CONCEPT

دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية: ضوابط الحماية والتعامل مع الحوادث



دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية: ضوابط الحماية والتعامل مع الحوادث

مقدمة:

دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية دورة تطبيقية مدتها 3 أيام لمديري الإدارات وموظفي تقنية المعلومات والأمن والعاملين في المخاطر والامتثال وملاك أصول المعلومات، وتنتهي بإعداد سجل مخاطر الأصول الرقمية والجاهزية للحوادث لوحدة عمل واحدة. فكثير من الوحدات لا تعرف على وجه الدقة ما تملكه من أنظمة وبيانات ولا الضوابط التي تحميها، فلا تظهر نقاط الضعف إلا عند وقوع حادث يعطل العمل. ويدير المشاركون أنظمة ومعلومات في وحداتهم أو يدعمونها، ويتدربون على دراسات حالة من قطاعات متعددة. وتقدم كور كونسبت هذه الدورة في حماية الأصول الرقمية من المخاطر السيبرانية.

أهداف الدورة:

- بناء سجل جرد للأصول الرقمية يحدد المالك والموقع ومستوى التصنيف لكل نظام ومجموعة بيانات
- تقييم المخاطر السيبرانية لكل أصل بربط التهديدات والثغرات بدرجات الاحتمال والأثر
- اختيار الضوابط الوقائية من المجموعة الأولى في CIS Controls v8.1 للمخاطر الأعلى درجة
- مواءمة ضوابط الوحدة مع وظائف إطار NIST CSF 2.0 ومحاور الضوابط في معيار ISO/IEC 27001:2022
- تطبيق خطوات التعامل مع الحوادث من الاكتشاف والإبلاغ إلى الاحتواء والتعافي واستخلاص الدروس
- إعداد سجل مخاطر الأصول الرقمية والجاهزية للحوادث مع المسؤولين وإجراءات المتابعة

الفئة المستهدفة:

- مديرو الإدارات المسؤولون عن أنظمة الوحدة وبياناتها وصلاحيات وصول موظفيها
- موظفو تقنية المعلومات والأمن المسؤولون عن إعداد أنظمة الأعمال وتحديثها ومراقبتها
- العاملون في المخاطر والامتثال المسؤولون عن تسجيل المخاطر والتحقق من عمل الضوابط
- ملاك المعلومات والبيانات المسؤولون عن تحديد التصنيف وصلاحيات الوصول إلى السجلات
- منسقو استمرارية الأعمال والعمليات المسؤولون عن استعادة الخدمات بعد الانقطاع

محاور الدورة:

اليوم 1: جرد الأصول الرقمية وأسس المخاطر السيبرانية

- وظائف إطار NIST CSF 2.0 الست لحماية الوحدة
- نموذج جرد الأصول الرقمية للأجهزة والبرمجيات والبيانات
- نظام تصنيف المعلومات وتعيين مالك لكل أصل
- قائمة التهديدات والثغرات الشائعة في أنظمة الأعمال
- تقييم سجل المخاطر السيبرانية حسب الاحتمال والأثر

اليوم 2: ضوابط الحماية الأساسية وخطوات التعامل مع الحوادث

- اختيار ضوابط المجموعة الأولى في CIS Controls v8.1
- مراجعة صلاحيات الوصول والتحقق من تغطية المصادقة متعددة العوامل
- قوائم التحقق من التحديثات والنسخ الاحتياطي والإعداد الآمن
- ربط محاور ضوابط ISO/IEC 27001:2022 بمخاطر الوحدة
- مسار معالجة الحوادث والإبلاغ وفق NIST SP 800-61 Rev. 3

اليوم 3: تطبيق دراسات الحالة وإعداد سجل الجاهزية

- دراسة حالة اختراق حساب عبر التصيد في وحدة مالية
- دراسة حالة انقطاع ببرمجية فدية في مركز عمليات خدمية
- استكمال سجل الاحتواء والتعافي والدروس المستفادة
- خطة توعية الموظفين المرتبطة بأسباب الحوادث المسجلة
- استكمال سجل مخاطر الأصول الرقمية والجاهزية للحوادث

