GHAYMAH CLOUD

خطة الاستجابة والتعافي من هجوم برامج الفدية (Ransomware)

خطة الطوارئ لأول ٦٠ دقيقة

السيناريو: جميع ملفات Block Storage على منصة Ghaymah Cloud تم تشفيرها ورافقها رسالة فدية.

إعداد: قسم الأمن السيبراني — Ghaymah Cloud
التاريخ: ٢٧ يوليو ٢٠٢٦
مبني على: دليل StopRansomware# المشترك بين CISA وFBI وNSA وMS-ISAC (تحديث مايو ٢٠٢٣)

نظرة عامة على السيناريو

اكتشف فريق العمليات في Ghaymah Cloud أن جميع ملفات التخزين الكتلي (Block Storage) المرتبطة بمجموعة من أحجام الإنتاج قد تم تشفيرها، وظهرت رسالة فدية (Ransom Note) تطالب بدفع مبلغ مالي مقابل مفتاح فك التشفير. هذه الوثيقة تقدّم خطة استجابة متكاملة مبنية على إطار عمل CISA للاستجابة لحوادث الفدية، وتغطي ثلاثة محاور:

- خطة طوارئ تفصيلية لأول ٦٠ دقيقة من اكتشاف الحادث.
- استراتيجية النسخ الاحتياطي والاستعادة في Ghaymah اعتمادًا على مفهومي RPO وRTO وقاعدة 3-2-1 للنسخ الاحتياطي.
- خطة وقاية شاملة لتقليل احتمالية تكرار الهجوم مستقبلًا.

القسم الأول — خطة الطوارئ: أول ٦٠ دقيقة

تلتزم هذه المرحلة بالخطوات الثلاث الأولى من منهجية CISA (الكشف والتحليل، ثم الإبلاغ والإخطار، ثم بدء الاحتواء)، مع إعطاء الأولوية لعزل الأنظمة المتأثرة بشكل منسّق يتجنب تنبيه المهاجمين، والحفاظ على الأدلة الرقمية قبل اتخاذ أي إجراء قد يفقدها.

الجهة المسؤولة	المرحلة والإجراءات المطلوبة	الوقت
قائد الحادث / SOC	**التأكيد والتفعيل** تأكيد وقوع الحادث: رسالة الفدية، امتدادات ملفات مشفّرة على أحجام Block Storage – تفعيل فريق الاستجابة للحوادث (IRT) عبر قناة اتصال خارج النطاق (هاتف/تطبيق منفصل) لتفادي تنبيه المهاجم – تعيين قائد للحادث (Incident Commander) وفتح سجل زمني موثّق للحادث	٠ – ٥ د
فريق العمليات / الأمن	**الاحتواء الفوري** عزل أحجام وأنظمة Block Storage المتأثرة على مستوى الشبكة/المفتاح، وليس فصل كل جهاز على حدة – تعليق مفاتيح API وبيانات اعتماد الحسابات المشبوهة (خاصة حسابات الإدارة) عدم إيقاف تشغيل الخوادم إلا كخيار أخير (للحفاظ على أدلة الذاكرة المتطايرة)	٥ – ١٥ د
فريق الطب الشرعي الرقمي	**حفظ الأدلة والتقييم الأولي** أخذ لقطات (Snapshots) فورية للأحجام المتأثرة قبل أي تعديل، لأغراض التحقيق الجنائي – تحديد نطاق الأثر: عدد الأحجام، الحسابات/العملاء المتأثرين إن كانت بيئة متعددة المستأجرين – تحديد نوع الفدية المحتمل من ملاحظة الفدية وأي مؤشرات اختراق أولية	١٥ – ٣٠ د
الإدارة العليا / قانوني	**الإخطار والتصعيد**	٣٠ – ٤٥ د

