JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك

31 يناير – 4 فبراير 2027

أونلاين

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك

المرجع: 86094_2308 **التاريخ:** 31 يناير – 4 فبراير 2027 **المكان:** أونلاين **الرسوم:** GBP 1900

الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك دورة تدريبية مدتها أسبوع لمهندسي أمن المعلومات ومختصي مخاطر التقنية في البنوك، تنقل أنظمة المدفوعات والأنظمة الأساسية بعيدا عن الخوارزميات المعرضة للكسر الكمي، وتنتهي بخارطة طريق الانتقال الآمن كميا. فالبيانات المشفرة التي تلتقط اليوم يمكن تخزينها وفك تشفيرها لاحقا، ما يعرض سجلات العملاء والتسويات طويلة العمر منذ الآن. وتقدم جوبيتر برايم للتدريب هذه الدورة في الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك.

لماذا يهم الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك الآن

ثلاث قوى تحرك هذا الملف. التقدم المتواصل في العتاد الكمي يقصر المدة المتبقية قبل أن تفقد خوارزميات المفتاح العام مثل RSA والتشفير بالمنحنيات الإهليلجية أمانها. والجهات الرقابية وشبكات البطاقات والبنوك المراسلة بدأت تطلب أدلة الاكتشاف وجداول الانتقال الزمنية. كما أن البيئة البنكية تضم مفاتيح مدمجة في وحدات أمن العتاد والبطاقات وأنظمة الرسائل ومنتجات الموردين. والبنك الذي يبدأ الجرد مبكرا يستبدل الخوارزميات بالتوازي مع دورات التحديث المعتادة، أما المتأخر فيواجه استبدالا متسرعا ومكلفا تحت الضغط. وترتكز الدورة على ممارسات البنية التحتية للمفتاح العام PKI ونموذج تهديد الجمع الآن وفك التشفير لاحقا ومبادئ معمارية المرونة التشفيرية.

المستفيدون من الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك

- المعماريون المسؤولون عن التصميم المستهدف لإدارة المفاتيح والشهادات الرقمية ووحدات أمن العتاد.
- مختصو مخاطر التقنية الذين يقيسون التعرض التشفيري ويرفعون نتائجه إلى لجان المخاطر.
- مهندسو منصات المدفوعات المسؤولون عن أمن البطاقات والمدفوعات الفورية والرسائل بين البنوك.
- قادة أمن التطبيقات الذين يحددون المكتبات والبروتوكولات المعتمدة لفرق التطوير.
- محللو مخاطر الأطراف الخارجية الذين يقيمون جاهزية موردي الأنظمة البنكية الأساسية والسحابة.

وتستفيد مجموعات معمارية الأمن أكثر عندما يحضر عدد من أعضائها معا ويتبنون منهجا واحدا للجرد.

قدرات الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك

يحول المشاركون التهديد الكمي إلى قائمة استبدال مرتبة ومجدولة.

- يبني قائمة المكونات التشفيرية لتطبيق بنكي — لتحديد نطاق الاكتشاف.
- يقيم عمر سرية البيانات مقابل الأفق الزمني للتهديد الكمي — لترتيب الأولويات أمام لجان المخاطر.
- يوازن بين تبادل المفاتيح الهجين والتبادل ما بعد الكمي الخالص — لاختيار بروتوكول القنوات.
- يحدد متطلبات المرونة التشفيرية في عقود الموردين — لقرارات المشتريات ومخاطر الأطراف الخارجية.
- يصمم موجات الانتقال حول دورات تحديث وحدات أمن العتاد — لجدولة تعتمدها مجالس المعمارية.
- يعرض التعرض المتبقي واحتياجات التمويل — للراعي التنفيذي ومجلس الإدارة.

مصطلحات الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك الأساسية

- الجمع الآن وفك التشفير لاحقا — هجوم تلتقط فيه البيانات المشفرة اليوم وتخزن حتى يتمكن حاسوب كمي من فك تشفيرها.
- الجرد التشفيري — سجل بكل خوارزمية ومفتاح وشهادة ومكتبة وبروتوكول مستخدم في الأنظمة.
- المرونة التشفيرية — القدرة على تبديل الخوارزميات أو أطوال المفاتيح عبر الإعدادات دون إعادة كتابة التطبيقات.
- تبادل المفاتيح الهجين — مصافحة تجمع خوارزمية تقليدية وأخرى ما بعد كمية بحيث يلزم كسرهما معا.
- التشفير القائم على الشبكات الرياضية — عائلة من خوارزميات المفتاح العام تبنى على مسائل رياضية صعبة يعتقد أنها تقاوم الهجوم الكمي.
- عمر سرية البيانات — المدة التي يجب أن تبقى خلالها المعلومات سرية.

الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك يوما بيوم

اليوم 1: التهديد الكمي والبيئة البنكية

- أساسيات الحوسبة الكمية — الخوارزميات التي تنكسر والتي تصمد
- نموذج تهديد الجمع الآن وفك التشفير لاحقا — تعرض حركة البيانات البنكية المخزنة
- رسم عمر سرية البيانات — آفاق سرية العملاء والتسويات والأرشيف
- خريطة التشفير البنكي — البطاقات والقنوات والرسائل ودفاتر الأستاذ الأساسية
- توقعات الجهات الرقابية والبنوك المراسلة — طلبات الأدلة وجداول الانتقال

اليوم 2: الاكتشاف والجرد التشفيري

- قائمة المكونات التشفيرية — المكتبات والمفاتيح والشهادات وإصدارات البروتوكولات
- المسح الآلي للاكتشاف — فجوات التغطية في الشبكة والشيفرة والأجهزة الطرفية
- مراجعة وحدات أمن العتاد — البرمجيات الثابتة والسعة ودورات الاستبدال
- سجلات دورة حياة الشهادات — الانتهاء وجهات الإصدار وتبعيات السلاسل
- استبيانات التشفير للموردين — جاهزية الأنظمة الأساسية والسحابة ومعالجي المدفوعات

اليوم 3: الخوارزميات ما بعد الكمية والمرونة التشفيرية

- خوارزميات الشبكات الرياضية والقائمة على دوال التجزئة — أطوال المفاتيح والسرعة وعرض النطاق
- تبادل المفاتيح الهجين في القنوات الآمنة — حماية مرحلية للخدمات البنكية الإلكترونية
- التواقيع الرقمية ما بعد الكمية — خيارات تفويض المدفوعات وتوقيع الشيفرة
- أنماط معمارية المرونة التشفيرية — طبقات التجريد وخدمات السياسات المركزية
- اختبار الأداء على الأجهزة محدودة الموارد — البطاقات ونقاط البيع وأجهزة الصراف الآلي

اليوم 4: ترتيب المخاطر وتسلسل الانتقال

- مصفوفة تقييم التعرض الكمي — عمر السرية وإمكانية الوصول والأهمية التشغيلية
- تصميم موجات الانتقال — المكاسب السريعة وتحديث المنصات والأنظمة المتأخرة
- التبعيات بين البنوك وشبكات البطاقات — نوافذ التحويل المنسقة
- تقديرات التكلفة والموارد — حالات الميزانية للجان التقنية
- خطط البديل والتراجع — إخفاقات التشغيل البيني أثناء الانتقال

اليوم 5: ممارسة خارطة طريق الانتقال الآمن كميا

- تطبيق الجرد — قائمة المكونات التشفيرية لمسار دفع للأفراد
- تطبيق اختيار الخوارزميات — تصميم قناة هجينة وتواقيع لتطبيق جوال
- تطبيق التسلسل — خطة موجات متوافقة مع مواعيد تحديث الوحدات
- محاكاة إحاطة مجلس الإدارة — التعرض المتبقي ومبررات التمويل
- خارطة طريق الانتقال الآمن كميا — المالكون والمعالم ومقاييس النجاح

تطبيق الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك بعد الدورة

- إعداد قائمة المكونات التشفيرية لتطبيق مدفوعات حرج وتقييم كل نتيجة على مصفوفة التعرض الكمي.
- إضافة بنود المرونة التشفيرية واستبدال الخوارزميات إلى التجديد القادم لعقد مورد نظام بنكي أساسي أو معالجة بطاقات.

أسئلة حول الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك

ما الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك، ولماذا يهم الآن؟

هو الاستبدال المخطط لخوارزميات المفتاح العام المعرضة للكسر الكمي في الأنظمة البنكية. ويهم الآن لأن البيانات الملتقطة اليوم قد يفك تشفيرها لاحقا، ولأن الاستبدال يستغرق سنوات.

من الأكثر استفادة من الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك؟

يستفيد منه أكثر معماريو الأمن ومختصو مخاطر التقنية. كما يفيد مهندسي المدفوعات وقادة أمن التطبيقات ومحللي مخاطر الموردين، فكل منهم يملك جزءا من البيئة التشفيرية.

كيف يختلف الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك عن دورة عامة في مخاطر الأمن السيبراني؟

يركز على تهديد واحد وفئة أصول واحدة: الخوارزميات والمفاتيح والشهادات داخل الأنظمة البنكية. أما دورة مخاطر الأمن السيبراني العامة فتغطي الضوابط الواسعة بدلا من ذلك.

ماذا تعود به من الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك؟

تعود بخارطة انتقال مبنية على مسار بنكي حقيقي. وتضم قالب جرد ومصفوفة تعرض وخطة موجات بأسماء المالكين.

الانتقال إلى التشفير المقاوم للحوسبة الكمية في البنوك: الطريق إلى الأمام

تحدد خارطة طريق الانتقال الآمن كميا أولا الأنظمة التي تدخل موجة الانتقال الأولى وتلك التي تنتظر التحديث المجدول للمنصات. ويستخدمها المعماريون ولجان المخاطر ومديرو الموردين للاتفاق على المالكين والميزانيات. وبعد تشغيل الموجة الأولى تستحق درجات التعرض وافتراضات عمر السرية مراجعة جديدة مع وضوح أداء الخوارزميات وتقدم العتاد.