



دورة الانتقال إلى التشفير ما بعد الكم: جرد الأصول التشفيرية والمرونة التشفيرية وتطبيق TLS الهجين



دورة الانتقال إلى التشفير ما بعد الكم: جرد الأصول التشفيرية والمرونة التشفيرية وتطبيق TLS الهجين

مقدمة:

الانتقال إلى التشفير ما بعد الكم، من جرد الأصول التشفيرية والمرونة التشفيرية إلى تطبيق بروتوكول TLS الهجين، هو موضوع هذه الدورة ذات أسبوع، الموجهة إلى وحدات معمارية الأمن والبنية التحتية للمفاتيح العامة وهندسة التشفير، وتنتهي بإعداد خطة الانتقال إلى التشفير ما بعد الكم لجهة الحالة. فاليابانات المشفرة التي تعترض اليوم قد تفك حين تظهر حواسيب كمية كبيرة، بينما تعجز جهات كثيرة عن تحديد مواقع مفاتيح RSA والمنحنيات الإهليلجية أو معرفة الموردين القادرين على تقديم البدائل. ويتولى المشاركون إعداد الخوادم أو الشهادات أو أدوات الأمن، ويتدربون في مختبرات بأدوات الاكتشاف واختبار المصافحة وقوالب الجرد. وتقدم كور كونسبت هذه الدورة.

أهداف الدورة:

- تقدير درجة التعرض الكمي لكل خدمة أعمال بالاستناد إلى مدة سرية البيانات وجهد الانتقال ومتباينة Mosca
- اختيار مجموعات معاملات ML-KEM أو ML-DSA أو SLH-DSA المناسبة لكل حاجة حماية وتبرير استخدام النمط الهجين
- بناء قائمة المواد التشفيرية CBOM من نتائج اكتشاف الشبكة والشفرة المصدرية والشهادات
- تصميم واجهات وسياسات خوارزميات مرنة تتيح استبدال الأساسيات التشفيرية دون إعادة كتابة التطبيقات
- اختبار تبادل المفاتيح الهجين في TLS وSSH من حيث تأخير الاستجابة وحجم الرسائل والتوافق مع العملاء القدامى
- إعداد خطة الانتقال إلى التشفير ما بعد الكم بموجات تنفيذ وسجل لجاهزية الموردين ومؤشرات متابعة

الفئة المستهدفة:

- وحدات معمارية الأمن التي تحدد متطلبات التشفير وتبادل المفاتيح والتوقيع للأنظمة الجديدة والقائمة
- وحدات تشغيل البنية التحتية للمفاتيح العامة والشهادات التي تدير هرميات الإصدار ووحدات HSM وتجديد الشهادات
- وحدات هندسة التشفير وأمن التطبيقات التي تراجع المكتبات والشفرة وإعدادات البروتوكولات
- وحدات البنية التحتية والشبكات التي تشغل موازنات الأحمال وبوابات VPN وخوادم SSH وإنهاء اتصالات TLS
- وحدات مخاطر تقنية المعلومات وإدارة موردي التقنية التي تتابع الاعتماديات التشفيرية في المنتجات المشتراة

محاورة الدورة:

اليوم 1: التعرض للتهديد الكمي وخط الأساس للأصول التشفيرية

- أثر خوارزمية Shor على مفاتيح RSA والمنحنيات الإهليلجية
- خوارزمية Grover وتعديل أطوال المفاتيح المتماثلة
- تعرض البيانات طويلة العمر لنمط الجمع الآن والفك لاحقاً
- احتساب متباينة Mosca لمدة سرية البيانات وجهود الانتقال
- خط أساس الاعتماديات التشفيرية الحالية لكل خدمة أعمال

اليوم 2: معايير التشفير ما بعد الكم ومعمارية البروتوكولات الهجينة

- مجموعات معاملات FIPS 203 ML-KEM ومسار تغليف المفاتيح
- أحجام توقيعات FIPS 204 ML-DSA وكلفة التحقق منها
- توقيعات FIPS 205 SLH-DSA المبنية على دوال التجزئة لتوقيع البرامج الثابتة
- تصميم تبادل المفاتيح الهجين بالجمع بين المخططات التقليدية والشبكية
- مرشحا Falcon و HQC في تخطيط اختيار الخوارزميات

اليوم 3: قائمة المواد التشفيرية وهندسة المرونة التشفيرية

- المسح الشبكي السلبي لمجموعات تشفير TLS و SSH
- تحليل الشيفرة المصدرية والملفات التنفيذية لاستدعاءات المكتبات التشفيرية
- سجلات قائمة المواد التشفيرية للخوارزميات والمفاتيح
- طبقات التجريد للمرونة التشفيرية وسياسات الخوارزميات القابلة للتهيئة
- مصفوفة ترتيب أولويات الأنظمة المعرضة للتهديد الكمي حسب المخاطر

اليوم 4: حالات إشكالية في TLS الهجين والبنية التحتية للمفاتيح ووحدات HSM وجاهزية الموردين