الجهة المسؤولة	المرحلة والإجراءات المطلوبة	الوقت
	– إبلاغ الإدارة العليا وفريق الاتصالات المؤسسي بالوضع – إخطار العملاء المتأثرين وفق التزامات SLA إن كانت بياناتهم متأثرة – التواصل الأولي مع CISA/الجهة الوطنية المختصة وجهة التأمين السيبراني إن وجدت	
قائد الحادث	**القرار والانتقال للمرحلة التالية** – تقييم الحاجة لعزل إضافي على مستوى الشبكة بالكامل – بدء تفعيل خطة النسخ الاحتياطي والتعافي (القسم الثاني) لتقييم جاهزية الاستعادة تحديد موعد الاجتماع التالي لفريق الاستجابة (خلال ساعة) وتوثيق كل ما سبق في سجل الحادث	٤٥ – ٦٠ د

ملاحظة مهمة: يُفضّل دائمًا عزل الأنظمة عبر الشبكة (مستوى المفتاح/الـ SDN) بدلًا من فصل كل جهاز على حدة، ويجب استخدام قنوات اتصال خارج النطاق (مكالمات هاتفية) بدلًا من البريد الإلكتروني أو الأنظمة الداخلية التي قد يراقبها المهاجم.

القسم الثاني — استراتيجية Ghaymah للنسخ الاحتياطي والاستعادة

مفهوما RPO وRTO

RPO (Recovery Point Objective) — نقطة الاستعادة المستهدفة: أقصى فترة زمنية من فقدان البيانات يمكن للمؤسسة تحمّلها، وتحدّد التردد المطلوب لأخذ النسخ الاحتياطية. RTO (Recovery Time Objective) — زمن الاستعادة المستهدف: أقصى وقت مقبول لإعادة تشغيل الخدمة بعد وقوع الحادث.

مستوى الخدمة	RPO المستهدف (الحد الأقصى المقبول لفقدان البيانات)	RTO المستهدف (الحد الأقصى المقبول لوقت الاستعادة)
الأنظمة الحرجة (لوحة التحكم / قواعد بيانات الإنتاج)	≤ ١٥ دقيقة	≤ ١ ساعة
أحجام Block Storage الخاصة بالعملاء (Tier 1)	≤ ١ ساعة	≤ ٤ ساعات
الأنظمة الثانوية وبيئات الاختبار	≤ ٢٤ ساعة	≤ ٢٤ ساعة

قاعدة النسخ الاحتياطي 3-2-1 (المعروفة أيضًا بقاعدة 1-2-3)

تعتمد Ghaymah على قاعدة النسخ الاحتياطي المعروفة عالميًا باسم 3-2-1، وتُطبَّق على بيانات العملاء على النحو التالي:

- ٣ نسخ على الأقل من البيانات: النسخة الأصلية الحيّة على Block Storage، بالإضافة إلى نسختين احتياطيتين مستقلتين.
- نسختان على وسيطي تخزين مختلفين: نسخة على شكل لقطات (Snapshots) دورية ضمن منطقة توفر مختلفة داخل نفس مركز البيانات، ونسخة أخرى على منصة/نظام تخزين مستقل (مثل تخزين كائنات Object Storage منفصل).
- نسخة واحدة على الأقل خارج الموقع ومعزولة (Offsite / Immutable / Air-gapped): محفوظة في موقع جغرافي منفصل، بصلاحيات وصول وبيانات اعتماد مستقلة تمامًا عن بيئة الإنتاج، وغير قابلة للتعديل أو الحذف (WORM) خلال فترة الاحتفاظ المحددة.

النقطة الأهم دفاعيًا: النسخة الاحتياطية المعزولة (غير القابلة للتعديل) هي خط الدفاع الأخير ضد الفدية، لأن العديد من هجمات الفدية الحديثة تستهدف النسخ الاحتياطية المتصلة بالشبكة نفسها لتعطيل إمكانية الاستعادة قبل تفعيل التشفير.

