قادة التقنية يتوقعون احتواء الهجمات، لكن قلة منهم تستطيع الوصول سريعاً إلى أجهزة الشبكة عند تعطل الشبكة الرئيسية



يظهر استطلاع لشركة Opengear شمل 514 من مديري التقنية والأمن أن الثقة بعزل الهجمات تفوق كثيراً القدرة على الوصول السريع إلى معدات الشبكة الحيوية عند تعطل الشبكة الرئيسية.

- استطلعت Opengear آراء 514 من مديري التقنية والأمن، ولم يتمكن سوى عدد قليل منهم من الوصول الإداري الآمن فوراً أو شبه فوري عند تعطل الشبكة الرئيسية.
- في المجموعة الأفضل استعداداً، أبدى 93% ثقتهم بعزل الأنظمة المصابة، بينما قال 15% فقط إنهم يستطيعون الوصول الآمن فوراً.
- أفاد نحو ثلاثة من كل أربعة مشاركين بتأخير مشروع للذكاء الاصطناعي أو الحوسبة الطرفية أو البنية الموزعة، أو تقليصه أو إيقافه، بسبب مخاوف المرونة والوصول عن بُعد والتعافي.
- نحو واحد من كل ستة لا يختبر مرونة الشبكة رسمياً، وأقل من واحد من كل أربعة يراعيها منذ

مرحلة التخطيط الأولى.

- يشير الباحثون إلى الإدارة خارج النطاق، أي اتصال منفصل يبقى يعمل عند تعطل الشبكة الرئيسية، كأحد الحلول.

يكشف استطلاع أجرته شركة Opengear على 514 من مديري التقنية ومديري أمن المعلومات عن فجوة بين الثقة والقدرة الفعلية. فمعظم المؤسسات لا تستطيع الحصول سريعاً على وصول إداري آمن إلى بنيتها الشبكية الحيوية عندما تتعطل الشبكة الرئيسية.

لماذا تهم هذه الفجوة

عند هجوم فدية أو تحديث معيب، يحتاج المهندسون إلى الدخول وعزل الجزء المصاب وإعادة الخدمات. وإذا كان المسار الوحيد إلى الأجهزة يمر عبر الشبكة المتعطلة، فإن التعافي ينتظر حضور مهندس إلى الموقع. ويُستشهد بتعطل CrowdStrike في يوليو 2024 مثالًا، إذ تطلب إصلاح ملايين أجهزة Windows تدخلًا يدوياً في الغالب.

والوصول ليس سوى الخطوة الأولى، فعلى الفرق بعدها فرز الحادثة وتحديد موضع العطل واختيار الاستجابة، وكل تأخير في الوصول يؤخر هذه الأعمال.

ما أظهره الاستطلاع

صنّف الباحثون المشاركين في مجموعتين وفق قدرتهم على التعافي عن بُعد وتكرار الاختبار والاعتماد على المهندسين في الموقع. في المجموعة الأفضل استعداداً، أبدى 93% ثقتهم بعزل الأنظمة المصابة مع بقاء الوصول إلى بقية الأنظمة، لكن 15% فقط قالوا إنهم يستطيعون الوصول الإداري الآمن فوراً. والأرقام ذاتية الإفادة، لذا فإن رقم الثقة هو الأقل صلابة.

وقال نحو ثلاثة من كل أربعة مشاركين إنهم أخّروا أو قلّصوا أو أوقفوا خلال العام الماضي مشروعاً واحداً على الأقل للذكاء الاصطناعي أو الحوسبة الطرفية أو البنية الموزعة بسبب مخاوف تتعلق بالمرونة والوصول عن بُعد والتعافي. وفي المجموعتين، لم يكن لدى أقل من الثلث وصول وتعافٍ آمنان عن بُعد قبل تشغيل هذه الأنظمة. ونحو واحد من كل ستة لا يختبر مرونة الشبكة رسمياً، وأقل من واحد من كل أربعة يراعيها منذ مرحلة التخطيط الأولى.

ويقترح الباحثون الإدارة خارج النطاق، وهي اتصال منفصل يظل متاحاً عند تعطل الشبكة الرئيسية.

ما يجب فعله الآن

1. تحقق من قدرة فرقكم على الوصول إلى معدات الشبكة الأساسية وجدران الحماية وأجهزة الفروع عند تعطل الشبكة الرئيسية، ودوّنوا الزمن اللازم لذلك.
2. قيّموا اعتماد الإدارة خارج النطاق للمواقع الحيوية والبعيدة، بحيث يتوافر مسار وصول منفصل أثناء الحوادث.
3. أدرجوا اختباراً بتعطيل الشبكة الرئيسية ضمن تمارين المرونة والتعافي الدورية، ووثّقوا نتائجه.
4. اشترطوا توافر الوصول والتعافي الآمنين عن بُعد قبل تشغيل أي مشروع جديد للذكاء الاصطناعي أو الحوسبة الطرفية أو الفروع.
5. ضمّنوا هذه الاعتمادات في خطط استمرارية الأعمال والاستجابة للحوادث، وعدّوا الثقة ذاتية الإفادة غير

مؤكدة إلى حين اختبارها.