CONCEPT

الأمن السيبراني في البنوك والمؤسسات المالية:
ضوابط المدفوعات والصمود السيبراني

8 – 12 مارس 2027

دبي - فندق خمس نجوم في وسط الأعمال



الأمن السيبراني في البنوك والمؤسسات المالية: ضوابط المدفوعات والصمود السيبراني

المرجع: 974_21957 **التاريخ:** 8 – 12 مارس 2027 **المكان:** دبي - فندق خمس نجوم في وسط الأعمال **الرسوم:** SAR 21450

مقدمة:

الأمن السيبراني في البنوك والمؤسسات المالية محور هذه الدورة الممتدة أسبوع، وهي موجهة إلى فرق أمن المعلومات ومخاطر التقنية والمخاطر التشغيلية والامتثال في البنوك وشركات التأمين وشركات الدفع، وتنتهي بإعداد تقييم للصمود السيبراني وتقرير لمجلس الإدارة لبنك افتراضي. تتكبد المؤسسات خسائر حين تقيم ضوابط احتيال المدفوعات ومصادقة العملاء وحماية قنوات البطاقات كلا على حدة، ثم ترفع إلى المجلس دون تقدير كمي للتعرض. يتولى المرشحون ضوابط أمنية أو يراجعونها في عملهم، وتقدم الدورة بأسلوب دراسة الحالة على تدفقات دفع وأدلة ضوابط وسيناريوهات خسارة واقعية. وقد صممت كور كونسبت هذه الدورة لمجموعات مختلطة من مؤسسات متعددة.

أهداف الدورة:

- ربط التهديدات السيبرانية التي تواجه البنوك وشركات التأمين وشركات الدفع بالخدمات الحيوية وحدود تحمل الأثر لكل منها
- تقييم بيئات البطاقات والمدفوعات والرسائل بين البنوك مقابل أهداف معيار PCI DSS لحماية بيانات البطاقات ومجموعات ضوابط أمن العملاء
- تحديد ضوابط التحقق من المدفوعات والمصادقة القوية للعملاء ومنع الاستيلاء على الحسابات في القنوات الرقمية وأجهزة الصراف الآلي والبطاقات
- تقدير التعرض لخسائر الحوادث السيبرانية كميا بنموذج FAIR لتحليل مخاطر المعلومات، وتحديد نطاق اختبارات الصمود المبنية على التهديدات وتمارين السيناريوهات
- تصنيف الحوادث السيبرانية التي تعطل الخدمات المالية والإبلاغ عنها وفق التوقعات الرقابية ومتطلبات إخطار العملاء
- إعداد تقييم الصمود السيبراني وتقرير مجلس الإدارة متضمنا المقاييس ومؤشرات المخاطر الرئيسية وخارطة معالجة مرتبة حسب الأولوية

الفئة المستهدفة:

- فرق أمن المعلومات المسؤولة عن حماية منصات المدفوعات والبطاقات والخدمات المصرفية الرقمية
- وحدات مخاطر التقنية التي تقيم المخاطر التقنية والسيبرانية في العمليات المصرفية والتأمينية
- وحدات المخاطر التشغيلية المسؤولة عن صمود الخدمات المالية الحيوية وبيانات أحداث الخسارة
- وحدات الامتثال التي تتابع التوقعات الرقابية في الأمن السيبراني وواجبات الإبلاغ عن الحوادث
- وحدات عمليات الدفع ومكافحة الاحتيال التي تملك قواعد التحقق من المعاملات والمصادقة
- وحدات الرقابة الداخلية والتأكيد التي تختبر الضوابط السيبرانية في المؤسسات المالية

محاور الدورة:

اليوم 1: مشهد التهديدات السيبرانية في القطاع المالي والوضع الراهن

- مصفوفة ملامح التهديدات للبنوك وشركات التأمين وشركات الدفع
- ربط الخدمات الحيوية بحدود تحمل الأثر السيبراني
- تصنيف خسائر الاحتيال المدعوم سيبرانيا في الخدمات المصرفية للأفراد والشركات
- ملف إطار NIST Cybersecurity Framework لإدارة مخاطر الأمن السيبراني في مؤسسة مالية
- خط أساس نضج الصمود السيبراني باستخدام بطاقة تقييم قطاعية

