أو المتسلسلة على الخوادم والأجهزة الأخرى سيساعد حتما في حمايتها من الفيروسات الضارة والمدمرة، وأحصنة طروادة، والبرمجيات الخبيثة (Bot Nets).

وتباعا فإن الحفاظ على قاعدة البيانات لهذه الحلول محدثة أمر مهم ويجب إدارته بشكل إحترافي من خلال حلول برمجية تقوم بتحديث هذه القاعدة على الأجهزة بالمؤسسة كافة.

وبمثل هذه الحلول يستطيع المدراء التحكم في التحديثات وكذلك في منع المستخدمين من تعطيل البرامج المضادة للفيروسات على أجهزتهم وذلك من خلال استخدام ميزة التهيئة (الضبط) المحمية بكلمة المرور، وبالتي لا يستطيع الوصول إليها و تعطيل هذه البرامج أو تغيير التهيئة، إلا من قبل المدراء أو الأشخاص المرخص لهم.

مسح البرامج الضارة

يقدم المركز الوطني للسلامة المعلوماتية للمستخدمين خدمة مسح أجهزتهم لاكتشاف أية برامج ضارة معروفة من خلال برامج خاصة والتي يمكن الاطلاع عليها عبر هذا الرابط http:// cert.gov.om/ccp/english.htm#!/pageHome

التدقيق الأمني

كلمات المرور

تعد كلمات المرور بمثابة خط الدفاع الأول ضد هجمات التسلل والاختراق الضارة، ولذا فمن المهم اختيار كلمة مرور معقدة، صعبة التخمين، وغير موجودة في القواميس اللغوية، إلا أن التحدي الأكبر هو ضمان تغيير كلمة المرور وتجديدها بشكل مستمر.

كما يجب أن تكون كلمات المرور معقدة، ونعني بذلك أن تحوز هذه الكلمات على إحدى هذه الخصائص على الأقل:

- حرف صغير (abcdefghijklmnopqrstuvwxyz)
- حرف كبير (ABCDEFGHIJKLMNOPQRSTUVWXY)
- عدد (٠ ١ ٢ ٣ ٤ ٥ ٦ ٧ ٨ ٩)
- رمز أو رقم مثل (/.،';[]=–`~?<>«:|"“+_()×&^٪$#@!)

وعلاوة على ذلك، يجب أن تكون لكلمات المرور تاريخ تنتهي فيه صلاحيتها! العديد من قواعد البيانات يتم التسلل إليها، وتتم سرقة هويات مستخدميها وصلاحياتهم، ولذا فمن المهم أن يتم تغيير كلمات المرور باستمرار، وهذا ممكن من خلال تفعيل ميزة تاريخ انتهاء صلاحية كلمات المرور الموجودة في معظم الخوادم المتقدمة.

للبيانات الحساسة، يوجد هناك مبدأ التثبت المزدوج أو ثنائي المستوى، الذي يطلب من المستخدمين إدخال كلمات المرور مع مفتاح إضافي يتم إصداره أمنيا ويعطى للمستخدم من قبل المختصين الأمنيين. والكثير من المؤسسات الكبيرة تستخدم أجهزة لإصدار هذه المفاتيح الإضافية وترتبط هذه الأجهزة بحسابات المستخدمين لرفع مستوى الأمن المعلوماتي. وبالإضافة إلى ذلك، هناك برمجيات تستخدم لإصدار هذه المفاتيح الإضافية مثل برنامج جوجل للتثبت من الهوية (Google Authenticator) الذي يصدر مفاتيح عددية والتي تتغير باستمرار على مدار مدة قصيرة من الزمن.

يعتقد العديد من المستخدمين ان كلمات المرور المعقدة، ونظام التثبت المزدوج امر شاق يصعب عليهم تحمله ، ولذا يجب توعية هؤلاء المستخدمين حول أهمية اتباع مثل هذه الإجراءات ودورها في حمايتهم ومعلوماتهم الشخصية بالاضافة الى المعلومات المتعلقة بمؤسساتهم.

التحكم في مستويات الوصول أو الدخول

من خلال التحكم بمستويات الوصول يتم تحديد هوية المستخدم المصرح له المستوى المعلومات التي يصل إليها.

وعلى المدراء في حالة بعض النماذج أن يكونوا على أهبة الاستعداد لأن يقوموا بالتثبت من الهوية مقابل الدليل النشط، ولضمان أن المستخدمين الأصيلين فقط هم من يستطيعون الدخول إلى شبكة المؤسسة للقيام بمهامهم المحددة لهم.

تلعب القانوانين دورا هاما للغاية في تحديد مستوى الوصول والدخول الممنوح للمستخدمين، وتضمن أن المستخدم لا يستطيع الوصول إلى بيانات مصنفة أو محدودة التداول لا ينبغي له الوصول إليها.

