CYLANCE

CASE STUDY RESTAURANT

Restaurant Chain Takes on Cybersecurity

The Company

A large U.S.-based restaurant chain offering casual dining experiences at locations across the globe.

The Situation

The company's management team had no idea that attackers had compromised the chain's point of sale (POS) systems for several months until credit and debit card data for thousands of customers was offered for sale on a black-market carding forum. The data was subsequently used to produce counterfeit cards and make fraudulent transactions, resulting in a customer class action lawsuit claiming the company had failed to adequately safeguard personal financial data. In turn, the chain's merchant bank reacted to the breach by imposing roughly $2 million in Payment Card Industry Data Security Standards assessments. The chain also faced the possibility of fines and penalties from government regulators. Overall, the incident revealed fundamental problems with the company's security infrastructure, business processes, and overall risk management posture.

The Process

Cylance consultants were called in immediately after the breach was discovered to perform an Incident Containment and Compromise Assessment. The team identified serious shortcomings in the chain's existing

INDUSTRY

Restaurant Chain

ENVIRONMENT

- Corporate workstations and servers in the United States and roughly 7,200 point of sale terminals at more than 270 restaurants across the globe

CHALLENGES

- Preventing malware and advanced persistent threats from compromising internal computing resources and payment processing systems at restaurants
- Complying with Payment Card Industry Data Security Standards
- Reducing cybersecurity costs and staffing requirements by seamlessly integrating advanced endpoint protection into managed security service provider's product portfolio
- Implementing comprehensive risk management controls by incorporating security policies into core business processes

SOLUTION

- Initially: Retain Cylance® consultants to perform an Incident Containment and Compromise Assessment and then deploy CylancePROTECT® on all servers, workstations, and point of sale devices across the enterprise
- Ongoing: Implement enhanced memory protection by enabling CylancePROTECT's advanced host-based intrusion detection monitoring and blocking capabilities

7,200

ENDPOINTS
PROTECTED

270

LOCATIONS
WORLDWIDE

cybersecurity controls as well as systemic failures with its application whitelisting platform and endpoint defense strategy. After a comprehensive evaluation, the IT organization selected CylancePROTECT as its new endpoint defense solution based on its innovative threat prevention capabilities, low administrative overhead, and ease of implementation.

Shortly thereafter, Cylance ThreatZERO™ consultants moved in to deploy CylancePROTECT in its default, out-of-the box functionality on roughly 7,200 POS devices as well as internal workstations and servers, eliminating all traces of the malware that had caused the breach and mitigating the possibility of further attacks targeting the payment network. With the immediate threat resolved, Cylance began working closely with the incoming Information Security Officer (ISO) to incorporate cybersecurity best practices into a comprehensive risk-management plan.

“Before I joined the firm, cybersecurity was considered an isolated problem to be solved with technology, rather than an approach to business processes that minimizes risk,” the ISO says now. “Among other things, that meant developing a consistent way to measure and prioritize cybersecurity investments that accounts for the true costs of a security incident and its long-term effects on employees, partners, customers, investors, and the value of our brand in the marketplace. CylancePROTECT plays a central role by ensuring that sophisticated malware and advanced persistent threats can no longer disrupt our restaurant operations or discourage us from offering cutting-edge payment methods and other innovations that help us grow the business.”

The Results

Cylance consultants and CylancePROTECT have enabled the company to achieve a solid cybersecurity footing. “We’re contending with a flat revenue growth environment, so it’s essential for us to control our operating costs and minimize our exposure to future attacks,” says the ISO. “We haven’t experienced a single security incident, cloud outage, or user complaint on any system equipped with CylancePROTECT.”

The chain has also been able to seamlessly integrate CylancePROTECT into the product portfolio of its managed security services provider, achieving close to 100% uptime with almost zero false positives. “Over an 18-month period, this has enabled us to reassign 50 of our internal resources to other important risk-management projects.”

Buoyed by these successes, the restaurant chain has scrapped its legacy application whitelisting platform and begun implementing CylancePROTECT’s advanced script and application control features to defend against memory-based attacks. “Cylance has enabled us to put the data breach behind us and focus on what we do best, providing customers with a relaxed and enjoyable dining experience.”

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE