

هجوم عن بُعد على وحدات تحكم التبريد من Danfoss يرفع حرارة الثلاجات في متاجر فرنسية



سيطر مهاجمون عن بُعد على وحدات تحكم التبريد من Danfoss في مئات المتاجر الفرنسية ليلة 11 أكتوبر، فارتفعت حرارة الثلاجات والمجمّعات واضطرت المتاجر إلى إتلاف الأغذية.

- تأثرت مئات المتاجر الفرنسية ليلة 11 أكتوبر بحسب عدة سلاسل تجزئة.
- رفع المهاجمون حرارة الثلاجات والمجمّعات، واضطرت المتاجر إلى التخلص من الأغذية.
- كانت نقطة الدخول وحدة التحكم من Danfoss التي تدير كل أنظمة التبريد في المتجر.
- تستطيع شركات الصيانة إدارة هذه الوحدة عن بُعد، وهو ما أتاح مسار الوصول.

ما الذي أُعلن

في ليلة 11 أكتوبر سيطر مهاجمون عن بُعد على معدات التبريد في مئات المتاجر الكبرى في فرنسا. جرى رفع حرارة

الثلاجات والمجمّادات عمدًا، وذكرت عدة سلاسل تجزئة أنها اضطرت إلى التخلص من كميات من الأغذية.

كيف تم الوصول

وصل المهاجمون إلى المعدات عبر وحدة التحكم التي تدير جميع ثلاجات المتجر ومجمّاداته. الجهاز من إنتاج شركة Danfoss الدنماركية، ويمكن لشركات الصيانة إدارته عن بُعد. لم يوضح المصدر الأسلوب المستخدم، لذا يفهم الحادث على أنه إساءة استخدام لإمكانية الصيانة عن بُعد في بيئة تقنية تشغيلية، وليس ثغرة برمجية مؤكدة.

الأهمية للجهات في المملكة

يبيّن الحادث أن وحدة تحكم واحدة في المبنى قد تحوّل اختراقًا سيبرانيًا إلى خسارة مادية: مخزون تالف وتعطل في العمل وهدر. وتعتمد متاجر التجزئة وموزعو الأغذية والمستشفيات والصيدليات ومشغلو سلاسل التبريد في المملكة غالبًا على وحدات مماثلة وعلى مزوّدي صيانة لديهم وصول عن بُعد. والاستجابة المناسبة هادئة وعملية: معرفة مواقع هذه الأجهزة ومن يصل إليها وسرعة اكتشاف أي انحراف في درجات الحرارة.

ما يجب فعله الآن

1. حصر وحدات التحكم في التبريد والمباني، بما فيها التي تديرها شركات صيانة تابعة لجهات خارجية.
2. مراجعة الموردين الذين لديهم وصول عن بُعد، وفرض المصادقة متعددة العوامل وحسابات محددة الهوية وجلسات محدودة المدة.
3. التأكد من عدم إمكانية الوصول إلى هذه الوحدات مباشرة من الإنترنت ومن عزلها عن الشبكة المؤسسية.
4. إعداد مراقبة وتنبيهات مستقلة لدرجات الحرارة لا تعتمد على وحدة التحكم نفسها.
5. تضمين انقطاع سلسلة التبريد في خطط استمرارية الأعمال والاستجابة للحوادث مع إجراء لقرار إتلاف المخزون.