How to prevent security breaches in your retail network

A retailer's multilayer security blueprint

Abstract

In today's era of multi-vector attacks, IT security in retail requires a new approach to security. In addition to protecting the perimeter, smart IT managers have begun to adopt a multilayer security blueprint to detect anomalies and intrusions inside the network.

This paper describes the multi-vector nature common to most high-profile security breaches in retail enterprises. IT directors and security officers will learn about several of the characteristics common to recent breaches, and take away Dell's blueprint for a viable security model to prevent breaches in retail networks.

Introduction

A soft target makes a cybercriminal's day. Why are so many retailers soft targets?

For criminals, retail is where the money is. The possibility of spiriting away and selling thousands or millions of credit card details and chunks of consumer information is powerful incentive.

Modern retailers have had decades to toughen their brick-and-mortar stores against theft, but only a few years to harden their IT networks against data theft. Criminals have turned to the more subtle and lucrative option of sneaking onto the network, exploiting internal gaps in security and quietly copying huge amounts of sensitive data to storage outside of the network.

These breaches include attack vectors as diverse as viruses, spyware, phishing, rogue software and spam. A multilayer strategy is the only realistic defense against them.

All IT managers dread the day that their company is named in the headlines and news sites.

Breaches in the headlines: Damages and casualties in the millions

Despite their best efforts to comply with the Payment Card Industry Data Security Standards (PCI DSS) and other measures for protecting electronic transactions, retailers remain under attack. A shortlist of high-profile breaches in North America alone includes trusted, household names:

- Target — With 40 million payment card numbers and personal information on an additional 70 million people stolen, this ranks as the largest breach in U.S. retail to date.[1]
- Home Depot — Over five months, cyberthieves took 56 million card numbers and 53 million email addresses.[2]
- Michael's — Hackers stole the details from 3 million payment cards over nine months.[3]
- Staples — During the back-to-school season, 1.16 million payment cards were exposed to criminals.[4]

Headlines and news sites are filled with these grisly details, and all IT managers dread the day that their company is named in them.

The impact on retail: An abundance of havoc

While these criminals do not steal tangible property from the retailers, their activities wreak even more havoc than if they had. Consider some of the ramifications of retail breaches:

To retailers

Most acute is the hard spend. Target, for example, spent $61 million in the first few months after the breach in measures like its customer response operation and its promise that consumers would not have to pay any fraudulent charges stemming from the breach. Then, business is disrupted as attention turns from sales to press relations and damage assessment; Target's profit for the holiday quarter was down 46 percent from that of the previous year.[5] To stop the bleeding, retailers like Staples offer to pay the costs of free identity protection – credit monitoring, identity theft insurance, free credit report — to customers who used their payment cards at those stores during specific time periods and might be at risk.[6]

More difficult to quantify is the cost of lingering doubt about future damage from the breach, prompting questions like, "What did they take that we don't know about?" and "What else is lurking on the network that we haven't yet found?"

To suppliers

External business relationships have prompted retailers to extend network connections and credentials up and down the supply chain. Home Depot, Target and Dairy Queen have each indicated that a supplier's stolen network credentials were among the precipitating events of their breaches.[7,8] High-profile attacks are often an early warning to a supplier that its own security has been compromised.

To consumers

How can a retailer recover from the brand damage and loss of consumer confidence? How can it regain the visits

[1]Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg BusinessWeek, March 13, 2014
[2]Gene Marks, "Why The Home Depot Breach Is Worse Than You Think," Forbes, September 22, 2014
[3]Elizabeth Harris, "Michaels Stores Breach Involved 3 Million Customers," New York Times, April 18, 2014
[4]"Staples Provides Update on Data Security Incident," Staples press release, December 19, 2014
[5]Riley, Elgin et al., "Missed Alarms . . ."
[6]Staples press release
[7]Jeremy Kirk, "US chain Home Depot says attackers stole a vendor's credentials to break in," PC World, November 7, 2014
[8]"Data Security Incident," Dairy Queen press release, October 9, 2014

and clicks that suddenly switch to its competitors? Worse yet, how can it head off the legal actions that outraged consumer groups take against it, as several have against Target?[9]

As a result, IT managers with retailers, suppliers and banks are worried not so much about how to comply with PCI DSS and industry standards as how to stay off the front page.

