West Texas Cyber Security Consortium

What Not To Do In a Cyberattack

How to keep calm and avoid common mistakes in an incident response operation.

[This is the third installment in a series on the evolution of incident response amid today's threat landscape. Read Part 1, Incident Response Now Shaping Security Operations, here and Part 2, Operation Exfiltration, here].

Detecting an attack can be difficult enough, but the chances of a quick cleanup and lockdown in the aftermath of an incident dramatically diminish if there's no official incident response plan and no incident response (IR) point person or team in place.

"The last thing you want are admins or other people logging in and trying to triage it themselves. Then they start ruining all the data and evidence," says a security and incident response team member at a large US manufacturer.

You need a designated incident response team -- either in-house or for hire -- in charge of stepping in when an attack gets detected. "A classic misstep I've seen at other companies is that there was nobody on point for IR. They had not thought it through ahead of time," says Sean Mason, global IR leader at CSC and former director of incident response at GE.

With the new reality that everyone is getting *pwned* even if they don't know it, the focus is now shifting to responding to the inevitable security incident or data breach. Roughly 60 percent of organizations surveyed recently by the Economist Intelligence Unit and Arbor Networks say they have IR plans in place, but another study by the Ponemon Group shows incident response represents less than 10% of the security budget. IR budgets have remained flat in the past 24 months, too, according to the Ponemon report.

"Most [respondents] thought they had an IR plan," says Tom Cross, director of security research at Lancope, which commissioned the Ponemon study. "But there were gaps in the level of preparedness. Everyone thinks they are ready."

Bottom line: Most organizations, even those with IR teams, make mistakes in the aftermath of an attack. Target, with its well-equipped security team, dismissed an alert that could have halted the hemorrhage of tens of millions of payment card

accounts and other customer information. Other organizations get tunnel vision in their investigation and inadvertently overlook the core of the problem.

Don't just remove malware from an infected machine and consider the attack over.

Malware is just a symptom of the attack. The biggest mistake organizations make when they start to respond to an attack is to shut down the infected machine in hopes of shaking the bad guys and preventing any further spread of malware. But that typically backfires, resulting in the loss of valuable logs or in-memory forensics -- and, in many cases, a deeper foothold for the attackers.

In targeted attacks like cyberspy operations or targeted payment card heists, the attackers often notice when the victim shuts down a machine or starts locking out some access to the attacker. "It's a human being, and he has remote access and an admin console, where he can see all systems he can access. If those systems start disappearing from the console, [attackers] will start hiding," because they then know they've been spotted, says Lucas Zaichkowsky, enterprise defense architect at AccessData.

Zaichkowsky cites the case of a large financial services company whose security team thought it was in the clear after cleaning up an SQL injection attack on one of its servers. "They had moved on. But the attacker saw them remediate, and [so he] dug in deeper elsewhere, because he had already planted other backdoors that hit other systems. He went silent and waited months for things to die down."

Another 200-300 backdoors already were in place. "They thought they had remediated, but it turns out they had backdoors in the network segment that were not even documented from [a] past acquisition. As the victim organization was investigating the attacker, the attacker group was looking at other techniques to maintain their foothold in the target." he says. "That's how the big boys do it."

Look around for signs of hacking tools in action, such as password dump programs, pass the hash, keyloggers, and RAM scrapers, he says. "A hacker uses a toolset when breaking into an organization. In most breaches [other than a SQL injection attack], it's a long process for the attacker."

The typical attack starts with a compromised user via a phishing attack or watering hole attack, and then it moves to privilege escalation to other systems

within the victim's organization -- and then the dreaded lateral movement and entrenchment in the network, Zaichkowsky says.

You can contain the attack without pulling a box offline. "It [shutting down the machine] will eat up evidence, and you won't be able to put together the entire puzzle," CSC's Mason says.

"Containment has to be smart ... make sure you have pre-approved servers that are yours and clean" and you can isolate the host only to communicate to those designated servers, he says.

Steven Adair, founder and CEO of the IR firm Volexity LLC, says the key is not to panic. "We have a process through IR, but [customers are often] in a panic wanting to shut down. They turn off machines a lot of times. But we like to grab memory, which is volatile... You have only one chance to catch up. If you turn it off, you can read the hard drive but lose what was in memory."

Leave the infected machine online, but block it from accessing the Internet. Adair recommends putting in place an isolated VLAN, or firewalling the machine from communicating outside the organization. This keeps the network connection enabled and on, but the infected system is no longer a danger to the rest of the network.

Block off your virtual private network, for instance, add two-factor authentication (if it doesn't already have it), and change all user passwords, he says. "Bad guys are using admin credentials. We know what they are going to do next: it's logical that they are going to use those."

Zaichkowsky concurs that you can isolate a machine you know has been compromised. "You can change the ACL [access control list] so it can only talk to the investigator's system," but that has to occur quickly and ideally via automations.

Don't keep the breach a secret in-house.

If your CEO first learns of the breach in the newspaper, you've not only lost control of the story, but you may also have just lost your job. "Communicate early and often to management. The earlier they know about it, the better," says Ken Silva, senior vice president of cyberstrategy at ManTech.

Panic tends to instill secrecy, he says. "When you panic, it tends to scare others around you, and information gets compartmented and things go sideways. When

information is not disseminated in a timely fashion, it gets fabricated by somebody, and false information" ensues. "That's why having an IR plan is so important: who's going to communicate, how often, and what they will and will not talk about," for example.

Two-thirds of executives surveyed by The Economist Intelligence Unit and Arbor Networks say that a well-handled response to a breach can actually boost their organization's reputation, so a smooth incident response and the smooth reporting of an incident are considered good PR in this new climate of inevitable breaches.

Cris Ewell, CISO at Seattle Children's Hospital, says that once a security event is identified as an incident, it's go time. The hospital's incident management team convenes. "We have a very aggressive plan." The team, which is made up of executives or leaders from various departments, discusses what to do next. "If it's really big, do we [employ] containment or remediation? If it's smaller, a smaller team that includes legal, compliance, and me, asks if it meets criteria for a breach."

If the event entails public disclosure, there's a communications plan, Ewell says. Marketing and communications would become involved, and a press conference might in order, depending on the size of the breach.

Don't shy away from sharing intelligence about the attack with other organizations.

Seattle Children's Hospital also communicates daily with other hospitals and organizations on the latest threats. This intelligence-sharing and communication model -- formal or informal -- is a crucial element of responding to and possibly preventing a full-blown data breach, experts say.

"There is a value in sharing," says Volexity's Adair. "The more open [you] are, and the more you share on detail," the better. That means not just passing the location of a bad domain to other organizations in your industry or group, but also providing real attack information. "That helps people have a better understanding," he says.

This summer, the retail industry will launch its own official intelligence-sharing mechanism, which is expected to mirror the model of information sharing and analysis centers in other industries. Until now, some retailers have informally swapped intelligence with one another.

"Don't stick your head in the weeds. You can't solve this problem by yourself. You have to share with other people," Seattle Children's Hospital's Ewell says. "I share with other CISOs all the time. We talk, and that is very helpful to solve issues, especially when we talk about incidents."

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

http://www.darkreading.com/attacks-breaches/what-not-to-do-in-a-cyberattack/d/d-id/1234954