

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

المخاطر الإستراتيجية التي تهدد أمن المعلومات والحلول

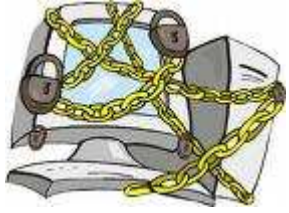
الرائد المهندس د. محمد بن عبدالله سعيد العسيري

وزارة الداخلية- حرس الحدود

المملكة العربية السعودية- الرياض

dr.aseeri@fg.gov.sa





استراتيجية أمن المعلومات

-أمن المعلومات: يعرف بالبحث في السياسات والاستراتيجيات التي ينبغي توخيها لحماية المعلومات من مختلف الاعتداءات التي قد تتعرض لها والمخاطر التي يمكن أن تهددها.

الناحية العملية: مجموعة الوسائل و التدابير و الإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر سواء من داخل بيئة المعلومات محل الحماية أو من خارجها.

استراتيجية أمن المعلومات: مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه و بلوغ أهدافه.

الهدف

- التعريف بواجب مستخدمي نظم المعلومات و الإداريين الذين لهم صلة مباشرة أو غير مباشرة بتلك النظم لحماية الحواسيب والشبكات والمعلومات في مختلف مراحل جمعها وتحصيلها داخل الحاسوب و تخزينها ومعالجتها واسترجاعها عند الحاجة و نقلها عبر الشبكات.
- ضبط الآليات التي تمكن من تنفيذ التزامات كل من له علاقة بنظم المعلومات وتحديد المسؤوليات عند حصول الخطر.
- الإجراءات التي ينبغي اتباعها تفاديا لما قد يحدث من تهديدات ومخاطر و كيفية التعامل معها عند حصولها.

عناصر الحماية

ضمان توفر العناصر الاساسية التي تؤمن الحماية للمعلومات ونظمها :

السرية

التعرف

الوثوقية

الاستمرارية

عدم الإنكار



منطلقات استراتيجية أمن المعلومات

ان البحث في السياسات و الاستراتيجيات و توفير الوسائل التقنية و الإجراءات الضرورية لحماية المعلومات تستوجب طرح تساؤلات من شأنها أن تسمح بتحديد منطلقات خطة واضحة المعالم تعد و تعتمد لضمان أمن المعلومات.

من أهم هذه التساؤلات على سبيل المثال :

- هل تتطلب كل المعلومات نفس القدر من الحماية؟
- ما الذي نريد أن نحمله ؟
- ماهي المخاطر التي يمكن أن تهدد المعلومات فتستوجب الحماية ؟
- ما هي وسائل هذه الحماية ؟
- كيف نتصرف في حالة تحقق خطر بالرغم من توفر هذه الوسائل ؟

- تصنيف المعلومات

- تحديد المخاطر

- وسائل الحماية

كيفية التعامل مع المعلومات الرئيسية المتصلة بأمن المعلومات

- تصنيف المعلومات Information classification
- التوثيق
- المهام والواجبات الإدارية والشخصية
- التعرف والتوثق Identification and Authorization
- سجل الأداء Logging
- عمليات الحفظ Back-up
- وسائل الأمن الفنية ونظام منع الاختراق
- نظام التعامل مع الحوادث Incident Handling System



حقائق لا بد من معرفتها

• حقيقة ١ :

علينا ان ندرك ابتداء ان الكمبيوتر الآمن على نحو مطلق هو فقط الكمبيوتر الذي لم يوصل بعد بمصدر الكهرباء ، وما يزال داخل الصندوق ، ولم يستعمل بعد. ومتى ما وضع الكمبيوتر في الاستخدام تبدأ المخاطر، وهي مخاطر تتراوح بين المخاطر التقليدية التي يتعرض لها أي مال منقول، وتمتد لمخاطر خاصة بطبيعة هذا الجهاز ووظائفه، وتنتهي بمخاطر يكون هو فيها مصدر الخطر لمصالح وحقوق الآخرين.

حقائق لا بد من معرفتها

• حقيقة ٢ :

الثغرات الأمنية تجدد باستمرار، للتطور المستمر في التقنيات والبرمجيات والبروتوكولات، والتجديد اما إيجابي يستخدم في رخاء البشرية او سلبي يستثمر لتحقيق اغراض غير مشروعة او ارتكاب أفعال مجرمة او أفعال ياباها السلوك الاخلاقي القويم .

ولذا ، فان تحديد المخاطر والثغرات والاعتداءات عملية مستمرة ، يوما بعد يوم ، وهي ما يميز خطط الأمن بعضها عن بعض .

