إطار الأمن السيبراني
مؤسسة النقد العربي السعودي (سما)

يساعد حل سيرتش انفورم (SearchInform)
مؤسستك على حماية المعلومات والتعاملات السرية وتحديد التهديدات الأمنية وإنشاء إطار واضح
المعالم للأداء الآمن في القطاع المالي والامتثال التنظيمي الآلي

عمليات الأمن السيبراني & التكنولوجيا

إدارة الأصول	الأمن المادي	الموارد البشرية	
تغيير الإدارة	أمان التطبيق	إدارة الهوية والوصول	البنية التحتية للأمن السيبراني
اجلب جهازك الخاص	التشفير	أمن البنية التحتية	
إدارة أحداث الأمن السيبراني	الخدمات المصرفية الإلكترونية	أنظمة الدفع	تأمين التخلص من أصول المعلومات
إدارة الثغرات الأمنية	إدارة التهديدات	إدارة حوادث الأمن السيبراني	

أمن البنية التحتية

يحتوي القانون على إشارة واضحة لأهمية نظام منع البيانات من التسرب والفقدان"DLP"
الفقرة 3.3.8 تشدد حول أمن البنية التحتية على ضرورة تقديم الحلول:

6"معيار أمن البنية التحتية يجب أن يشمل :
أ. تطبيق ضوابط الأمن السيبراني (على سبيل المثال ، معلمات التكوين ، والأحداث لرصدها والاحتفاظ بها [بما في ذلك الوصول إلى النظام والبيانات] ، ومنع تسرب البيانات [DLP] ، وإدارة الهوية والوصول ، والصيانة عن بُعد) ؛

ج. حماية البيانات المحاذة (المتفق عليه) نظام التصنيف (بما في ذلك سرية بيانات العميل ، وتجنب الوصول غير المصرح به و تسرب البيانات المقصود أو الغير مقصود) ؛

البنية التحتية للأمن السيبراني

الفقرة 3.3.4 تصف نظاما مشابها لنظامنا " Risk Monitor"
- مراجعة حوادث الأمان
- البنية التحتية لتكنولوجيا المعلومات وجرد البيانات
- عرض تدفق البيانات
- مراقبة حالة أنظمة الأمان

الأمن المادي

المهام:
- النظام يسمح لك بمراقبة نشاط الموظف على محطة العمل
- البرامج المستخدمة
- النشاط على الإنترنت
- تسجيل صوت من خلال ميكرفون الحاسوب
- تسجيل صوت لمكالمات العمل
- تسجيل فيديو لنشاطات المستخدم
- التقاط صور وفيديو للموظفين على محطة العمل(على سبيل المثال : عندما يتم ادخال اسم المستخدم وكلمة المرور الى أنظمة العمل)
- تدقيق على عمليات نظام الملفات وخوادم الملفات
- التدقيق على البيانات المنقولة من خلال قنوات التواصل أو التي يتم تحميلها إلى الأجهزة

3." عمليات الأمن المادي يجب ان تشكل (على سبيل المثال وليس الحصر) :
ب.مراقبة والإشراف (على سبيل المثال: أنظمة مراقبة عبر الكاميرات ، تتبع مواقع ماكينات الصراف الآلي ،جهاز استقبال الحساسية)
ج. حماية مراكز البيانات وغرف البيانات
هـ. حماية أصول المعلومات أثناء دورة الحياة (بما في ذلك النقل والتخلص الآمن ، وتجنب الوصول غير المصرح به و تسرب البيانات المقصود أو غير مقصود. "

الموارد البشرية

الفقرة 3.3.1 " الموارد البشرية تلمح الى وجود مشكلات معينة والتي يمكن حلها من خلال حلولنا "TimeInformer & FileAuditor" :
- وجود الموظف أو غيابه (مع مراعاة أنشطة الموظف على محطة العمل وبيانات الاتصال وأرشفة الصور)
- الوقت الذي يقضيه في مواقع الويب والعمل مع برامج محددة ، بما في ذلك تصنيف الأنشطة (المتعلقة بالعمل ، غير المرتبطة بالعمل ، المحايدة ، غير المحددة)
- كفاءة أداء الموظف
- مراجعة حقوق الوصول
- سجل استخدام البيانات على أجهزة الكمبيوتر وعلى خوادم الملفات

- مسح المحتوى وتصنيف المعلومات المخزنة

"اعتبارات التحكم
1. ينبغي أن تحدد عملية الموارد البشرية متطلبات الأمن السيبراني وتوافق عليها وتنفذها.
2. يجب مراقبة فعالية عملية الموارد البشرية وقياسها وتقييمها دوريًا.
3- يجب أن تشمل عملية الموارد البشرية:
أ. مسؤوليات الأمن السيبراني وشروط عدم الكشف في اتفاقيات الموظفين (أثناء وبعد التوظيف)
ب. يجب أن يتلقى الموظفون الوعي بالأمن السيبراني في بداية عملهم وخلاله ؛
ج. عندما تكون حاجة الى تطبيق الإجراءات التأديبية
د. الفحص والتحقق من الخلفية
هـ. أنشطة الأمن السيبراني بعد التوظيف ، مثل:
1. إلغاء حقوق الوصول
2. إعادة أصول المعلومات المخصصة (على سبيل المثال ، شارة الدخول ، الرموز ، الأجهزة المحمولة ، جميع المعلومات الإلكترونية والمادية). "