Why this has happened: The advent of multi-vector attacks

How can breaches occur at such huge retailers, with their large budgets, ample resources and vast security infrastructure? Many high-profile attacks have common characteristics:

- Employees for either the retailer or its suppliers are inadequately trained in security awareness. Without the human factor there can be no break-in, and employees who divulge passwords, fall victim to phishing schemes, visit compromising websites or fail to react to security warnings form the weakest link.
- Once inside the network, attackers set about elevating their rights to give themselves greater privileges and access.
- Lax firewall policies between network segments and in the B2B portal soften the target to the attacker who is already inside.
- Criminals infect point-of-sale (POS) and back-office systems with multiple types of RAM-scraper malware. The code captures payment and consumer data and copies it to other compromised systems.
- Reliance on a single layer of defense (usually endpoint anti-malware) or an array of poorly integrated products prevents companies from blocking legitimate threats, such as code that sends captured data outside the network.

The breaches that cause the most damage entail multiple vectors. These include contact and infection at different points, times and levels through the many parts of a retail enterprise's network.

In the past, the combination of a firewall appliance and anti-virus software sufficed as a solid perimeter. However, in an age of methodical, large-scale, multi-vector breaches, tools that simply protect the perimeter and rely on traditional, trust-based security models are inadequate.

Smart IT managers have switched their focus from the no longer achievable goal of keeping every attacker out. Instead, they are adopting tools that detect anomalies and intrusions at multiple points and times inside the network and slow the progress of multi-vector attacks.

How retailers can more effectively approach network security

Every retailer is just a small oversight away from months of damage control, and no single layer of security can take care of everything. Protecting the brand now includes protecting the network, through multiple layers of security and threat intelligence that prevent and respond to attacks:

- Adopting a security policy that trusts nothing (network resources) and nobody (vendors, franchisees, internal personnel), then adding explicit and specific exceptions only
- Separating groups and zones to keep attackers who have gained network access from penetrating further
- Inspecting all traffic at every node on every segment, inbound and outbound, and automatically investigating anomalies
- Enforcing email security to block malware in spam and phishing email attacks
- Unifying multiple technologies into a platform that protects against threats
- Not sacrificing security for performance

This multilayer approach has the potential to thwart multi-vector attacks by impeding their progress through the network, identifying them and eliminating them.

Reliance on a single layer of defense or an array of poorly integrated products prevents companies from blocking legitimate threats.

[9] *Riley, Elgin et al., "Missed Alarms . . ."*

For example, zone-based security would permit data from POS to advance for payment processing but prevent it from going elsewhere.

A blueprint for a multilayer retail defense

Based on data accumulated over years of defending businesses of all sizes, Dell has developed, and built into its line of SonicWALL next-generation firewalls, a blueprint for multilayer defense against attacks on the networks of retail enterprises. The blueprint spans the security layers needed to slow and stop attempted breaches.

Zone-based security in stores

In a typical retail breach, data captured at POS suddenly moves through network segments that should have no common lines of communication (interfaces) with one another. That is one result of a firewall policy too complicated and inscrutable even for its administrators.

Zone-based security allows administrators to separate and protect network resources from unapproved access or attack. A network security zone is a logical grouping of interfaces with intuitive names mapped to security rules that permit or prevent the movement of data. With zone-based security, administrators can more easily standardize by grouping similar interfaces and applying the same policies to them, then adding back only necessary exceptions.

With resources like customer-facing machines, inventory servers and back-office data warehouses organized in separate zones, retailers can more easily ensure that only authorized, trusted users have access to them. In the Dell blueprint, zone-based security would, for example, permit data from POS to advance for payment processing but prevent it from going elsewhere.

