April 2020

FEATURE

Under Siege

The convenience retailing industry is a prime target for data attacks. What are you doing to protect your network? And how will you respond if a breach occurs?

BY JERRY SOVERINSKY

Print
Share
0 Comments (/issues/april-2020/under-siege)

Convenience stores are in the news and for unenviable reasons. A recent spate of data breaches has led to the theft of credit and debit card information from millions of customers, while infiltrating critical operating systems for convenience retailers.

“Attacks Targeting Point-of-Sale at Fuel Dispenser Merchants,” warned a November 2019 Visa Security Alert, notifying merchants of increased efforts by cybercriminals to target fuel dispenser merchants. But these were not pump-based attacks. Rather, they struck at the nerve center of these merchants’ data infrastructure: POS systems. “It is important to note that [the attacks] differ significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant’s internal network,” Visa continued.

These POS attacks are an evolving threat that requires an all-hands-on-deck approach from fuel marketers to minimize vulnerabilities.

Indeed, earlier this year, York, Pa.-based Rutter’s announced that it had uncovered a data breach of customer information that may have begun as far back as August 2018. An “unauthorized actor may have accessed payment card data from cards used on point-of-sale (POS) devices at some fuel pumps and inside some of our convenience stores through malware installed on the payment processing systems,” Rutter’s said in a press release.

This came just two months after Wawa, Pa.-based Wawa announced that it discovered a data breach—up to nine months after “malware began running on in-store payment processing systems at potentially all Wawa locations,” the company said in a press release. The result? The compromise of more than 30 million payment cards, according to security news site *Krebs on Security*.

Popular Articles

FEATURE

U.S. Convenience Store Count Stands at 152,720 Stores (/issues/february-2020/us-convenience-store-count-stands-152720-stores)

The industry is faring better than other retail channels, but the number of small companies is declining.

FEATURE

The 2020 NACS Consumer Fuels Survey (/issues/march-2020/2020-nacs-consumer-fuels-survey)

Four insights shed light on how fuel retailers can further delight customers in 2020.

FEATURE

Know Thyself, Know Thy Customer (/issues/february-2020/know-thyself-know-thy-customer-0)

Five ways to find success in this new era of convenience retailing.

Why are petroleum retailers being targeted?

According to Mark Carl, CEO of ControlScan, cybercriminals are intensifying their efforts on the petroleum industry because they have discovered vulnerabilities. "As these attacks continue to deliver huge successes for the attackers, they will continue to target both upstream and downstream petroleum resources to look for additional value," he said.

The effort is not new, according to Carl. "The threats began in earnest with the breach of a vendor back in early 2016, which likely produced a significant amount of technical knowledge that the attackers could use to perpetrate attacks. Given the success that they've seen, they've also gained significant knowledge of petroleum systems along the way."

PREVENTION, NOT DETECTION

Despite these ominous findings, a compromise is not inevitable, cybersecurity professionals insist. Instead, retailers should proactively reassess their IT infrastructure and antivirus protection to minimize the impact from cyberattacks.

For those with sufficient resources, it's not a matter of simply boosting security personnel, for whom demand far outstrips supply. By 2022, the global shortage of IT workers will reach 1.8 million, according to the Center for Cyber Safety and Education.

And even for those companies that maintain an internal IT department, an increased number of false security alerts are straining their availability to deal with more critical cybersecurity pursuits, while evolving complexities make it difficult for them to respond effectively. "While many IT staff are good at defensive security, they haven't really worked with systems that are under attack and therefore don't necessarily know what they are looking for," Carl said. "Firewalls will not completely keep attackers out of environments."

The key is pursuing a *proactive* posture, one predicated on *prevention*, Carl said, rather than a reactive one, which operates on *detection*. The latter is characterized by signature-based antivirus software that spots known threats. (You know these solutions all too well. They bloat system resources and slow boot up time as they continuously download updates in their endless game of cat-and-mouse against cybercriminals.)

But systems that rely on such *reactive* protection are vulnerable to new strains. The network systems for large enterprises include hundreds/thousands of endpoints, each of which creates an additional vulnerability for the company.

It wasn't always this way, of course. Historically, networks consisted of a primary, standalone hub. But as personal computers proliferated during the past 25 years, their ability to link to a central hub has created a complex web of touchpoints—endpoints, actually—each creating an entry point for a would-be cyberattack. And as cyberattacks grow increasingly more deceptive, human error has led to an increased number of breaches.

> "
> Firewalls will not completely keep attackers out of environments.

"Phishing is one common threat vector," said Linda Toth, director of standards for Conexxus. "People are composing emails that look like they're originating from within the organization, capturing information from LinkedIn and other social media outlets that makes it look authentic. And all it takes is just one employee to trigger a breach."

