N-able تؤكد أن هجومًا سيبرانيًا وراء تعطل خدمتي Mail Assure وSpamExperts



أفادت N-able بأن اختراق خادم ويب واحد تسبب في تعطل SpamExperts Hosted Mail Assure وCloud لعدة أيام. استمر تصفية البريد، بينما ما زالت البوابة وواجهة API معطلتين والتحقيق جارٍ.

- بدأ التعطل في 16 نوفمبر وشمل جميع المناطق، وعزته N-able في البداية إلى إعدادات المنصة واعتمادية الخدمات.
- في 18 نوفمبر أكدت الشركة وقوع هجوم سيبراني اقتصر على خادم ويب واحد قد يكون المهاجم وصل عبره إلى بيانات اعتماد مخزنة على المنصة.
- لا يوجد لدى الشركة دليل على اختراق بيانات العملاء، والتحقيق مستمر.
- لم يتأثر تدفق البريد ولا التصفية، لكن توقفت خدمات السجلات ومزامنة صناديق البريد والبوابة والحجر.
- أُلغيت رموز API للعملاء وأُبطلت رموز OAuth وأُعيد ضبط كلمات مرور المستخدمين المحليين،

وما زال الوصول إلى البوابة وAPI معطلاً.

أكدت N-able أن هجومًا سيبرانيًا كان وراء تعطل خدمتي Mail Assure وSpamExperts Hosted Cloud، الذي بدأ في 16 نوفمبر واستمر عدة أيام في جميع المناطق. وكانت الشركة قد عزت المشكلة في البداية إلى إعدادات المنصة واعتمادية الخدمات، ثم أكدت الهجوم في 18 نوفمبر.

ما الذي حدث

وفق N-able، اقتصر الحادث على خادم ويب واحد، وربما تمكن طرف غير مصرح له من الوصول إلى بعض بيانات الاعتماد المخزنة على المنصة. لم يتأثر تدفق البريد ولا التصفية، لكن أُوقفت خدمات السجلات ومزامنة صناديق البريد وبوابة الإدارة والحجر. وتقول الشركة إنها لم تجد دليلاً على اختراق بيانات العملاء.

الاحتواء والوضع الحالي

أوقفت N-able الخادم المتأثر، وبدّلت بيانات الاعتماد الداخلية للمنصة، وألغت رموز API الحالية للعملاء، وأبطلت رموز OAuth، وأعادت ضبط كلمات مرور المستخدمين المحليين استباقيًا. تعمل تصفية البريد الوارد والصادر، لكن الوصول إلى البوابة وواجهة API ما زال معطلاً إلى حين استعادته بأمان. والتحقيق مستمر. وتؤكد الشركة أن الحادث لا علاقة له بحادثة N-central الأخيرة.

الأهمية للجهات في المملكة

قد تلاحظ الجهات التي تستخدم هذه الخدمات مباشرة أو عبر مزود خدمات مُدارة توقف التكاملات المعتمدة على رموز API أو OAuth. وبما أن بيانات اعتماد قد تكون تعرضت للكشف، فالحادث يستوجب تسجيله ومتابعته ضمن مخاطر الأطراف الخارجية، رغم عدم رصد اختراق لبيانات العملاء حتى الآن. وتفيد N-able بأنها زودت العملاء بإرشادات محددة بحسب طريقة وصولهم وإعدادهم للخدمتين، وستواصل نشر التحديثات.

ما يجب فعله الآن

1. تحقق مما إذا كانت جهتك أو مزودو الخدمات المُدارة لديها يستخدمون Mail Assure أو SpamExperts Hosted Cloud، وحدد من يديرها.
2. اتبع الإرشادات التي أصدرتها N-able للعملاء وتابع تحديثاتها.
3. حدد التكاملات المعتمدة على رموز API أو OAuth مع هذه الخدمات، وخطط لإعادة إصدارها عند استعادة الوصول.
4. راجع بيانات الاعتماد وكلمات المرور المرتبطة بالخدمة، وبدّل ما يُعاد استخدامه في أنظمة أخرى.
5. سجّل الحادث في سجل مخاطر الأطراف الخارجية واطلب من المزود نتائج التحقيق عند توفرها.
6. راقب بوابة أمن البريد لرصد أي خلل في التسليم أو التصفية ما دامت البوابة والحجر غير متاحين.