Adaptive security policy

As new network threats emerge, administrators need to update the intrusion prevention signatures that firewalls use to recognize them. Since many firewalls suffer a performance penalty as more and more signatures are added, administrators tend to manually vet the updates first, and then install only the most critical ones. That cumbersome process leads to gaps between the time they receive the update, the time they get around to reviewing it and the time they can apply it.

Dell's blueprint includes an adaptive security policy in which administrators set their own high-medium-low policy for intrusion protection. The firewall automatically downloads updates, identifies new signatures and then, based on the organization's high-medium-low policy for protection against threats, immediately applies the signatures in prevention mode or detection mode only.

This adaptive response to emerging threats means the retailers can eliminate the need for manual review and avoid the risk gap that results from the delay in applying protection.

Unified, cross-threat intelligence

The most effective measure for protecting against multi-vector attacks is to pool intelligence about different threat categories and update firewalls with unified signatures. The Dell blueprint centralizes this cross-threat intelligence in cloud-based gateway anti-virus (GAV).

GAV collects samples of data — spam and botnet feeds, phishing and content filtering submissions, honeypots, etc. — and analyzes them in the cloud. If it identifies a potential threat, GAV creates a signature and makes it available for automatic download to next-generation firewalls (NGFWs) worldwide. Pooling the intelligence on content filtering, anti-virus, Intrusion prevention systems (IPS) and spam detection offer shorter response time and greater computing power than any single organization could achieve on its own.

The biggest benefit for retailers is the concurrent protection against a huge array of attack vectors, exploits, vulnerabilities and malware. With the

heavy lifting of threat assessment offloaded to the cloud, administrators can enable full protection on NGFWs without sacrificing performance.

Multi-vector threat identification

To block threats and intrusions, the firewall must first recognize them. The Dell blueprint includes technologies at several layers:

- Byte-by-byte packet inspection — A low-latency, Reassembly-Free Deep Packet Inspection (RFDPI) engine inspects every byte of every packet to block threats inside of files, attachments and compressed archives and transform them as needed for normalized traffic analysis. Scanning all traffic, regardless of port or protocol, is the best way to protect the network from internal and external attacks.
- Encrypted traffic inspection — Cybercriminals increasingly use the Secure Sockets Layer (SSL) protocol to encrypt their attacks and evade detection. By activating the SSL decryption and inspection functionality of the RFDPI engine, retailers can inspect SSL-encrypted traffic — including HTTPS and FTPS — regardless of the port being used.
- Automated threat investigation and prevention — Malware lives and grows in families, so threat prevention includes anticipating how they will evolve. The RFDPI engine uses specific code fragments common to malware families to identify malicious code in new mutations.
- Email scanning — Email security blocks malware trying to enter in spam and phishing email attacks. It checks the IP address reputation of senders of inbound email and verifies message content, structure, links, images and attachments for deeper security. Retail workforces run the gamut of technical sophistication, and email security helps prevent unsuspecting users from inadvertently launching malware.
- IPS with anti-evasion capabilities — Cybercriminals often try to circumvent IPS by disguising their attacks as benign data. To combat this, the firewall must normalize data and decode any threats before handing the data off to the IPS. Installing IPS with anti-evasion capabilities at the store level mitigates the risk of vulnerabilities in applications, clients and servers.

With this blueprint, IT administrators in retail enterprises can defend their networks against the malware, spyware, viruses, intrusions, rogue applications, spam and phishing attacks with a multilayer strategy.

Conclusion

By nature, retail networks contain many moving parts: the corporate network, regions, stores, point-of-sale (POS) machines, vendors, suppliers, customers, web and mobile. While keeping the perimeter hardened, IT also needs to focus on detecting anomalies and intrusions inside the network.

Attackers succeed not with a single entry or exploit, but through multiple entries and at multiple levels through interconnected systems. In an era of multi-vector attacks and advanced persistent threats, Dell's multilayer blueprint for defeating security breaches — implemented across its line of SonicWALL next-generation firewalls — is designed help retail win by slowing the progress of an attack enough to identify it, then stop it before it wreaks havoc.

Email security helps prevent unsuspecting users from inadvertently launching malware.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.