المتسللين (hackers) سيسعون دائما إلى الوصول إلى شبكة المؤسسة لسرقة معلومات أو للقيام بهجمة من خلال تغيير بعض القواعد والقوانين أو فك شفرة كلمة المرور أو من خلال باب خلفي. يجب التعرف على مثل هذه المحاولات في وقت مبكر ويجب صدها وحجبها بشكل فوري.

الاتصال الآمن عن بعد

في كثير من الأحوال سيحتاج المستخدمون إلى الوصول إلى بياناتهم السرية من خارج مقر المؤسسة، مثل البريد الإلكتروني، و يجب أن يتم ذلك من خلال قنوات مؤمنة لتقليل من خطر تسرب المعلومات، ويمكن القيام بذلك عبر إحدى الوسائل التالية:

بروتوكول آمن لنقل الملفات (Secure FTP): وهذا بروتوكول برمجي تابع للشبكة يقوم بالوصول إلى الملفات وإدارتها على أنظمة ملفات خارجية عن بعد. والدور الأساسي لهذا البروتوكول هو تشفير المعلومات والبيانات سويا، مما يمنع الكشف عن كلمات المرور والبيانات الحساسة عند عبورها الشبكة.

النماذج الآمنة (SSL) (Secure Forms): تعتمد خوادم المواقع وبرامج التصفح على طبقة تعرف بطبقة القوابس الآمنة (Secure Sockets Layer) (SSL) وهي بمثابة بروتوكول يساعد المستخدمين في حماية بياناتهم خلال عملية تبادلها من خلال إيجاد قناة خاصة بها يتم تشفيرها على نحو فريد لتمكين التواصل الخاص والآمن عبر الانترنت. وتتكون شهادة النماذج الآمنة من مفاتيح مزدوجة بالإضافة إلى معلومات موثقة عن هوية البيانات المشفرة. وعندما يقوم برنامج التصفح بالإشارة إلى موقع مؤمن، يقوم الخادم بإطلاعه على المفتاح الرئيس العام مع المتصفح لإصدار طريقة التشفير ورمز خاص بالجلسة الحالية. يقوم بعدها البرنامج بتأكيد تعرفه على مصدر شهادة النماذج الآمنة وأنه موثوق به. تسمى هذه العملية بالمصافحة (SSL handshake) وبها تبدأ جلسات الاستخدام المؤمنة التي تحمي خصوصية الرسالة، وسلامتها، وأمن الخادم. ويمكن شراء شهادة النماذج الأمنة هذه عن طريق الانترنت من شركات معروفة مثل فيريساين (Verisign) أو سيمانتك (Symantec) وغيرها من هيئات أو جهات الإصدار.

شبكات خاصة افتراضية: وتسمح هذه الشبكات بالوصول بأمان إلى شبكات خاصة وتبادل المعلومات عن بعد عبر شبكات عامة. وهي مثل الجدار الناري الذي يحمي البيانات على الجهاز، وتقوم هذه الشبكات بحمايتها على الشبكات إلكترونيا. وبينما يمكن القول أن الشبكات الافتراضية هذه هي تقنيا مثل الشبكات الواسعة (Wide Area Network)، إلا أن واجهتها تحافظ على نفس الوظائف والميزات الأمنية والمظهر للشبكات الخاصة.

الغلاف الأمن (SSH) (Secure Shell): يوجد الغلاف الأمن قناة لشبكة خاصة افتراضية والتشفير الذي يحميها. ويسمح هذا للمستخدمين بنقل بيانات ومعلومات غير مؤمنة من خلال توجيهها من خوادم خارجية عن بعد للمرور عبر قناة مشفرة. وفي حين أن البيانات والمعلومات غير مشفرة ، إلا أن القناة التي تنتقل عبرها مشفرة. وتقوم الأجهزة العميلة التابعة للغلاف الآمن بإيجاد هذه التوصيلات والتي تقوم بدورها بتوجيه البيانات المتبادلة من منفذ محلي إلى مخدم خارجي عن بعد. وتمر جميع البيانات بين نهايتي هذه القناة عبر المنافذ المحددة.

التشفير

ينصح دائما بتشفير البيانات والمعلومات المخزنة في جهاز المستخدم أو الخادم أو أي جهاز للتخزين يضم معلومات حساسة. يمكن أن يسبب التشفير تأخيرا في استرجاع البيانات والمعلومات إذا كان حجمها كبيرا حيث يتطلب فك شفرتها إلى هيئة معروفة للجهاز قبل إعادة إرسالها إلى المستخدم. غير أنه مع تقدم المعالجات هذه الأيام، فلا ينبغي أن يشكل هذا الأمر معضلة أو عائقا حيث أن الفائدة تفوق هذا التأخير بكثير.

ولقد قامت العديد من المؤسسات مثل هيئة تقنية المعلومات بفرض سياسة تشفير جميع الأجهزة بما في ذلك الحاسوب المحمول، وذلك لإضافة طبقة أمنية تحميه في حالة سرقة أو ضياع هذه الأجهزة نظرا لما تضمه من معلومات وبيانات حساسة.