حقائق لا بد من معرفتها

• حقيقة ٣ :

ثمة تحديد للمخاطر على ضوء الوسائل وعلى ضوء طبيعة المعلومات وعلى ضوء الاستخدام، وثمة تحديد للثغرات الأمنية على ضوء بيئة وواسطة التقنية، وانه لا يوجد مؤلف او باحث او مرجع يقدم قائمة شاملة للمخاطر والاعتداءات وثغرات الحماية ، لان ذلك يعني الوقوف على كل الوسائل التقنية والوقوف على كل الاستخدامات .

تصنيف المخاطر

• أولاً : خرق الحماية المادية:

- التفتيش في مخلفات التقنية: Dumpster diving

- الالتقاط السلبي : Wiretapping

- استراق الأمواج

- انكار او إلغاء الخدمة Denial or Degradation of Service

تصنيف المخاطر

• ثانيا : خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين

- التخفي بانتحال صلاحيات شخص مفوض

- الهندسة الاجتماعية

- قرصنة البرمجيات وقرصنة البرامج

تصنيف المخاطر

• ثالثا : خرق الحماية المتصلة بالاتصالات والمعطيات

• هجمات المعطيات Data Attacks

- النسخ غير المصرح به للمعطيات
- تحليل الاتصالات
- القنوات المخفية

• هجمات البرمجيات

- المصائد او الابواب الخلفية
- السرقه او اختلاس المعلومة او الاستخدام اللحظي
- الهجمات عبر التلاعب بنقل المعطيات عبر انفاق النقل
- الهجمات الوقتية
- البرمجيات الخبيثة

تصنيف المخاطر تبعا لموضع المعلومة من النظام وتبعا للواسطة التقنية

- اغلب قوائم تصنيف المخاطر تعتمد معيار موضع المعلومات من النظام، ومن ذلك مثلا قائمة منظمة الشرطة العالمية الانتربول التي نعرضها تاليا والتي تقوم من ضمن معيارها على تبويب المخاطر تبعا لموضع المعلومة أولا حيث تصنف الى ثلاثة طوائف:

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة خلق واسترجاع وتعديل وإلغاء المعلومات ، وجامعها وجود المعلومات داخل النظام .
- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة النقل ، أي التبادل بين أنظمة الكمبيوتر.
- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام .

تصنيف المخاطر والأساليب التقنية في الاعتداء تبعا لأساليب الهجوم وتقنياته وقيمة المعلومات

- على سبيل المثال:

تصنف الاعتداءات والمخاطر تبعا للدور المناط بالمعلومات موضوع الاعتداء او الحماية فقواعد معلومات المواقع العسكرية مستهدفة من جهات عديدة ، اما جهات احترافية لغايات التجسس وكشف المعلومات ، قد تكون دولاً او منظمات او افراد.

مثال : لنظام امني



وسائل الأمن

- وسائل الأمن متعددة من حيث الطبيعة والغرض ، لكن بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية الى الاتي :
 - وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته
 - الوسائل المتعلقة بالتحكم بالدخول والنفاز الى الشبكة
 - الوسائل التي تهدف الى منع افشاء المعلومات لغير المخولين بذلك
 - الوسائل المتعلقة بمنع الانكار
 - وسائل مراقبة الاستخدام وتتبع سجلات النفاذ او الأداء

أكثر وسائل الأمان شيوعاً في بيئة نظم المعلومات

- برمجيات كشف ومقاومة الفيروسات
- الجدران النارية Firewall
- التحقق من هوية المستخدمين
- الشبكات الافتراضية الخاصة
- مراقبة المحتوى
- البحث عن الفيروسات ، ومراقبة عناوين الإنترنت ، منع برمجيات جافا ، وبرمجيات فحص ومراقبة الكلمات السرية
- التشفير

الخاتمة

- يجب عدم اعتبار أن مسؤولية أمن المعلومات تقع على عاتق مسؤولي الأمن فقط، بل أنها أصبحت تهم المؤسسة بأكملها. فالأمن ليس بعملية تتم مرة واحدة فقط ولا يمكن تناوله بالحلول التي ترضى جميع الأطراف، فإنها عملية متواصلة لإدارة التغيير.
- يجب أن تتوافق آليات الأمن والسياسات والأساليب والإجراءات الأمنية والاستراتيجيات مع التغيير في المخاطر، والضروريات والمتطلبات والحلول التقنية والابتكار، وقواعد وإجراءات التعامل .
- يجب أن يتم التفاعل مع الأحداث وأن يكون فعالا في منع المخاطر قبل وقوعها .
- يجب ان يتم التعبير عن مزايا الأمن الجيد بتفاديه النتائج السيئة بدلاً من أن يحقق نتائج إيجابية فقط.

شكرًا على اصغائكم