



التوعية بالأمن السيبراني للقيادات التنفيذية: التحديات والرقابة وقرارات الأزمات

16 - 20 Aug 2027

لندن - فندق أربع نجوم في وسط لندن



التوعية بالأمن السيبراني للقيادات التنفيذية: التهديدات والرقابة وقرارات النزاهات

المرجع: 1016_300 التاريخ: 20 Aug 2027 - 16 الموقع: لندن - فندق أربع نجوم في وسط لندن الرسوم: SAR 23000

العقود التقني: مفاهيمي - أسلوب التطبيق: محاكاة

مقدمة

يستهدف المهاجمون القيادات العليا مباشرة بصورة متزايدة، عبر طلبات دفع منتحلة ومكالمات بالترتيب العميق وأجهزة شخصية مخترقة، وسرعان ما يتحول الحادث السيبراني إلى أزمة قيادية لها تبعات نظامية ومالية وأثر على السمعة. وما زال كثير من التنفيذيين يعدون الأمن السيبراني شأنًا تقنيًا، فيواجهون أول قرار حقيقي في أثناء الهجوم. تبني هذه الدورة من كور كونسبت الوعي والتقدير اللذين تحتاجهما القيادات لحماية أنفسهما ومساءلة تقارير الأمن والتصرف تحت الضغط. ويتدرب المشاركون على القرارات في محاكاة محددة بزمن، ويخرجون بخطة الجاهزية السيبرانية للقيادات التنفيذية.

أهداف الدورة

- التعرف على أنماط الهجوم الأكثر استهدافًا للقيادات والمؤسسات، من برامج الفدية إلى الاحتيال بالترتيب العميق
- فهم إطار 2.0 CSF NIST والمواصفتين IEC/ISO 27001 و IEC/ISO 27014 بها يكفي لمساءلة قيادات الأمن والحكم على تقاريرهم
- تطبيق ممارسات الأمن الشخصي وبروتوكولات التحقق التي تحمي حسابات القيادات وأجهزتهم واعتداداتهم
- مساءلة التقارير الإدارية عن المخاطر السيبرانية ومستوى تقبل المخاطر ومخاطر الأطراف الثالثة بأسئلة ودروس
- اتخاذ القرارات الحرجة زمنيًا في أثناء الحادث السيبراني وإبلاغها ضمن هيكل متفق عليه لإدارة النزاهات
- الالتزام بخطة الجاهزية السيبرانية للقيادات التنفيذية للمتابعة على المستويين الشخصي والمؤسسي

الفئة المستهدفة

- الرؤساء التنفيذيون والمديرون العامون المسؤولون عن المخاطر المؤسسية
- أعضاء مجالس الإدارة ولجان المراجعة المشرفون على المخاطر السيبرانية
- الرؤساء التنفيذيون للمالية المسؤولون عن ضوابط المدفوعات والتأمين السيبراني
- رؤساء الشؤون القانونية والامتثال والاتصال المؤسسي الذين يتحركون في النزاهات السيبرانية
- الرؤساء التنفيذيون للعمليات ورؤساء وحدات الأعمال الذين تعهد خدماتهم على الأنظمة الرقمية
- القيادات العليا في القطاع العام المسؤولة عن الخدمات المقدمة للمواطنين

محاور الدورة

اليوم الأول: بيئة التهديدات التي تواجه القيادات

- أنواع الجهات المهاجمة ودوافعها بأثلة من إطار MITRE ATT&CK لتكتيكات الهجوم
- نهاذج أعمال برامج الفدية والابتزاز المزدوج
- اختراق البريد الإلكتروني للأعمال وأنماط انتحال صفة القيادات
- الاحتيال بالصوت والفيديو المزيفين عميقًا لاستهداف القيادات العليا
- لحظة عن التعرض السيبراني للمؤسسة باستخدام ملفات 2.0 CSF NIST