الجدار الناري

الجدار الناري هو نظام تم تصميمه لمنع أي دخول غير مرخص من وإلى الشبكة الخاصة. ويمكن أن يكون الجدار الناري في شكل جهاز أو برنامج ، أو مزيج من الاثنين. وتستخدم الجدر النارية عادة في منع مستخدمي الانترنت غير المرخص لهم من الدخول إلى الشبكات الخاصة الموصلة بالانترنت، لا سيما الشبكات الداخلية التي تتداخل مع الانترنت أو تلك التي تعتمد على الانترنت في توصيلاتها الداخلية. جميع الرسائل التي تدخل إلى الشبكة أو تخرج منها تمر عبر الجدار الناري، الذي يفحص كل رسالة ويحجب التي لا تفي بالمعايير الأمنية المحددة.

يمكن للجدار الناري أن يكون في شكل جهاز أو برنامج ، ولكن الأفضل أن يكون مزيجا من الاثنين. وبالإضافة إلى تقييد الدخول إلى الشبكة والأجهزة، فإن الجدار الناري مفيد أيضا في السماح للوصول عن بعد إلى الشبكة الخاصة من خلال شهادات هوية مرخصة وعمليات مرور آمنة .

يمكن شراء جهاز الجدار الناري كجهاز مستقل، وكما يوجد أيضا موجهات أو مسيرات النطاق العريض، ويجب أخذ الجدار الناري بعين الاعتبار لأنه جزء هام للغاية من أي نظام أو شبكة. معظم أجهزة الجدر النارية تحوز على أربعة منافذ على الأقل لربط أجهزة الحاسوب بها، إلا أنه وللشبكات الكبيرة توجد حلول خاصة للجدر النارية.

يمكن تنصيب برمجيات الجدر النارية على الحاسوب (مثلها مثل أي برنامج) وبالإمكان تكييفه ليتفق مع احتياجاتك الخاصة، مما يعطي قدرة على التحكم في وظائف هذه البرمجيات وميزات الحماية. إن برنامج الجدار الناري سيحمي الحاسوب من المحاولات الخارجية للتحكم فيه أو الدخول إليه.

الجدار الناري للتطبيقات

تؤمن الجدر النارية للتطبيقات حماية للتطبيقات، أي بنفس الطريقة التي تقوم بها الجدر النارية للشبكات بحماية وتأمين اتصالات الشبكات. ومن خلال الوعي باللغة المستخدمة من قبل التطبيق في نقل البيانات وتبادلها، فيمكن للجدار الناري للتطبيقات أن يرفض أو يعدل في أي نشاط غير صالح أو مشبوه.

تشمل الجدر النارية الشائعة الاستعمال في هذا المجال: مودسيكيوريتي (Mod Security) ويو آر إل سكان (URL Scan).

فصل البيئات

من الجيد دائما فصل البيئة المستخدمة لأنها تساعد في تقليل مخاطر انتشار التطبيقات الضارة، وهناك ٣ بيئات ينصح بها.

بيئة الاختبار

توفر هذه البيئة قيودا محدودة للمدراء والمطورين ضمن أية مؤسسة وذلك لاختبار تطبيقاتها تحت مختلف الظروف، على سبيل المثال إدخال البيانات الخطأ، اختبار الاختراق، اختبار أمن الترميز، إرسال حزمة ضارة، القيام بتصرفات أو خطوات لا يمكن عكسها، وغير ذلك.

وهذه البيئة مهمة جدا لأنها تمكن المطورين من العمل في بيئة طبق الأصل لبيئة الإنتاج، ولكن بدون الخوف من تدميرها إبان القيام بالاختبارات كونها بيئة خاصة وغير متاحة للعامة.

بيئة التطوير

تعد هذه البيئة مساحة حرة خاصة بالمطورين، لأنهم يتحكمون فيها بالكامل من حيث الدخول ، ومستويات التحكم في التطبيقات، والتهيئة ، والتنصيب، والإزالة، وغير ذلك.

يمكن للمطورين أن يقوم بتطوير التطبيقات واختبارها وتجريبها في هذه البيئة كما يرون ووفق احتياجاتهم ومتطلباتهم.

بيئة الإنتاج

هذه البيئة حساسة ويجب التحكم في مستويات الدخول والوصول من قبل مدراء محترفين لضمان أن هذه البيئة صالحة وفعالة بشكل مستمر. ويجب تهيئة وسائل التحكم، والجدر النارية، وأنظمة الكشف عن التسلل والحماية منه جميعا لحماية هذه البيئة من المتسللين ومخترقي الفضاء السيبراني.

وعادة ما يجب أن يمر التطبيق بالبيئتين سالفتي الذكر لضمان استقراره قبل نقله إلى هذه البيئة من قبل مدراء مختصين.

الاسترجاع

استرجاع البيانات هي عملية استعادة البيانات التي فقدت أو حذفت بالخطأ أو فسدت أو لم يعد ممكنا الوصول إليها.