متطلبات تشغيلية إضافية

- اختبار استعادة فعلي (Restore Drill) للنسخ الاحتياطية بشكل ربع سنوي على الأقل، للتأكد من صلاحيتها الفعلية.
- تشفير النسخ الاحتياطية أثناء النقل والتخزين، مع إدارة مفاتيح منفصلة عن بيئة الإنتاج.
- فصل صلاحيات إدارة النسخ الاحتياطي تمامًا عن صلاحيات إدارة الإنتاج (لا يملك مسؤول الإنتاج صلاحية حذف النسخ الاحتياطية).
- الاحتفاظ بسجل نسخ متعدد الإصدارات (Versioning) يسمح بالرجوع لنقطة زمنية سابقة على الإصابة.

القسم الثالث — خطة وقاية شاملة لمنع تكرار الهجوم

١. إدارة الهوية والتحكم في الوصول

- تفعيل المصادقة متعددة العوامل (MFA) إلزاميًا لجميع الحسابات الإدارية وواجهات برمجة التطبيقات (API).
- تطبيق مبدأ الصلاحية الأقل (Least Privilege) وفصل المهام الحساسة بين موظفين مختلفين.
- مراجعة دورية لحسابات المسؤولين (Domain/Cloud Admins) وإزالة الحسابات الخاملة أو غير الضرورية.
- تدوير مفاتيح API وكلمات المرور وبيانات الاعتماد بشكل دوري ومجدول.

٢. أمن الشبكة والتقسيم

- تقسيم الشبكة (Network Segmentation) بين بيئة إدارة البنية التحتية وبيئة بيانات العملاء.
- عزل واجهات إدارة Block Storage عن الوصول العام من الإنترنت، والسماح بالوصول فقط عبر VPN أو Bastion Host مُراقب.
- تطبيق قواعد جدار حماية صارمة على حركة المرور الداخلية (East-West) لمنع الحركة الجانبية للمهاجمين.

٣. الكشف والاستجابة المستمرة

- نشر حلول الكشف والاستجابة على نقاط النهاية (EDR/XDR) على جميع الخوادم المضيفة.
- مراقبة مركزية عبر نظام SIEM لرصد الأنماط المشبوهة: استخدام غير معتاد لـ PowerShell، أدوات PsTools، أو أدوات مثل Cobalt Strike.
- تنبيهات آلية فورية عند أي تعديل على صلاحيات الهوية (IAM) الحرجة أو قواعد الشبكة، مع إجراء تلقائي لإبطال التغييرات المشبوهة.

٤. حماية النسخ الاحتياطية بشكل خاص

- الإبقاء على نسخة احتياطية واحدة على الأقل غير قابلة للتعديل (Immutable) ومعزولة منطقيًا عن بيانات اعتماد الإنتاج.
- اختبار استعادة دوري موثّق لضمان جاهزية النسخ الاحتياطية عمليًا وليس نظريًا فقط.

٥. إدارة الثغرات والتصحيحات

- برنامج تصحيحات (Patch Management) منتظم لأنظمة التشغيل والـ Hypervisors وطبقة تخزين البيانات.
- فحوصات دورية للثغرات (Vulnerability Scanning) واختبارات اختراق (Penetration Testing) مجدولة.

٦. الوعي البشري والتدريب

- تدريب الموظفين بشكل دوري على التعرف على رسائل التصيّد الاحتيالي (Phishing) وأساليب الهندسة الاجتماعية.
- إجراء تدريبات محاكاة (Tabletop Exercises) لسيناريوهات هجمات الفدية لاختبار جاهزية فريق الاستجابة.

٧. الحوكمة والتخطيط المستمر

- مراجعة وتحديث خطة الاستجابة للحوادث وخطة التعافي من الكوارث بشكل دوري.
- عقد جلسة "الدروس المستفادة" (Lessons Learned) بعد أي حادث فعلي أو تدريب، وتحديث السياسات بناءً عليها.
- مشاركة مؤشرات الاختراق (IOCs) والدروس المستفادة مع CISA أو الجهات الوطنية المعنية لدعم المجتمع الأوسع للأمن السيبراني.

المصدر المرجعي: CISA / FBI / NSA / MS-ISAC — دليل StopRansomware Guide# (تحديث مايو ٢٠٢٣).