- اختبار مصافحة TLS الهجينة لتأخير الاستجابة وحجم الحزم
- تشخيص إخفاقات التوافق مع الأجهزة الوسيطة والعملاء القدامى
- خيارات الشهادات الهجينة والمركبة لهرميات الإصدار
- مسارات تحديث البرامج الثابتة لوحدات HSM لتوليد مفاتيح ما بعد الكم
- استبيان جاهزية الموردين وبنود المرونة التشفيرية في العقود

اليوم 5: عمل مختبري لإعداد خطة الانتقال إلى التشفير ما بعد الكم

- ملف جهة الحالة للمدفوعات والأرشيف والخدمات الإلكترونية
- بناء مستخرج CBOM من مخرجات مسح الاكتشاف لجهة الحالة
- ترتيب موجات الانتقال حسب درجة التعرض والاعتماديات
- سجل جاهزية الموردين وورقة متابعة المعالجة
- استكمال خطة الانتقال إلى التشفير ما بعد الكم ومراجعتها مع الأقران

المهارات التي ستكتسبها:

- تقدير التعرض الكمي
- اختيار خوارزميات ما بعد الكم
- الاكتشاف التشفيري وبناء قائمة CBOM
- تصميم معمارية مرنة تشفيريا
- اختبار المصافحة الهجينة
- تقييم جاهزية وحدات HSM والموردين
- تخطيط موجات الانتقال

لماذا تحضر هذه الدورة:

- تقديم خطة الانتقال إلى التشفير ما بعد الكم مع مستخرج CBOM وموجات التنفيذ إلى مدير أمن المعلومات ومجلس المعمارية
- تحديد الخدمات التي تنتقل أولا إلى تبادل المفاتيح الهجين، والشهادات التي تحتاج خوارزميات توقيع جديدة، وما يمكن تأجيله
- تجنب الاستبدال المتأخر والمتعجل للخوارزميات وإخفاق المصافحة مع العملاء القدامى وشراء وحدات HSM لا تدعم مفاتيح ما بعد الكم
- نقل أساليب مسح الاكتشاف وتحديث قائمة CBOM واستبيانات الجاهزية إلى فرق البنية التحتية والتطبيقات وإدارة الموردين

الخاتمة:

بعد العودة إلى العمل يعرض المشاركون على مدير أمن المعلومات ومجلس المعمارية خطة الانتقال إلى التشفير ما بعد الكم، وهي خطة تربط كل نظام معرض للتهديد الكمي بدرجة تعرض وموجة انتقال وخوارزمية مستهدفة ومالك مسؤول. ويستند المجلس إليها في اعتماد التمويل ومتطلبات الموردين وترتيب انتقال نقاط TLS والشهادات ووحدات HSM والتطبيقات. وبعد الموجة الأولى تعيد الوحدة مسح البيئة وتحديث قائمة CBOM وتسجل نتائج المصافحة والأداء، ثم تعدل الموجات اللاحقة ومواعيد الموردين.

الأسئلة الشائعة:

ما الذي يحتاجه المشاركون قبل دورة الانتقال إلى التشفير ما بعد الكم؟

يحتاج المشاركون إلى خبرة عملية في شهادات TLS أو SSH أو إدارة المفاتيح أو معمارية الأمن، وفهم عملي للتشفير بالمفتاح العام والتشفير المتماثل. ولا تتطلب الدورة رياضيات متقدمة، إذ تشرح المخططات الشبكية والمبنية على التجزئة من خلال معاملاتها وأحجامها وأثرها في النشر.

بم تختلف دورة الانتقال إلى التشفير ما بعد الكم عن دورات الحوسبة الكمية التعريفية أو دورات تشغيل البنية التحتية للمفاتيح العامة؟

هذه الدورة هندسة انتقال عملية: مسح الاكتشاف وبناء قائمة CBOM واختبار المصافحة الهجينة وجاهزية وحدات HSM والموردين وتخطيط الموجات. أما الدورات التعريفية بالحوسبة الكمية فتبقى على مستوى الأعمال وحالات الاستخدام، ودورات البنية التحتية للمفاتيح العامة تعنى بتشغيل جهات التصديق يوميا.

لماذا يبدأ الانتقال إلى التشفير ما بعد الكم بجرد الأصول التشفيرية؟

لأن الجهة لا تستطيع استبدال خوارزميات لا تعرف مواقعها، ويبين الجرد أين توجد مفاتيح RSA والمنحنيات الإهليلجية والبروتوكولات والمكتبات، وأي بيانات تحميها، وكما يجب أن تبقى سرية، فيرتب الانتقال حسب التعرض الفعلي.

ماذا يعود به المشاركون من دورة الانتقال إلى التشفير ما بعد الكم؟

يعود المشاركون بخطة الانتقال إلى التشفير ما بعد الكم لجهة الحالة، ومعها مستخرج CBOM ودرجات التعرض وموجات التنفيذ وسجل جاهزية الموردين ومؤشرات متابعة يمكن تكييفها لأنظمة جهته ومورديها.