وفي تقنية المعلومات الخاصة بالمؤسسات، يقصد باسترجاع البيانات هي عملية إعادة البيانات إلى حاسوب مكتبي أو محمول أو خادم أو جهاز تخزين خارجي من وسيط تخزين احتياطي.

وتتفاوت عملية استرجاع البيانات بحسب ظروف ضياع البيانات، أو برنامج استرجاع البيانات الذي استخدم في التخزين الاحتياطي، ووسيط التخزين الاحتياطي. على سبيل المثال تسمح العديد من الحواسيب للمستخدمين استعادة الملفات المفقودة من قبل المستخدمين أنفسهم، بينما تعد عملية استعادة الملفات من قاعدة البيانات ومن شريط التخزين الاحتياطي عملية معقدة تتطلب تدخل وحدة تقنية المعلومات. كما يمكن تقديم عملية استرجاع البيانات ككخدمة، ومثل هذه الخدمات عادة ما تكون لاستعادة ملفات هامة لم يتم تخزينها احتياطيا أو أزيلت خطأ من نظام الملفات في أحد الأجهزة ولكنها (أي الملفات) ما تزال مخزنة على القرص الصلب في أجزاء متناثرة.

ينبغي على خطة الكوارث والاسترجاع في المؤسسة أن توضح بشكل جلي من المسؤول عن استرجاع البيانات، وأن تقدم استراتيجية لاسترجاع البيانات وتوثيق مناطق الاسترجاع المقبولة والمعايير الزمنية للاسترجاع.

في حالة الطوارئ يجب القيام باسترجاع كامل أو جزئي لتمكين النظام من العودة مرة أخرى ببيانات صحيحة ودقيقة.

كيف تتعامل مع هجمات التسلل؟

توضح هذه الجزئية كيفية التعامل مع هجمات التسلل التي تنجح في الوصول إلى نظام البريد الإلكتروني أو الموقع أو الشبكة أو قاعدة البيانات، وخلافه.

أول خطوة ينبغي القيام بها هي إخطار جهة معروفة وموثوقة قادرة على إجراء الفحوصات اللازمة وحل مثل هذه الحوادث السيبرانية مع الحفاظ على خصوصيتك. ويفي المركز الوطني للسلامة المعلوماتية بهذه المواصفات وسيساعدكم بدون أية تكلفة كما سيتفاعل معكم بشكل فوري.

المركز الوطني للسلامة المعلوماتية

طرق الابلاغ عن الحوادث الأمنية

يوفر المركز الوطني للسلامة المعلوماتية قنوات اتصال مختلفة بما في ذلك:

- الإبلاغ الإلكتروني عن طريق الموقع
- البريد الإلكتروني: ocert999@ita.gov.om
- هاتف رقم: ٢٤١٦٦٨٢٨ (٩٦٨+)

ما يجب تحضيره؟

بينما تنتظر ردا من المركز الوطني للسلامة المعلوماتية، يمكن تحضير البيانات التالية التي ستتطلبها عملية الفحص والتحقيق:

- السجلات (سجل الدخول، سجل ملفات الخادم، سجل الأخطاء)
- نسخة من الملف المصاب .
- نسخة كاملة من النظام المصاب .

يمكن طلب بيانات أو معلومات إضافية بحسب نتائج الفحص والتحقيق الأولي، وسيتم طلب ذلك في مرحلة متقدمة.

التعامل مع الأدلة

تعد أيا من الأجهزة أو الخادم أو الشبكة المتسلل إليها أو المصابة أداة من أدوات الجريمة، ولذا يجب التعامل معها وفقا لذلك. يجب عدم إعادة تشغيل الأجهزة أو إيقافها عن العمل تحت أي ظرف. يجب فصل كابلات شبكات الانترنت والانترانت الداخلية فورا، وذلك لبدء عملية التحكم في الضرر.

في حالة توجيه تهم جنائية، فإن الأجهزة المصابة ستستخدم كأدلة رقمية، وسيقوم فريق الأدلة الرقمية بتحليل هذه الأدلة وتقديم تقرير بشأنها لاستخدامه في المحكمة.

استعادة التحكم

مع الأخذ بعين الاعتبار ماذكر أعلاه، فمن المهم استعادة التحكم على الأجهزة المصابة أو الموبوءة:

- افصل الأجهزة المصابة عن الانترنت، وعن أي وصول داخلي أو خارجي.
- حاول إزالة الملفات المصابة أو البرامج الضارة.

سرعان ما تنتهي من هذه العملية وقمت بالإبلاغ عن الحادث، يمكنك البدء في تقييم الضرر الذي نتج من هذا الحادث:

- هل كانوا يبحثون عن معلومات حساسة؟
- هل أرادوا التحكم على الموقع لأغراض أخرى؟
- ابحث عن أية ملفات معدلة أو تم تحميلها على خادم الموقع.
- تأكد من سجلات الخادم ما إذا كانت هناك أية أنشطة مشبوهة، مثل محاولات دخول فاشلة، تاريخ الأوامر الموجهة (لا سيما على مستوى الدليل الجذر(Root)، أسماء مستخدمين غير معروفة، وغير ذلك.
- حدد نطاق المشكلة – هل لديك مواقع أخرى معرضة للإصابة؟

من المهم أيضا فهم انك لم تتمكن إلى الآن من حل مصدر المشكلة ، فلا تحاول أن تسترجع الموقع وتعيد نشره بعد.

