

شركة أهولـد ديليز تعطل أنظمتها إثر هجوم سيبراني



أكدت شركة أهولـد ديليز العالمية للبيع بالتجزئة تعرضها لحادث أمن سيبراني أجبرها على تعطيل أنظمتها، مما أثر على وصول الموظفين والمنصات الموجهة للعملاء في عدة أسواق.

- أكدت شركة أهولـد ديليز التي تدير أكثر من 9,400 متجر عالمياً بمبيعات سنوية تبلغ 104 مليار دولار تعرضها لحادث أمن سيبراني في 12 أكتوبر 2026
- عطلت الشركة أنظمتها كإجراء وقائي بينما تظل المتاجر مفتوحة للعملاء
- لا يستطيع موظفو Stop & Shop الوصول إلى جداولهم أو كشف رواتبهم؛ وتعطلت منصات العملاء في متاجر Delhaizeg Gall & Gall Etosg Albert Heijn
- تشير مذكرات داخلية إلى انقطاعات تقنية تؤثر على قدرات تنفيذ الطلبات في مواقع Food Lion
- هذا هو الحادث الكبير الثاني لشركة أهولـد ديليز بعد هجوم فدية في نوفمبر 2024 أثر على 2.2 مليون شخص

نظرة عامة على الحادث

أكدت شركة أهولدا ديليز، إحدى أكبر سلاسل بيع المواد الغذائية بالتجزئة في العالم، في 12 أكتوبر 2026 تعرضها لحادث أمن سيرراني استدعى من الشركة تعطيل أنظمتها كإجراء وقائي. تدير الشركة متعددة الجنسيات أكثر من 9,400 متجر في أوروبا والولايات المتحدة وإندونيسيا، وتوظف ما يقرب من 400,000 شخص، وتخدم حوالي 60 مليون عميل أسبوعياً. وأعلنت الشركة عن مبيعات صافية تجاوزت 104 مليار دولار في عام 2024.

في بيان موجز، أفادت أهولدا ديليز أن فرقها تعمل على تقييم الحادث واحتوائه وأن المتاجر تظل مفتوحة وتخدم العملاء. وأكدت الشركة أن حماية بنيتها التحتية لصالح العملاء والموظفين والشركاء تمثل أولوية قصوى.

التأثير التشغيلي

تسبب الحادث في اضطرابات عبر أسواق متعددة. لا يستطيع موظفو سلسلة Stop & Shop في الولايات المتحدة الوصول إلى جداول عملهم أو كشف رواتبهم. كما تعطلت المنصات الموجهة للعملاء بما في ذلك المواقع الإلكترونية والتطبيقات وأنظمة خدمة العملاء في متاجر Gall & Gall Etosg Albert Heijn في هولندا، وفي مواقع Delhaize في بلجيكا.

وصفت الاتصالات الداخلية في متاجر Food Lion بالولايات المتحدة الوضع بأنه انقطاع تقني، محذرة الموظفين من أن المتاجر قد تكون غير قادرة على التسوق أو تجهيز أو تسليم الطلبات. ورفضت الشركة تقديم تفاصيل حول ما إذا كان الحادث قد أثر على الأنظمة المؤسسية وأنظمة المتاجر معاً، أو النطاق الجغرافي للاضطرابات، أو ما إذا تم تشفير الأجهزة.

حادث سابق

يمثل هذا الحادث الأمني السيرراني الكبير الثاني لشركة أهولدا ديليز في السنوات الأخيرة. ففي نوفمبر 2024، اخترقت مجموعة الفدية INC Ransom أنظمة الشركة في الولايات المتحدة، وسرقت معلومات شخصية ومالية وصحية تخص أكثر من 2.2 مليون شخص.

ما يجب فعله الآن

- مراجعة واختبار خطط استمرارية الأعمال للسيناريوهات التي تتطلب تعطيل الأنظمة التشغيلية الأساسية أثناء حادث نشط
- التحقق من وجود إجراءات موثقة للوصول البديل أو دون اتصال لأنظمة الموارد البشرية الحيوية (الرواتب، الجداول الزمنية) للموظفين
- تقييم اعتماديات المنصات الموجهة للعملاء وإنشاء بروتوكولات اتصال للاضطرابات التي تؤثر على القنوات الرقمية
- تقييم ضوابط التجزئة بين الشبكات المؤسسية وأنظمة نقاط البيع أو أنظمة مستوى المتاجر للحد من الحركة الجانبية
- إجراء تمارين محاكاة لانقطاعات تقنية مطولة تؤثر على تنفيذ الطلبات وعمليات سلسلة التوريد
- مراجعة أدلة الاستجابة للحوادث لضمان مسارات تصعيد واضحة ومعايير قرار لتعطيل الأنظمة مقابل الحفاظ على التوافر