إدارة الهوية والوصول

الفقرة 3.3.5 تشير إلى المشكلات التي يتم حلها بواسطة حلولنا "SIEM & FileAuditor "
- مراقبة الوصول الى الملفات في نظام الملفات
- مراقبة العمليات على الملفات الموجودة على خوادم الملفات ومحطات العمل المحلية ، في مجلدات الشبكة
- مراقبة تخزين الملفات فيما يتعلق بتوافق المحتوى مع مستوى الوصول
- مراقبة التغييرات التي تم إجراؤها على إعدادات الأمان لأنظمة تقنية المعلومات
- رصد الأحداث الأمنية الحرجة في أنظمة تكنولوجيا المعلومات

الهدف
للتأكد من أن فقط عنصر المؤسسة يتوفر على امتيازات وصول مصرح بها وكافية للمستخدمين المعتمدين.
اعتبارات التحكم
1. يجب تحديد سياسة إدارة الهوية والوصول ، بما في ذلك المساءلة والمسؤوليات ، والموافقة عليها وتنفيذها.
2. يجب مراقبة الامتثال لسياسة الهوية والوصول.
3. ينبغي قياس فعالية ضوابط الأمن السيبراني ضمن سياسة إدارة الهوية والوصول وتقييمها دوريًا.
4. تتم الموافقة رسميًا على طلبات وصول المستخدمين وفقًا لمتطلبات العمل والامتثال (أي ، الحاجة إلى امتلاكها أو الحاجة إلى معرفتها لتجنب الوصول غير المصرح به و تسرب البيانات المقصود أو الغير مقصود)) ؛
5. يجب معالجة التغييرات في حقوق الوصول في الوقت المناسب ؛
6. يجب مراجعة حقوق وصول المستخدم والحسابات بشكل دوري

التشفير

الفقرة 3.3.9 توفر لنا متطلبات التشفير
يسهل برنامجنا إنشاء محيط تشفير لأجهزة التخزين المحمولة الخاصة بالعمل حيث يتم تحميل البيانات على محركات أقراص فلاش ونقلها بحرية ولكن يمكن استخدامها فقط داخل شبكة الشركة أو على أجهزة الكمبيوتر الخاصة للشركات.
يتيح لك الحل تقييد الوصول إلى البيانات المحمية وامكانية منح حقوق الوصول لمجموعات محددة من المستخدمين.

تأمين التخلص من أصول المعلومات

الفقرة 3.3.11 تسلط الضوء على مهام "تأمين التخلص من أصول المعلومات" والتي يمكن إدارتها بمساعدة حلولنا "DLP, FileAuditor" (لتحديد النقل غير المنظم أو تخزين البيانات التي يجب حذفها)
تحديد النسخ غير المحذوفة:

- على أجهزة الكمبيوتر المحلية (مجلد المستندات ، سطح المكتب ، إلخ ، بما في ذلك طباعة الشاشة)
- في مجلدات الشبكة
- على خوادم الملفات
- في التخزين السحابي
- شبكة التخزين المرفقة
- في نظام إدارة قواعد البيانات
- في أنظمة العمل (CRM ، إلخ)

المبدأ
يجب استبعاد أصول المعلومات بشكل آمن في حال أن عضو المؤسسة لم يعد يحتاج الى هذه الأصول.
الهدف
لضمان حماية أعمال عضو المؤسسة والعميل والمعلومات الحساسة الأخرى من التسرب أو الكشف غير المصرح به عند التخلص منها.
اعتبارات التحكم
1- ينبغي تحديد معيار وإجراءات التخلص الآمن وإقرارها وتنفيذها.
2. يجب مراقبة الامتثال لمعايير وإجراءات التخلص الآمن.
3. ينبغي قياس فعالية ضوابط الأمن السيبراني للتخلص الآمن وتقييمها دورياً
4. يجب التخلص من أصول المعلومات وفقًا للمتطلبات القانونية والتنظيمية ، عندما لا تكون هناك حاجة (على سبيل المثال ، استيفاء لوائح خصوصية البيانات لتجنب الوصول غير المصرح به وتجنب تسرب البيانات المقصود أو الغير مقصود).

إدارة أحداث الأمن السيبراني

الفقرة 3.3.14 "إدارة أحداث الأمن السيبراني" تشرح عن نظام إدارة أحداث أمن المعلومات " SIEM"
مشابه لحل شركة سيرتش انفورم SearchInform
SIEM SearchInform يجمع الأحداث من مصادر مختلفة:

- سجلات الأحداث للخوادم ومحطات العمل
- المعدات النشطة في الشبكة
- التحكم في الوصول ، والتوثيق
- مضادات الفيروسات
- البيئات الافتراضية

يقوم SIEM بتحليل البيانات والكشف عن الحوادث وتنفيذ تقارير الحوادث في الوقت الفعلي.
يحدد النظام:

- أوبئة الفيروس و الالتهابات الفيروسية المنفصلة
- محاولات للوصول غير المصرح به إلى المعلومات السرية
- الأخطاء والفشل في تشغيل نظم المعلومات
- تزوير الاعتماد
- الأحداث الحرجة أثناء تشغيل نظام الأمن

المبدأ
يجب على عضو المؤسسة أن يحدد عملية إدارة الأحداث الأمنية والموافقة عليها وتنفيذها لتحليل سجلات التشغيل والأمان والرد على أحداث الأمان. ينبغي قياس فعالية هذه العملية وتقييمها بشكل دوري.