التحقيق

مراجعة السجل

سيرسل المركز الوطني للسلامة المعلوماتية تقريرا تفصيليا كاملا بالنتائج التي توصل إليها مع مقترحات للعلاج، وسيوجهك خلال عملية الاسترجاع.

وحيث أن مؤسستك أضحت هدفا، فينصح إحالة كل سجلات الدخول إلى فريق المراقبة بالمركز حتى يتمكن من متابعة المراقبة والكشف المبكر عن أية أنشطة ضارة ومنعها. هناك عدد من البرامج والتطبيقات الموجودة ضمن أنظمة المركز والتي ستساعد المدراء في الكشف عن محاولات التسلل ومنعها. من هذه الأدوات برنامج ضابط سلامة المحتوى أو (Content Integrity Agent) الذي يمنع المتسللسن من إضافة أي ملف أو تعديله على خوادم الموقع.

المراجع

1. OWASP SCP Quick Reference Guide v2
2. Server Hardening Website
3. 10 Steps to harden Windows Servers
4. Linux Server Hardening Tips
5. Why penetration testing is important?
6. Internal vs. External Pen–Testing
7. Security Monitoring and Attack Detection
8. Secure Sockets Layer (SSL): How It Works

كيفية الحصول على دعم الإدارة العليا لمكاتب أمن المعلومات

المقدمة

«لفرض سياسات أمن المعلومات بالمؤسسة، يجب الحصول على الدعم الكامل من الإدارة العليا» إرآ وينكلر، رئيس التخطيط الإستراتيجي بأمن المعلومات بشركة CODENOMICON

إعتماداً على إحصائية قام بها موقع Infosectoday.com لعام ٢٠١٣ تم فيها التصويت على أهم التحديات التي تواجه أمن المعلومات تم إكتشاف أن غالبية الأصوات اشارت إلى أن «قلة الدعم من الإدارة العليا» هو أكبر تحدي يواجه مكاتب أمن المعلومات في ارساء قواعد أمن المعلومات في مؤسساتهم. ولهذا قمنا بتخصيص هذا المقرر لمناقشة الحلول التي بإمكانها التغلب على مسألة ممانعة الإدارة العليا لفكرة إنشاء مكاتب أمن المعلومات بالمؤسسات الحكومية والقطاعات الحيوية.

لطالما تم النظر إلى أمن المعلومات كعائق أمام إنتاجية الموظفين وللأسف مازال هذا الإعتقاد سائداً حتى يومنا هذا. في حقيقة الأمر إذا ما تم إعطاء مدراء أمن المعلومات الدعم والموارد اللازمة لممارسة صلاحياتهم في تكوين وتأسيس خطط إستراتيجية لتفعيل دور أمن المعلومات وربطها بكافة الأقسام والدوائر المختلفة لحصل عكس ذلك تماماً! فعند تطبيق ممارسات أمن المعلومات بطريقة صحية وسليمة فذلك يمكن أن يفيض إلى تحسين الإنتاجية والسرعة في أداء العمل.

بما أنه من الصعب تحديد العائد المادي من الإستثمار في أمن المعلومات مما يشكل عائق كبير أمام مدراء أمن المعلومات أثناء محاولة تبرير الإستثمار المطلوب للإدارة العليا فإنه ومن خلال الأقسام المختلفة لهذا المقرر فإنك ستتعرف على بعض المهارات والتقنيات التي من شأنها تسهيل عملية التبرير والمساومة مع الإدارة العليا وأعضاء مجلس الإدارة.

أسباب عدم مساندة الإدارة العليا لمشاريع أمن المعلومات

قبل البدء في شرح الحلول والوسائل الفعالة في إقناع الإدارة بأهمية أمن المعلومات يتوجب علينا معرفة الأسباب الكامنة وراء عدم مساندة الإدارة العليا لأمن المعلومات في المؤسسات المختلفة للدولة.

الجميع يعتقد إن أمن المعلومات عامل تنفيذي وليس إستراتيجي

معظم أعضاء الإدارة العليا لا ينظرون إلى أمن المعلومات كعامل إستراتيجي قد يتفاعل مع جميع أقسام المؤسسة المختلفة بل ينظرون إلى قسم أمن المعلومات كقسم

صغير من المفترض أن يعمل على أداء مهامه الوظيفية بأقل تكلفة وبأقل موارد ممكنة. هذا الإعتقاد السائد سبب في تجاهل قسم أمن المعلومات وحكره بمهام ومسؤوليات صغيرة لا تتماشى مع الهدف الأسمى الذي نطمح تحقيقة من خلال هذا القسم الإستراتيجي.