With legacy antivirus software, these endpoints are unable to prevent more complex attacks from executing, necessitating a more powerful

Popular Categories

- NACS News »
- Feature »
- Retailer Focus »
- Trends and Research »
- Legislative »
- Inside Washington »
- Foodservice »

solution. “Advanced threat detection and response capabilities must be employed to fully protect the environments,” Carl said. Solutions such as Managed Detection and Response (MDR) from third-party vendors “deploy advanced endpoint security to all assets, active email monitoring and logging all activity to a centralized SIEM [Security and Information and Event Management]. But the most important part remains the human factor. Only staff that understand specific tactics and methods of a sophisticated adversary are likely to detect them, as is demonstrated with recent successful breaches that went undetected by IT staff for months.”

Carl said that even with advanced detection solutions in place, a retailer should focus on making sure that systems are closely monitored: “The right team will proactively monitor the entire environment 24/7/365 to know when a compromise has occurred, will have tools to quarantine individual systems from the environment and will take immediate action to contain and limit the scope of the attack.”

Jim Shepard, director of data protection and reg compliance for Phillips 66, agrees, “As a merchant, your core business activity is selling products, and you may not have the staff to successfully manage the security of your operating environment. That’s when it’s necessary to get help with a managed security provider.”

The stakes are significant, and perfection is the only acceptable outcome. “We have to get it right 100% of the time. The crook has to get it right just once,” Shepard said.

A TEAM EFFORT

There is of course no way to prevent cybercriminals from launching attacks. But until legacy antivirus applications have been replaced with advanced threat detection and response capabilities, human error will continue to create system vulnerabilities, a weakness that cybercriminals rely on to inflict damage. And when that happens, all efforts must turn toward remediation to prevent further widespread damage from lateral attacks in the environment.

The first step in the process is activating an incident response plan, a prepared course of action for disasters (see “The First Line of Defense” in the October 2019 issue of *NACS Magazine*). Ideally, this would be a plan that you continually update, incorporating best practices from previous events. And all plans begin with a first point of contact. “Reach out to your first responders; they are responsible for activating your plan,” Shepard said.

Even if you manage a robust, internal IT staff, remediation must tap third-party professionals who specialize in addressing breach scenarios. “Work with an incident response team. If you don’t have one, bring in somebody who understands the specific tactics, tools and methods of sophisticated attack groups,” Carl advised.

Next comes containment mode. “That means disconnecting from your network. Not powering off your systems, because that could be problematic, but going offline to reduce your exposure,” Shepard said.

Carl and his team deploy endpoint security, “identifying where the attacker is and extracting them from the environment, including cloud-based systems like Office365 that may be commonly overlooked.”

Next is the post-recovery phase. “Figure out what that entails for your organization,” Shepard said. “You’ll want to preserve your logs and other evidence that could explain what happened. This will go a long way toward helping you remediate and prevent future occurrences.”

Backups are critical for restoring operations, and Carl said operators should adopt a robust backup protocol. “It won’t stop a ransomware attack, but it will reduce its impact, and you might not have to pay to decrypt critical data,” he said.

Finally, building on your learnings from the remediation process, revise your existing plan, ensuring that any subsequent efforts gain efficiency and effectiveness.

A NEW PERSPECTIVE

Protecting your data and your customers' information is an ongoing challenge. Successfully addressing this escalating industry concern depends on a smarter approach, one that employs proactive prevention, rather than detection. The success of your company—and the safeguarding of your customers' sensitive data—depend on it.

Related: Feature (/category/Feature), Technology (/category/Technology)

ABOUT JERRY SOVERINSKY

Jerry Soverinsky is a Chicago-based freelance writer and *NACS Magazine* contributing writer.

Articles You May Be Interested In

(/issues/november-2016/its-playtime)

November 2016

FEATURE

It's Playtime (/issues/november-2016/its-playtime)

Before the NACS Show, industry leaders came together to give back to an Atlanta community.

BY JEFF LENARD

(/issues/february-2017/balanced-diet)

February 2017

FEATURE

A Balanced Diet (/issues/february-2017/balanced-diet)

Surveyed consumers insist they want healthy foods, but they also crave waffle breakfast sandwiches and oversized, spicy hot dogs.

BY PAT PAPE

(/issues/june-2017/how-did-we-get-here)

June 2017

FEATURE

How Did We Get Here? (/issues/june-2017/how-did-we-get-here)

The past three years may have given the industry a false sense of security, or a taste of the new normal.

BY CHRIS BLASINSKY

NACS

NACS serves the convenience and fuel retailing industry by providing industry knowledge, connections and advocacy to ensure the competitive viability of its members' businesses.

About NACS Magazine

Subscribe (https://www.convenience.org/Media/NACS-Magazine/Subscribe/SubscriptionForm)

Advertise (https://www.convenience.org/advertise)

Editorial Guidelines & Submissions (/content/editorial-guidelines-submissions)

Permissions & Reprints (/content/permissions-reprints)

Contact NACS Media Group (/content/contact-nacs-media-group)

(http://(https://

● Back to Top

HELP (HTTP://WWW.CONVENIENCE.ORG/HELP)

Privacy Policy (http://www.nacsonline.com/Pages/PrivacyPolicy.aspx) | Terms of Use (http://www.nacsonline.com/Pages/TermsofUse.aspx)