Safety & Security

Web Article

http://www.cio.com/article/3187693/cio-role/it-leaders-share-how-they-quell-cybersecurity-attacks.html

IT leaders share how they quell cybersecurity attacks

Three IT executives discuss their greatest cybersecurity fears and some of their favorite tools they use to quell them.

By Clint Boulton

Senior Writer, CIO | APR 4, 2017 12:53 PM PT

Ask CIOs and CISOs what cybersecurity fears keep them up at night and you'll hear a range of responses -- from social engineering hacks such as phishing, as well as malware that enables perpetrators to hijack users' websites -- the dreaded ransomware -- and denial-of-service attacks. Depending on their business you might hear them say "all of the above."

These threats are driving increased spending on cybersecurity tools intended to protect corporate data from nation-state actors, lone wolf attackers and other malcontents who are seeking access to corporate data. IT leaders know that it takes only one well-placed exploit to infiltrate a corporate network, but they also

acknowledge that the best approach is to shrink their attack surface and be ready to respond to an incident in the event of an attack.

Being ready requires significant investments, both in talent and technologies. IDC says corporations will spend $101.6 billion on cybersecurity software, services and hardware, a 38 percent increase from the $73.7 billion it expected companies to spend in 2016. To help you develop your strategy, two chief security officers and one CIO share their experiences with their favorite security tools.

Anthony Belfiore, chief security officer, Aon


Aon

Anthony Belfiore, chief security officer, Aon

As one of the largest insurance and reinsurance businesses, Aon is a big target for prospective hackers. Aon CSO Anthony Belfiore says he is most concerned about distributed denial-of-service (DDOS) attacks. In an attempt to integrate businesses more quickly, most enterprises have largely consolidated their computing systems. They tend to run corporate software, including VOIP, chat and email on one central system. This isn't just an on-premises scenario as many companies are also centralizing their computing capabilities to cloud vendors. If a cloud vendor goes down ---as Amazon Web Services did last month -- the companies using it feel it immediately.

"God forbid someone drop a cyber nuke or DDOS from malware -- they can take down a whole environment," Belfiore says. "If we're down it doesn't really matter how secure we are -- we have a problem."

Even so, security chiefs have to protect their data. Aon is a heavy consumer ofTanium, whose endpoint security software monitors IT operations and detects malware, among other threats. Belfiore says the software covers anything from kernel operations of a server processor to the application portfolio that is operating on it.

"Think of it as an agent, almost like a spy to every asset on environment to give you real-time status on any attribute related to operations and security," says Belfiore who joined Tanium's board of directors this year. "It's almost like a central management system on steroids for security and operations."

This isn’t Belfiore’s first brush with Tanium, which Target implemented in the wake of its 2013 breach. Prior to joining Aon, Belfiore used Tanium to track software licenses at First Data and to wipe out shadow IT at JP Morgan Chase.

Mike Sherwood, CIO, City of Las Vegas


City of Las Vegas

Mike Sherwood, CIO, City of Las Vegas.
Managing IT for municipal organizations presents its own sets of challenges. Employees need to access various websites to find information that helps them complete their work. For example, law enforcement officials will often conduct searches that lead to Dark Web sites, a Wild West where criminals lurk and set traps with known and unknown malware. Such threats, along with phishing schemes, ransomware and a legion of dangerous payloads keep Las Vegas CIO Mike Sherwood on his toes. As Sherwood puts it, “I can’t always be at everyone’s desk to make sure they are clicking on the right links.”

[The CSO guide to top security conferences]

Sherwood has one ace in the hole in the form of software from Darktrace, which he began using in his former role as the CIO of the City of Irvine, Calif. The application monitors inbound and outbound traffic on his computer network, a crucial task he couldn’t achieve with his one full-time security engineer and four contract workers.

Darktrace uses artificial intelligence and machine learning capabilities to learn more from vulnerabilities as they are discovered. His staff programmed Darktrace to watch for certain threats, alert administrators and make multiple recommendations for remediation. “It's as good as any human engineer as far as learning and adapting,” Sherwood says.

Darktrace worked well enough at Irvine that it was among the first tools Sherwood purchased when he took the CIO job in Las Vegas in 2016. He says the city’s footprint is much larger because of Las Vegas “smart city” initiative to wire downtown with sensors that monitor traffic flow and other activities. “It's coming with me no matter where I go,” Sherwood says, of Darktrace.

Vince Skinner, vice president of information security, D.A. Davidson

 D.A. Davidson

Vince Skinner, vice president of information security, D.A. Davidson,
As cyber attacks go, D.A. Davidson may have already experienced its worst fear. In 2007, Latvian hackersbreached the financial services firm using a SQL injection attack to access the company's database, an infiltration that cost the company $375,000 in fines. In 2008, the firm hired Vince Skinner to build out its cybersecurity program.

Skinner says that while he was given a lot of latitude and resources to shore up D.A. Davidson's digital defenses, an open checkbook doesn't guarantee success. "Even with money you need people, processes and technology" to adequately protect a company, Skinner says.

Although it's been nearly a decade since the Latvian breach, Skinner says that cyber attacks are remarkably similar, albeit more sophisticated, with PowerShell and macros attacks on every cyber professional's radar. Compromised Gmail accounts beget wire fraud and ransomware has proliferated. Skinner protects his company with frequent penetration testing, poking his network and applications for vulnerabilities.

Skinner relies on Carbon Black, which he uses for application whitelisting and behavioral analytics that help detect anomalies. The software tells him if an executable code is known, unknown or known but can be exploited.

"Carbon Black's defense won out due to its protective capabilities and feedback loop to provide super detail behind the [attack] chain," Skinner says.