إختلاف في لغة الحوار

غالباً يهتم أعضاء الإدارة العليا بلغة الأرقام و المصطلحات المادية مثل النفقات والارباح والعائد من الإستثمار ، في حين يتهم مسؤولي أمن المعلومات بمدى أهمية المعلومات وسبل حمايتها من خلال الممارسات المثلى والقوانين والتدريب والتوعية التي يستصعب قياسها بشكل مادي.

صعوبة قياس مدى كفاءة سياسة أمن المعلومات

في معظم الأحيان يتم قياس مدى الكفاءة والإنتاجية بالمردود المادي وبالرغم من مدى أهمية النتائج التي تحققها أقسام أمن المعلومات في تأمين معلومات المؤسسة إلا إنه من الصعب قياسها مادياً.

التضارب في دور قسم أمن المعلومات وقسم إدارة تقنية المعلومات

يعتقد أعضاء الأدارة العليا بأن مسؤولية أمن المعلومات يجب أن تندرج تحت مهام قسم إدارة تقنية المعلومات دون الفهم الحقيقي لدور قسم أمن المعلومات ومدى أهمية كونه قسماً منفصلاً من ناحية الإدارة لأداء مسؤولياته بشكل فعال.

عجز الإدارة العليا في فهم المخاطر المتعلقة بالجرائم الإلكترونية

للأسف حين يطرح موضوع أمن المعلومات في الإجتماعات الإدارية لا يحظى بالإهتمام المطلوب فغالباً ما يخصص له وقت ضيق لا يتمكن خلاله مدراء أمن المعلومات من طرح إقتراحاتهم و الحصول على الدعم المطلوب.

الحلول

بعد التعرف على التحديات التي تحول دون توفير الدعم الكامل لأقسام أمن المعلومات من قبل الإدارة العليا فإنه يتوجب علينا التسلح بالتقنيات والحلول المثلى للحصول على الدعم المناسب ومعرفة الطرق المناسبة لإقناع الإدارة بأهمية أمن المعلومات للمؤسسة ككل.

التعرف على الشخص المناسب لدعم قسم أمن المعلومات

من الضروري مشاركة آرائك ومقترحاتك مع المدير المالي أو الرئيس التنفيذي أو مدير التدقيق الداخلي بالمؤسسة حيث بإمكانهم إعطائك النصائح الهامة في كيفية التعامل مع باقي أعضاء الإدارة. وهذه المحادثات فرصة ممتازة لإطلاع أفراد من الإدارة العليا على التحديات والمخاطر التي تواجه المؤسسة تقنياً.

أطلع الرئيس التنفيذي للمؤسسة على القوانين التنظيمية في مجال أمن المعلومات

أمن المعلومات أصبح امراً إجبارياً من حيث سن القوانين اللازمة لتنظيم كيفية التعامل مع معلومات المؤسسة وكيفية نقلها وتخزينها والإفصاح عنها. والرئيس التنفيذي يمثل أفضل شخص بإمكانه نقل ودعم رسالة أمن المعلومات إلى أعضاء مجلس الإدارة ولهذا وجب إطلاعه على القوانين الهامة والمستحدثة في مجال أمن المعلومات.

إنتهز الفرص المناسبة لدعم قسم أمن المعلومات

عادة ما يقوم الرؤساء التنفيذيون بالمؤسسات بإختيار ما يتم عرضه لمجلس الإدارة وعليك العمل على إضافة أمن المعلومات إلى طاولة الحوار من خلال إنتهاز الأحداث المحلية والعالمية المتعلقة بأمن المعلومات وعلى سبيل المثال موجة الإختراقات التي تعرضت لها العديد من مؤسسات الدولة في الفترة الماضية وبالإضافة إلى الثغرة الدولية التي تم إكتشافها (Heart bleed) وهذا كفيل بالحصول على إهتمام أعضاء مجلس الإدارة الى المخاطر التي قد تتعرض لها المؤسسة. عند عرض مثل هذه الأحداث يجب ان يتم توثيقها بإحصائيات ومعلومات ملموسة.

إعرض مدى تقدم المؤسسات الأخرى في مجال أمن المعلومات

لتحفيز روح المنافسة عليك أن تقدم مدى التقدم المحرز في مجال أمن المعلومات من قبل المؤسسات المختلفة بالدولة وعلى سبيل المثال حصول إحدى المؤسسات على شهادة أيزو ٢٧٠٠١ أو إنشاء احدى المؤسسات لقسم أمن معلومات فعال في التصدي للهجمات الإلكترونية.