اليوم الثاني: النظر التي ينبغي أن يعرفها كل تنفيذي

- وظيفة الحوكمة Govern في NIST CSF 2.0 ومسؤوليات القيادة
- أساسيات نظام إدارة أمن المعلومات وفق IEC/ISO 27001:2022
- عمليات حوكمة أمن المعلومات وفق IEC/ISO 27014
- مبادئ ISA-NACD لرقابة مجالس الإدارة على المخاطر السيبرانية
- مفاهيم القياس الكمي للمخاطر السيبرانية بنموذج FAIR

اليوم الثالث: سلوكيات القيادة وأسلحة الرقابة

- الذهن الشخصي للقيادات: الأجهزة والسفر والبصمة على وسائل التواصل الاجتماعي
- بروتوكولات التحقق من المدفوعات والاعتمادات لمواجهة الانتحال
- أسئلة لوحة معلومات الأمن السيبراني ومؤشرات النداء الرئيسية في التقارير الإدارية
- مبادئ بيان تقبل المخاطر السيبرانية
- أسئلة مخاطر الأمن السيبراني للطرف الثالث وسلسلة الإمداد الموجهة إلى الموردين

اليوم الرابع: الحوادث وقرارات النزاهات والصمود

- دورة إدارة الحوادث وفق IEC/ISO 27035-1
- اعتبارات قرار دفع الفدية ودور المستشار القانوني
- بروتوكول التواصل في النزاهات مع الجهات التنظيمية والعملاء ووسائل الإعلام
- أهداف التعافي وربطها باستمرارية الأعمال وفق ISO 22301
- أخطاء القيادات المستخلصة من مراجعات منشورة لحوادث اختراق

اليوم الخامس: محاكاة الطاولة والتخطيط للعمل

- محاكاة طاولة لهجوم فدية: الساعات الأربع النولى
- محاكاة احتيال بالترتيب العميق لصوت أحد التنفيذيين: اعتداء دفعة تحت الضغط
- استخلاص الدروس من المحاكاة ومراجعة سجل القرارات
- إعداد مسودة خطة الجاهزية السيبرانية للقيادات التنفيذية
- مراجعة العملاء للتخطيط والتدريب على إحاطة مجلس الإدارة

المهارات المكتسبة

- الوعي بالتهديدات السيبرانية
- الرقابة على المخاطر السيبرانية
- كشف أساليب الهندسة الاجتماعية
- اتخاذ القرار في النزاهات
- التواصل في النزاهات السيبرانية
- قراءة تقارير الأمن السيبراني
- مساءلة مخاطر الأطراف الثالثة
- التخطيط للصمود المؤسسي

لهذا تحضر هذه الدورة

- تعود إلى عملك بخطة الجاهزية السيبرانية للقيادات التنفيذية وقد اختبرت في محاكاة لهجوم فدية واحتيال بالترتيب العميق
- تعرف القرارات التي تقع على عاتقك في الساعات الأولى من الحادث ومن يجب أن يكون إلى جانبك
- تسد الثغرات في أجهزتك وحساباتك وعادات الاعتقاد لديك التي يستغلها المهاجمون للوصول إلى المؤسسة
- تستمع إلى تجارب قيادات من قطاعات ودول مختلفة في التعامل مع الاختراقات وما كانوا سيغيرونه

الخاتمة

يحسم الذهن السيبراني في قاعات مجالس الإدارة ومكاتب القيادات بقدر ما يحسم في مراكز العمليات الذهنية. تنتقل هذه الدورة من التهديدات التي تستهدف القيادات، مروراً بالنظر التي ينبغي أن يعرفها التنفيذيون وأسلحة الرقابة التي يطرحونها، وصولاً إلى القرارات التي ترسم الساعات الأولى من النزعة. ويضع اليوم النذير المشاركين في محاكاة محددة بزمن، ويحول الدروس إلى خطة الجاهزية السيبرانية للقيادات التنفيذية، حتى تواجه المحاولة التالية على المؤسسة فريق قيادة مستعداً.