فرنسا تنسب تخريب وحدات التحكم في التبريد في نحو 700 موقع تجزئة إلى إيران



أعلنت فرنسا أن وحدة سيبرانية تابعة للحرس الثوري الإيراني غيّرت إعدادات إذابة الجليد في وحدات تحكم التبريد في نحو 700 موقع تجزئة في 11 أكتوبر، ما تسبب بخسائر غذائية وما لا يقل عن 15 حريقاً.

- تنسب الحكومة الفرنسية الهجوم إلى وحدة سيبرانية تابعة للحرس الثوري الإيراني.
- اخترق المهاجمون وحدات تحكم التبريد في نحو 700 موقع تجزئة ليلة 11 أكتوبر.
- ضبط المهاجمون إعدادات إذابة الجليد على درجات حرارة مرتفعة.
- نتج عن ذلك خسائر في الأغذية وحرائق في 15 حالة على الأقل.

ما الذي حدث

أعلنت الحكومة الفرنسية أن هجوماً سيبرانياً وقع في أكتوبر على وحدات تحكم التبريد في نحو 700 موقع تجزئة نفّذته

وحدة سيبرانية تابعة للحرس الثوري الإيراني. ووفق الخبر، تمكن المهاجمون من الوصول إلى وحدات التحكم ليلة 11 أكتوبر.

وبعد الدخول غيّروا إعدادات إذابة الجليد إلى درجات حرارة مرتفعة. وكانت النتيجة خسائر في الأغذية، وحرائق في 15 حالة على الأقل.

أهمية الخبر

تمثل الحادثة تخريباً يستهدف المعدات المادية عبر طبقة التحكم فيها، لا سرقة بيانات. وتنتشر وحدات تحكم التبريد في قطاعات التجزئة وتوزيع الأغذية والخدمات اللوجستية، وغالباً ما تُدار عن بُعد وتقع خارج نطاق برامج أمن المعلومات التقليدية. وتُظهر النتيجة المعلنة أن مجرد تغيير الإعدادات قد يسبب أضراراً على السلامة وخسائر مالية.

ولا يذكر المقتطف المتاح طريقة الدخول ولا الجهة المصنِّعة لوحدات التحكم ولا مؤشرات فنية، لذلك لا نستنتج شيئاً في هذه النقاط.

الخطوات المقترحة

ينبغي للجهات في المملكة التي تعمل في التجزئة أو الأغذية أو سلاسل التبريد أن تعامل وحدات التحكم في المباني والتبريد كتقنية تشغيلية ضمن سجل المخاطر. ومن الخطوات العملية الأولى مراجعة الحصر والوصول عن بُعد والتنبيه على تغيير الإعدادات، مع التأكد من أن إجراءات الحوادث تشمل الوقائع المؤثرة على السلامة المادية.

ما يجب فعله الآن

1. حصر وحدات التحكم في التبريد والمباني في جميع المواقع، وتحديد من يستطيع الوصول إليها عن بُعد.
2. إزالة التعرض المباشر للإنترنت واشتراط الاتصال عبر VPN مع المصادقة متعددة العوامل للإدارة عن بُعد.
3. تغيير بيانات الدخول الافتراضية وقصر وصول الموردين على جلسات معتمدة ومحددة المدة.
4. التنبيه عند تغيير إعدادات الحرارة وإذابة الجليد، وتفعيل حدود أمان صارمة على المعدات.
5. إضافة سيناريوهات الأثر المادي مثل الحريق وفقدان المخزون إلى خطط الاستجابة للحوادث واستمرارية الأعمال.