قم بالإشارة إلى مدى أهمية قسم أمن المعلومات

عليك الإشارة إلى مدى أهمية قسم أمن المعلومات والفوائد الإيجابية التي يمكن لهذا القسم تحقيقها والتركيز على الفوائد الأربع التالية:

الإمتثال للمعايير العالمية

تسعى معظم المؤسسات إلى الأمتثال إلى المعايير الدولية في معظم المجالات وبإمكانك التركيز على المعايير الدولية التي بالإمكان الحصول عليها من خلال قسم أمن المعلومات لما لها من مردود يمثل العائد من الإستثمار ومدى سهولة تطبيق هذه المعايير وأهمها ايزو ٢٧٠٠١ والتي تعتبر أعلى معيار تقاس به مدى كفاءة أمن المعلومات.

التسويق للمؤسسة

في ظل التنافس العالمي بين مختلف المؤسسات فإنه من الضروري الإشادة إلى دور أمن المعلومات في إضافة ميزة تنافسية للمؤسسة من خلال التسويق لمدى مستوى آمان معلومات المستخدمين بالمؤسسة.

تقليل المصاريف

عادة يعتبر الأستثمار في أمن المعلومات تكلفة بدون عائد مادي ملموس ولكن في الواقع بإمكان سياسات أمن المعلومات ان تعمل على حماية الإستثمارات في حال وقوع إختراق إلكتروني ولهذا فإن وجود سياسة للتعامل مع الإختراقات الأمنية يسهم في خفض التكلفة والمصاريف المتعلقة بالتصدي للهجمات الإلكترونية.

تنظيم العمل الداخلي

مع التطور السريع للمؤسسات في الآونة الأخيرة فإن أمن المعلومات قد يساعد في تنظيم العمل الداخلي بحيث ينظم عملية إتخاذ القرارات المتعلقة بمعلومات المؤسسة ومن المصرح بالتعامل معها والإفصاح عنها.

إستخدم الطرق المالية المثلى في عملية تبرير تكلفة إنشاء قسم أمن المعلومات بالمؤسسة

كما ذكرنا سابقاً فإن أعضاء الأدارة يتخذون قراراتهم حسب العائد المادي للإستثمار ولهذا عليك أن تستخدم الطرق المالية المثلى لتبرير التكلفة وعلى سبيل المثال في حال إختراق قاعدة بيانات المؤسسة ما هو المبلغ الذي سيتم إستثماره في الإحتواء والتعامل مع هذا الإختراق فبوجود قسم لأمن المعلومات بالإمكان تفادي الأختراق والحفاظ على أموال المؤسسة.

المسؤولية التنفيذية

في حالة حدوث إختراق إلكتروني لإحدى المؤسسات فإن اصابع الإتهام ستوجه للإدارة العليا ولذلك فمن الضروري إعلام الإدارة بالمخاطر المتوقع حدوثها وطرح الحلول المناسبة لتفادي أية هجمات محتملة.

الربح والخسارة في تطبيق معايير الـ PCI-DSS

في حال إستلام مؤسستك لمبالغ مادية عن طريق الإنترنت فإنه من الضروري الإمتثال لمعايير الـ PCI–DSS والتي يتوجب على المؤسسة الخضوع إلى تدقيق خارجي لمدى تطبيق هذه المعايير وبتواجد قسم أمن معلومات داخلي بالمؤسسة فإنه بالإمكان تفادي التكلفة العالية التي تترتب على طلب الخدمة من مؤسسة تعمل في مجال أمن المعلومات لتقييم وضع المؤسسة ومدى إمتثالها للمعايير العالمية.

الآثار المترتبة على وقف عمل المؤسسة بسبب الإختراقات الإلكترونية

في حالة عدم توافر قسم لإدارة أمن المعلومات بالمؤسسة فإنه من المحتمل إيقاف عمل مؤسسة بالكامل في حال حدوث إختراق إلكتروني مما يعرض المؤسسة لخسائر مادية ومعنوية. ولهذا فإنه من الضروري وجود قسم داخلي لأمن المعلومات للتعامل مع الإختراقات الأمنية.

المخترقين

الإنظمة والشبكات الغير مؤمنة قد تكون عرضة للإختراق من قبل المخترقين أصحاب القبعات السوداء وتتمثل نتائج هذه الإختراقات في:

- سرقة معلومات بنكية أو الحصول على معلومات دخول المستخدمين
- إبلاغ المستخدمين عن الإختراق ومدى الضرر الناجم عن هذا الإختراق
- الإذعان لمطالب المخترقين والتي قد تتمثل في دفع مبلغ مالي لإعادة التحكم بالنظام المخترق
- دفع مبالغ طائلة لشركات أمن المعلومات للتعامل مع الأختراق وسد الثغرات المكتشفة.

ولهذا فمن الضروري وجود قسم لأمن المعلومات بالمؤسسة للتعامل مع الإختراقات وسد الثغرات بأنظمة وشبكات المؤسسة لتفادي الإختراقات المحتملة.