اليوم 2: معايير الأمن في القطاع المالي والتوقعات الرقابية

- مبادئ الصمود التشغيلي للبنوك وأدوار حوكمة الأمن السيبراني
- مواءمة ضوابط ISO/IEC 27001 لنظم إدارة أمن المعلومات مع العمليات المصرفية الأساسية
- أهداف الضوابط الستة في معيار PCI DSS لبيئات بيانات حاملي البطاقات
- ضوابط أمن العملاء في شبكات الرسائل بين البنوك والتصديق المستقل
- تحليل الفجوات مقابل التوقعات الرقابية باستخدام سجل المتطلبات

اليوم 3: ضوابط المدفوعات والقنوات ومصادقة العملاء

- التحقق من أوامر الدفع وضوابط معاودة الاتصال لتحويلات الخزينة
- عوامل المصادقة القوية للعملاء وتصميم الربط الديناميكي للمعاملة
- منع الاستيلاء على الحسابات بربط الأجهزة والمؤشرات السلوكية
- مراجعة قائمة ضوابط أمن أجهزة الصراف الآلي وقنوات البطاقات
- استبيان العناية الواجبة الأمنية لشركاء التقنية المالية ومزودي الحوسبة السحابية

اليوم 4: القياس الكمي للمخاطر السيبرانية واختبار الصمود والإبلاغ عن الحوادث

- سيناريوهات الخسارة بنموذج FAIR لأحداث احتيال المدفوعات
- نطاق اختبار الصمود المبني على التهديدات وخطة التحقق من الضوابط
- تصميم تمرين سيناريو سيبراني حاد لكنه معقول الحدوث
- تصنيف الحوادث وفق ISO/IEC 27035 لإدارة حوادث أمن المعلومات عند تعطل الخدمات المالية
- نموذج الإخطار الرقابي بالحادث وسجل التواصل مع العملاء

اليوم 5: دراسة حالة: تقييم الصمود السيبراني لبنك افتراضي

- ملف البنك الافتراضي مع تدفقات الدفع وجرد القنوات
- بناء الحالة: تقييم الصمود السيبراني مقابل مجموعات الضوابط السابقة
- لوحة مؤشرات المخاطر الرئيسية ومقاييس الأمن لمجلس الإدارة
- خارطة معالجة مرتبة حسب التعرض الكمي للخسارة
- استكمال تقرير الصمود السيبراني لمجلس الإدارة ومراجعة الأقران

المهارات التي ستكتسبها:

- تحديد ملامح التهديدات في القطاع المالي
- وضع حدود تحمل الأثر
- مراجعة بيئات بيانات حاملي البطاقات
- تصميم ضوابط احتيال المدفوعات
- تصميم مصادقة العملاء
- القياس الكمي للخسائر السيبرانية
- اختبار سيناريوهات الصمود
- الإخطار بالحوادث السيبرانية

لماذا تحضر هذه الدورة:

- العودة بتقييم للصمود السيبراني وتقرير لمجلس الإدارة مبنيين على بنك افتراضي، جاهزين لمراجعة الرئيس التنفيذي للمخاطر ولجنة المخاطر في المجلس
- تحديد ضوابط المدفوعات والمصادقة وقنوات البطاقات التي تستحق التعزيز أولا بناء على التعرض الكمي للخسارة لا على ملاحظات التدقيق وحدها
- تجنب الإخطارات المتأخرة أو الناقصة بالحوادث وافتراضات التعافي غير المختبرة التي تعرض المؤسسة لملاحظات رقابية وضرر للعملاء
- نقل مصفوفة ملامح التهديدات وتصميم تمرين السيناريو ولوحة المقاييس إلى فرق الأمن ومكافحة الاحتيال والمخاطر التشغيلية

الخاتمة:

بعد عودة المشاركين، يستطيع الرئيس التنفيذي للمخاطر ولجنة المخاطر في مجلس الإدارة استخدام تقييم الصمود السيبراني وتقرير المجلس لتحديد نقاط الضعف في المدفوعات والمصادقة وقنوات البطاقات التي تمول معالجتها أولا، وحدود تحمل الأثر المقبولة. وتعيد فرق الأمن ومكافحة الاحتيال استخدام لوحة المقاييس في التقارير الدورية، وتضيف وحدة المخاطر التشغيلية سيناريوهات الخسارة إلى سجل المخاطر. وبعد أول دورة لتقارير المجلس، تراجع المؤسسة ما إذا تحركت مؤشرات المخاطر الرئيسية كما هو متوقع، وما إذا كشف تمرين السيناريو فجوات لم تشملها خارطة المعالجة.