العبث بأنظمة التحكم في التبريد في متاجر أوروبية وسحب أغذية من الرفوف



غيّر مهاجمون عن بُعد إعدادات التحكم في التبريد في متاجر بلجيكا والسويد وإستونيا ودول أوروبية أخرى، فارتفعت حرارة الثلاجات والمجمدات، وأتلفت بعض المتاجر أغذية مبردة ومجمدة أو سحبتها.

- جرى تغيير الإعدادات عن بُعد خلال الليل وصولًا إلى صباح الاثنين 2 نوفمبر.
- شملت الحوادث متاجر في بلجيكا والسويد وإستونيا ودول أوروبية أخرى.
- لم تُبلغ أي سلسلة عن تضرر أكثر من بضع عشرات من المتاجر.
- أتلفت بعض المتاجر أغذية مبردة ومجمدة أو أزالتها من الرفوف.
- ورد في التقرير اسم Danfoss، الشركة الدنماركية المصنعة لأنظمة التحكم في التبريد.

ما الذي حدث

وفق ما نشره موقع The Hacker News، غيّر مهاجمون عن بُعد إعدادات أجهزة التحكم في التبريد داخل متاجر في بلجيكا والسويد وإستونيا ودول أوروبية أخرى. وقعت التغييرات خلال الليل وصولًا إلى صباح الاثنين 2 نوفمبر، فارتفعت حرارة الثلاجات والمجمدات.

لم تُبلغ أي سلسلة عن تضرر أكثر من بضع عشرات من المتاجر، واضطرت بعض المتاجر إلى التخلص من أغذية مبردة ومجمدة أو سحبها من الرفوف. ويذكر التقرير شركة Danfoss الدنماركية المصنعة لأنظمة التحكم في التبريد، بينما لا يتضمن الجزء المتاح من المصدر تفاصيل أسلوب الهجوم أو ردّ الشركة.

أهمية الأمر للجهات المنظمة

تُظهر الحادثة أن العبث بالتقنيات التشغيلية قد يسبب خسائر مادية وتجارية دون سرقة أي بيانات. وغالباً ما تُدار معدات سلسلة التبريد عن بُعد، وقد تقع خارج نطاق المراجعات الأمنية الدورية لتقنية المعلومات.

وقد تواجه المنشآت في المملكة التي تشغّل مرافق للتجزئة أو الغذاء أو الرعاية الصحية أو الأدوية أو الخدمات اللوجستية، أو تموّلها أو تؤمّن عليها، تعرضاً مشابهاً عبر أنظمة المباني والتبريد.

الخطوات المقترحة

ننصح باعتبار الحادثة دافعاً لمراجعة الوصول عن بُعد إلى أنظمة التبريد والمباني، والتأكد من أن مراقبة درجات الحرارة وإجراءات التشغيل اليدوي البديلة تعمل بمعزل عن شبكة التحكم.

ما يجب فعله الآن

1. حصر أجهزة التحكم في التبريد والمباني في المتاجر والمستودعات ومواقع سلسلة التبريد، وتحديد من يستطيع الوصول إليها عن بُعد.
2. تقييد الوصول عن بُعد إلى هذه الأجهزة، واشتراط مصادقة قوية، وإزالة أي تعرض مباشر للإنترنت.
3. اعتماد مراقبة مستقلة لدرجات الحرارة مع تنبيهات لا تعتمد على نظام التحكم نفسه.
4. الاستفسار من موردي التبريد والمرافق عن النشرات الأمنية والتحديثات وممارسات الوصول عن بُعد لأجهزتهم.
5. تجربة إجراء بديل يدوي وإجراء التخلص من المخزون عند تجاوز درجات الحرارة، وإدراجهما في خطط استمرارية الأعمال.