خلق بيئة معلوماتية آمنة

من الضروري خلق بيئة معلوماتية آمنة لجميع العاملين بالمؤسسة من أجل دعم دور قسم أمن المعلومات وأهدافه التي تتمثل في إيجاد الطرق الآمنة للتعامل مع معلومات المؤسسة. ولعل أهم أهداف خلق هذه البيئة الآمنة هو تأثير هذه البيئة على الترابط الحيوي بين مختلف أقسام المؤسسة الداخلية والذي من شأنه رفع مستوى الثقة بين العاملين بالمؤسسة وتسهيل عملية الإمتثال للمعايير الدولية والقوانين التنظيمية لأمن المعلومات.

أيــن يقع قســم أمن المعلومــات فــي الهيكل التنظيمي للمؤسسة

هناك وجهات نظر مختلفة فيما يخص موقع قسم أمن المعلومات بالهيكل التنظيمي للمؤسسة حيث إن هذا القسم المستحدث يحتاج إلى الدعم الكامل من الإدارة العليا ولهذا يرى الكثير من الأخصائيين إنه يجب أن يتبع لمكتب الرئيس التنفيذي لما سيقدمه هذا الموقع من سهولة إلى الوصول إلى مجلس الإدارة والسهولة في الحصول على الدعم المطلوب. ولكن بغض النظر عن موقع قسم أمن المعلومات في الهيكل التنظيمي فبتوافر الدعم اللازم فبأمكان هذا القسم ان يؤدي مهامه أينما كان ولا يجب أن يشكل موقع القسم عائقاً أمام العاملين به من تأدية مهامهم المناطة إليهم.

دور المركز الوطني للسلامة المعلوماتية في دعم أقسام أمن المعلومات

قام المركز الوطني للسلامة المعلوماتية بإعداد برنامج متكامل لأقسام أمن المعلومات بمختلف المؤسسات الحكومية وقطاع الصناعات الحيوية ويقدم هذا البرنامج كافة الأدوات والقوانين والهيكل التنظيمي والمواد التوعوية اللازمة لتعزيز دور هذه الأقسام حسب دراسة علمية دقيقة قام بتنفيذها مجموعة من الأخصائيين في مجال أمن المعلومات.

بالإضافة إلى إستعداد المركز الوطني للسلامة المعلوماتية بتقديم حلقات عمل للإدارة العليا بمختلف المؤسسات لعرض مدى أهمية قسم أمن المعلومات والحصول على دعم أعضاء الإدارة العليا لإقامة قسم أمن معلومات أو تعزيز دور قسم أمن المعلومات الحالي.

الخاتمة

في الختام نود التنويه بإن الحصول على دعم الإدارة العليا يعتبر افضل وسيلة لتعزيز دور قسم أمن المعلومات ولهذا فإن هذا المقرر يعتبر حجر الأساس لإنشاء وإقامة قسم أمن معلومات يمتلك الدعم اللازم لممارسة مسؤولياته وتحقيق أهدافه.

المراجع

- ISO/IEC 17799:2005. “Information Technology - Security Techniques - Code of Practice for Information Security Management”, ISO, Geneve. (2005).
- ISO/IEC 27001:2005. “Information Technology - Security Techniques - Information Security Management Systems - Requirements”, ISO, Geneve. (2005).
- Heikkinen, I., Ramet, T., “E-Learning as a Part of Information Security Education Development from Organisational Point of View”. Oulu University, Oulu, Finland., In Finnish (2004).
- Kajava, J., “Critical Success Factors in Information Security Management in Organizations: The Commitment of Senior Management and the Information Security Awareness Programme” (Abstract in English). Hallinnon tutkimus - Administrative Studies, Volume 22, Number 1, Tampere. (2003).
- Lempinen H., “Security Model as a Part of the Strategy of a Private Hospital” (In Finnish), University of Oulu, Finland. (2002).
- OECD, “OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security”, OECD Publications, Paris, France, 29 p. (2002).

الخـــاتمة

لقد غطى هذا الكتاب الكثير من المفاهيم والمواضيع، وبإنهائك له فأنت مستعد للتعامل مع العديد من الأمور المحتمل أن تواجهها، إلا أنه من المهم التأكيد مجددا على نقطتين:

الأولى. إن موارد تقنية المعلومات المتوفرة هي للاستعمال النافع، وليست للتلاعب أو الاعتداء على خصوصيات الآخرين، فوظيفتها الأساسة هي تيسير العمل.

الثانية. إن القوانين والسياسات والإجراءات التي سُنت ليست فقط لحماية المعلومات، ولكنها أيضا للمساعدة في تحقيق الأهداف العملية والشخصية؛ لذا فمن مسؤوليتنا جميعا المساعدة في حماية هذه المعلومات.

إن من واجبك الأمني أن تقوم بتبليغ السلطات المختصة عن أية مخالفات قد تتعرض لها ولو كان لمجرد الشك، فهناك أشخاص مؤهلون واجبهم التأكد. لا تقم بعملية التحري بنفسك فقد تقوم بإتلاف بعض الأدلة المهمة، وعليك أن تتعرف على سياسة مؤسستك في تسلسل عملية البلاغ عن الاختراقات الأمنية المتعلقة بأمن المعلومات.