CASE STUDY

Fueling a Healthy Security Diet

To consumers, the specter of hacked grocery stores doesn't elicit the same visceral reaction as the idea of, say, a bank attack. But in reality, because food is a necessity—and because grocers of all sizes have digitized their business practices—a compromised grocery store can create not just inconvenience and lost sales, but also real public health threats and food shortages. The possible scenarios are wide-ranging: In addition to stealing customers' credit card data, hackers can now tamper with a grocer's digitally-controlled pricing displays, causing a pack of Oreos to suddenly register a $450 price tag, or—worse still—take down its entire refrigeration system.

Trustwave®

Client Spotlight

A non-profit grocers trade association located in the Midwest of the United States. The association is focused on providing leadership and guidance to independent grocer operators and their suppliers to help educate and improve their businesses.

The Challenge

In addition to staying abreast of regulatory issues and providing services like money order and coupon processing to 420 independent grocer clients, this grocers association from the Midwest also offers back-up internet to its members to ensure business continuity. But its third-party provider simply wasn't cutting it. The association's president and director of IT were tired of fielding phone calls from irate grocers complaining that the back-up didn't work, and that the vendor took days to call them back or send a technician. Dissatisfaction intensified when the provider installed a subpar firewall system, intended to protect the stores' point-of-sale systems, that prevented the grocers from accessing their own back-end and important websites.

"The previous vendor would make global updates to firewalls, and suddenly our clients would lose access to websites, including business-critical ones like those of wholesale suppliers," says the association's director of IT. "Even worse, when our clients called the vendor for assistance, they'd be told a fix would take three to five days." In some cases, the unreliable internet shut down checkout lanes and led to a retailer's worst nightmare: Lines of customers simply abandoning their carts and leaving the store.

As a result, the association's management needed to find a more responsive and sophisticated vendor to provide back-up broadband, firewall management and endpoint protection, plus guidance in meeting the Payment Card Industry Data Security Standard (PCI DSS) standards. "We needed a tailored supermarket solution that provided a more stable standard of service," the IT director says.

> *"As a business, not going down when your internet goes down is priceless—but we found Trustwave's services to be remarkably cost-effective, too."*
>
> – CEO, major grocers association in the Midwest

The Solution

The IT director and the association's CEO reached out to Trustwave for a custom bundle of managed security services. Trustwave's customer service and offerings—from back-up 4G internet service that can plug into a sophisticated firewall, to a new portal that allows each individual retailer to view its own security activity—blew the association away. In the event of a problem, the association's clients can now speak or text immediately with Trustwave experts.

> *"The bad guys aren't just going after the big players anymore. Trustwave's services are geared toward small businesses that need help."*
>
> — Director of IT, major grocers association in the Midwest

Trustwave also addresses problems the association's members never imagined. When Trustwave set up a new firewall in one retailer, for example, the engineer immediately halted the process because he realized that, thanks to malware, a checkout lane's individual IP address was communicating with unauthorized addresses in Russia. Trustwave also helped educate the association and its members about the threat: In just one fiscal quarter, for example, the site of a grocery chain with about 20 stores received millions of hits from "bad guys" trying to access its system. The new portal now allows retailers to maintain that awareness and better fight back against threats.

Industry Threat

Like retailers, food chains have spent years dealing with data breaches and ensuing litigation. Now radio-frequency identification (RFID) sensors and other IoT sensors are exposing grocers to increasing DDoS attacks on IoT devices, a problem compounded by IoT manufacturers' ongoing slowness in implementing security standards. As a result, research firm Forrester expects cyber-criminals to target these systems with ever-increasing sophistication, as well as to continue ransomware attacks on POS systems.

Trustwave®

©2018 Trustwave Holdings, Inc