West Texas Cyber Security Consortium

Incident Response Now Shaping Security Operations

How an organization reacts to hackers infiltrating its network is becoming the key to damage control for data -- and the corporate image.

First in an occasional series on a new sense of urgency for incident response after a cyber attack

The backdoor malware discovered on a server at a US manufacturing company was spotted and cleaned up within 24 hours of its implantation, and by all accounts that particular cyber espionage attack had been thwarted. But the next day, two new backdoors were spotted on two other servers, and the company realized its incident response operation had not been so successful after all.

"We knew the Trojan on that [first] system, but we missed out on a couple of other machines. As soon as we cleaned up the one machine, there they were the next day," says the IR security team member at the manufacturing firm, who spoke on the condition that his company not be named. "They had moved laterally and installed two completely different backdoors, so IOCs [indicators of compromise]/signatures were useless.

"We made a decision too quickly... you have to be quick and thorough. This was a learning lesson for us."

Now that organizations and the security industry for the most part have accepted the ugly truth that breaches are inevitable and the bad guys are going to find a way to get inside, the new focus is on how you respond to an attack or attack attempt and minimize the damage. Mega-retailer Target's missteps in its post-breach operation have driven home a new sense of urgency in establishing a solid incident response operation that is as much about protecting data as it is about protecting the corporate image.

Incident response (IR) is becoming part and parcel of a security strategy, experts say. More than 60 percent of organizations say they have IR plans in place, according to a recent report by Arbor Networks and The Economist Intelligence Unit, which surveyed some 360 C-level or board-level business executives around the globe on their incident response postures. According to the data, around two-thirds of the organizations say a successful and smooth incident response operation in the face of a breach could ultimately enhance their reputation. "The saving-face piece is big," says Dan Holden, director of Arbor's ASERT.

"Security is now about resilience -- it's not about defense," says renowned security expert Bruce Schneier, who is CTO for Co3 Systems, an IR vendor. The key lesson learned in the aftermath of most cyber attack responses is simple, Schneier says: "We forgot something. It was a crisis and we forgot something, or we didn't follow up thoroughly enough."

Sean Mason, global IR leader at CSC and former director of incident response at GE, says IR -- especially coupled with detailed postmortems on an attack -- is becoming a key element to security strategy. "The IR and cyber intelligence shift is already happening at some companies. It's becoming the cornerstone of a security strategy," Mason says. "Even if you're not a mature [security] organization, you need to look at dissecting these incidents."

As the manufacturing company hit by cyberspies found out, attackers usually aren't just in one of your boxes. "If I see attackers in the network, I work as quickly as possible," CSC's Mason says. "I want to look for all indications of lateral movement so I can contain them. The last thing you want is [their having] a larger and more robust foothold in your network."

Target's story has become a cautionary tale of what can go wrong after a breach, by virtue of the size and scope of its breach. But the retailer's security team apparently dismissing its FireEye security platform alerts of suspicious activity on

the network is what stands out most here: If the team had followed up on the alerts, they could have caught the attackers red-handed before they siphoned off some 40 million payment card account numbers, experts say. The popular retailer apparently had the security and IR team, the million-dollar tools, and the expertise that would be the envy of many smaller organizations.

Target, for its part, is currently investigating why the security events logged from November 30 and December 2, during the breach, weren't acted upon. "Like any large company, each week at Target there are a vast number of technical events that take place and are logged," a Target spokesperson said in response to inquiries for this article. "Through our investigation, we learned that after these criminals entered our network, a small amount of their activity was logged and surfaced to our team. That activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow-up. With the benefit of hindsight, we are investigating whether, if different judgments had been made, the outcome may have been different."

Getting a handle on every potential porthole into an organization is a tall order. Not only is there the constant threat of a user falling for a phishing email or getting scooped up in a watering hole attack, but many organizations either don't log events in their networks, or if they do, they don't have a way to correlate or make sense of them. And even if they get alerts, they may write them off as false alarms (think Target).

"We don't want to spend our time looking at every single malformed packet. That's what we're all struggling to do. We want to aggregate a series of events that are meaningful," says the director of security at a biotechnology firm who requested anonymity.

But more often than not, organizations don't have a full picture of all of the potential entry points into their networks. Aside from the glaring problem with third-party suppliers like Target's HVAC contractor -- patient zero in that attack -- there also are blind spots in internal networks. "I've seen this numerous times, where in a Fortune 500 company, there may be some segments that are external-facing where web servers may live, and for some reason, those organizations don't instrument those networks as well as they do their internal network," says Joshua Goldfarb, chief security officer at nPulse. "I often saw networks or segments of networks that had been intruded but were not properly

monitored, so when it came time to do forensics, the data wasn't there... There was no evidence trail, so it's difficult to piece together what happened."

A disjointed and disorganized incident response can permit the attack to spread, as the good guys scramble to get on top of the source or sources of the problem, while the bad guys go to town pilfering data.

Goldfarb says one common mistake is for upper-level management to try to control the process without full knowledge of the incident. "Management and executives have the best of intentions. They want to do what's right for the company, but they may not have any technical knowledge at all," he says. "If you're a CIO or a CEO, you may have a lot of conjecture about what could have happened, but the truth is, the people who have hands on the keyboards know the fastest way to get that information. [Executives' over-interference] ends up pulling the investigation off-task."

The rash of data breaches and cyber espionage attacks over the past year has put the squeeze on CSOs and companies worried about bad PR in the wake of an attack going public. That includes how they inform their customers, the press, and shareholders. "This is now forcing organizations to take a more militant approach to IR," says Joe Loomis, co-founder and CEO of IR technology vendor CyberSponse. "If you accept the fact that failure is going to happen, that's a scary thought. Imagine if you're a CSO [thinking] 'If I'm compromised, my career is over.' IR is really the only way to somewhat save a company's reputation, and how they respond to certain types of threats."

A year ago, incident response wasn't even a profit-and-loss item at most corporations, notes Loomis. "Now," he says, "the lowest-paid security guy doesn't patch a server, and he causes billions of dollars in losses."

Schneier, meanwhile, sums it up this way: The worst time to ask what the IR/disaster plan says is after discovering you've been hacked.

Kelly Jackson Higgins is Senior Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise Magazine, ... View Full Bio

http://www.darkreading.com/informationweek-home/incident-response-now-shaping-security-operations/d/d-id/1141584

http://www.csoonline.com/article/2150444/todays-mobile-malware-vastly-different-from-a-decade-ago-fortinet.html