المهارات التي ستكتسبها:

- إدارة جرد الأصول الرقمية
- تصنيف المعلومات
- تقدير درجات المخاطر السيبرانية
- اختيار الضوابط الأمنية
- مراجعة صلاحيات الوصول
- التحقق من النسخ الاحتياطي والتحديثات
- فرز الحوادث والإبلاغ عنها
- تحليل الدروس المستفادة

لماذا تحضر هذه الدورة:

- تسليم سجل مخاطر الأصول الرقمية والجاهزية للحوادث إلى رئيس الوحدة وإدارة أمن المعلومات
- تحديد المخاطر السيبرانية التي تحتاج ضوابط جديدة أولا بناء على قيمة الأصل ودرجة التعرض
- تجنب الانقطاعات الطويلة وفقدان البيانات الناتجة عن نسخ احتياطية غير مختبرة وتحديثات ناقصة وإبلاغ غير واضح
- إرشاد الزملاء إلى الإبلاغ عن الأحداث المشبوهة واتباع خطوات التعامل مع الحوادث في الوحدة

الخاتمة:

بعد العودة إلى العمل يعرض المشارك سجل مخاطر الأصول الرقمية والجاهزية للحوادث على رئيس الوحدة وإدارة أمن المعلومات. ويعتمدان عليه في الاتفاق على الضوابط التي تمول أو تعزز، وتحديد مالك كل أصل، وطريقة الإبلاغ عن الحوادث وتصعيدها. وبعد أول تمرين على الحوادث أو حادث فعلي ينبغي أن تحدث الوحدة درجات المخاطر، وتسجل ما أبطأ الاحتواء أو التعافي، وتتأكد من إتمام اختبارات استعادة النسخ الاحتياطية ومراجعات الصلاحيات كما خطط لها.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية؟

يحتاج المشارك إلى معرفة الأنظمة والبيانات والموردين الرئيسيين الذين تعتمد عليهم وحدته. ويساعد إحضار قائمة بالتطبيقات المهمة وأي سجل أصول أو مخاطر قائم وحادث أو شبه حادث وقع مؤخرا على ربط دراسات الحالة بوحدته.

بم تختلف دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية عن دورات حوكمة الأمن السيبراني لمجالس الإدارة؟

تساعد دورات الحوكمة على مستوى المجلس أعضاءه على تحديد شهية المخاطر والإشراف على برامج الأمن السيبراني. أما هذه الدورة فتعمل على مستوى الوحدة، فتبني جرد الأصول وتقيم المخاطر وتتحقق من الضوابط وتتدرب على خطوات التعامل مع الحوادث التي ينفذها المديرون والموظفون بأنفسهم.

ما الضوابط التي تدعم إدارة المخاطر السيبرانية وحماية الأصول الرقمية؟

تحدد المجموعة الأولى في CIS Controls v8.1 ضوابط النظافة السيبرانية الأساسية، مثل جرد الأصول والإعداد الآمن وإدارة الصلاحيات والتحديثات والنسخ الاحتياطي والتوعية. ويجمع إطار NIST CSF 2.0 هذه النتائج في وظائف الحوكمة والتحديد والحماية والاكتشاف والاستجابة والتعافي.

ماذا يعود به المشارك من دورة إدارة المخاطر السيبرانية وحماية الأصول الرقمية؟

يعود المشارك بسجل مخاطر الأصول الرقمية والجاهزية للحوادث، ويضم الأصول ومالكيها وتصنيفها ودرجات مخاطرها والضوابط المختارة وجهات الإبلاغ عن الحوادث، إضافة إلى قوائم تحقق لمراجعة الصلاحيات والنسخ الاحتياطي والتحديثات ونموذج لسجل الدروس المستفادة.