After the breach: Surviving cyber attack

Catherine Bolgar December 1, 2014

Cyber breaches may be inevitable, but the best companies limit their frequency and damage, while learning how to improve security.

Gerry Kane

Cyber Security Segment Director, The Zurich Services Corporation

About this expert

SHARE THIS ARTICLE: E-Mail | Facebook | Google+ | Linkedin

Companies need to stress speedy identification of breaches and resilience to limit cyber risks.

Cyber security until recently has focused on preventing attacks. However, companies that rely too much on prevention may be caught out if they haven't also planned what to do after their defenses have been penetrated.

"Most companies don't have an incident-response plan, nor do they have a proper partner. When the crisis happens, it's panic mode and the damage is even worse," says Christophe Nicolas, Senior Vice President of Kudelski Security, the cyber security division of Kudelski Group SA.

"Many organizations don't recognize that breaches are inevitable," says Charles Carmakal, Managing Director of Mandiant, a unit of cyber security firm FireEye Inc. "Companies have to get security right every time – an attacker only has to get it right once.

"Sometimes getting hacked doesn't mean you've fallen asleep at the wheel. In fact, some of the most secure organizations in the world have been attacked and breached a number of times because threat actors are willing to spend significant time and resources to steal their intellectual property. Companies with mature security capabilities learn from the attacks and improve their defenses," says Mr. Carmakal.

You aren't a defeatist, but rather a realist, if you admit that no matter how good your defenses you will be breached. So what should you do when it happens?

> "Companies have to get security right every time – an attacker only has to get it right once." "

Assess the situation

Larry Collins, Vice President, E-Solutions at Zurich Insurance Group, says companies need to ask, "How far did they get? What did they get? Who were 'they'? How do I recover? Whom do I need to inform? What business plans do I need to replace that stolen intellectual property? What are my liabilities?"

One important thing that can't always be determined definitively is what data was exposed versus what data was stolen. "Maybe the intruders had the ability to access certain data, which isn't the same as knowing the attackers viewed it or copied the data from the environment," says Mr. Carmakal.

Act quickly

While the intruders may have been in your system for months, you have only hours to react once a breach is discovered. That's because breaches often come to light when customers notice incorrect invoices, fraudulent charges on their credit cards or evidence of stolen identities. Law enforcement agencies, which monitor shady actors—who often operate off yet another victim's IT system—might alert you to a breach. Stolen intellectual property cases might be kept under wraps, but stolen employee or customer data is hard to keep secret.

“You have to assume that a breach will be disclosed by someone,” Mr. Nicolas of Kudelski says. “We now think it’s better to disclose the breach than have it done by someone else.”

Mr. Nicolas cites a rule of eight: “You have eight minutes to make a decision on what to say, eight hours to decide what to do, and in eight days you’ll be measured on how well you reacted.”

> “ While the intruders may have been in your system for months, you have only hours to react once a breach is discovered." ”

Be thorough

Hackers are careful to install multiple ways to access a network, says Jim Jaeger, Chief Cyber Services Strategist with General Dynamics Fidelis Cybersecurity Solutions. “If you find and clean up four or five of those back doors and stop the breach and clean up a lot of their malware, they’ll still have ways to get back in,” he says. “They’ll stop while you’re doing the investigation, and in a month or two they’ll come back. Sometimes they’ll just keep going.”

That’s why it’s necessary to find and eradicate all back doors and other tools used by the attackers at the same time. “If you do it sequentially and focus on Europe, then Asia, then North America, or on some systems and not your entire network, they’ll come back in through one of the data centers or systems you haven’t eradicated yet, and they’ll infect areas you just cleaned up,” Mr. Jaeger says. “We found with a big multinational that it took almost two months to plan the eradication phase and orchestrate the resources around the world to conduct the operation simultaneously.”

Rather than spending time trying to isolate, study and eradicate malware, some companies practice speedier “wipe and rebuild” procedures. As soon as evidence of malware is detected on a device, it is wiped—all disks erased and reformatted—and rebuilt according to standard configurations with data restored from backups.

Plan ahead

“The time is now, before you know you have a problem,” Mr. Collins says. “Do your homework now, so when you have to make that emergency phone call at 2 a.m. you already have someone you know is going to help you.”

> “ You have to discover the risks your controls are already addressing, the risks you may want to transfer to insurance or the risks you can’t realistically do much about and that you have to accept." ”

A good plan includes internal and external elements:

Forensics. Dealing with a breach is too big a job for most IT departments, so an outside cyber forensics specialist should be on retainer—you don’t want to hunt one down in the midst of a crisis.

"Your IT people will know forensics companies, but you probably will have to push to get the names," Mr. Collins says. "There's lots of pride in workmanship in IT. They like to think their system will never get hacked. People have to understand it's a moving target. Line it up in advance and say you want three recommendations. And somebody on the senior team has to be willing to write the check to get these services on a retainer basis. Some cost is involved."

Relationships with local and federal law enforcement agencies are also important.

Legal counsel. If you have a breach, "there's a strong likelihood that there will be some sort of legal action as a result," Mr. Jaeger says. "With cyber crime, too often the victim is the one that gets sued by credit card companies, the state attorneys general and the whole range of regulatory agencies. Therefore, you want your incident-response [forensics] firm to be contracted through the outside counsel cyber law firm so communications with it are covered by attorney-client privilege."

Every country in the European Union has its own data privacy office; laws in Asia and Latin America vary by country. Forty-six U.S. states have data privacy laws. "They all might have different requirements about what to report," Mr. Collins says. In the face of such a complex web of authorities, "you usually need an outside legal counsel who knows who has to be notified."

Depending on the data that has been compromised, you may need to inform regulators, customers, business partners, credit-card companies or your payment processor, Mr. Carmakal says.

Insurance. "Cyber insurance makes you value your data," says Lillian Ablon, researcher at the RAND Corp., a think tank "But the greater value you put on it, the more you pay."

A risk assessment is crucial, says Alan Brill, Senior Managing Director for Kroll Inc., a risk and security company. "You have to discover the risks your controls are already addressing, the risks you may want to transfer to insurance or the risks you can't realistically do much about and that you have to accept."

Backups. "Because it takes so long to learn about a compromise, forensic evidence may no longer be available," Mr. Carmakal says. "Logs may be written over. Certain standards require that logs be kept for at least a year. Having security logs dating back to the beginning of the compromise will facilitate a quicker and more comprehensive investigation."

Relevant logs include those concerning firewalls, domain name system (DNS), dynamic host configuration protocol (DHCP), Web server and security events.

War games. "Usually the first time your team gets together is after the first breach happens," Mr. Collins says. "Have a practice run before so it's not a surprise; so there are no turf wars. Work that out in advance. Make sure everybody has actually met. Have you met the forensics people yet?"

Too often, incident-response plans focus on IT and network security personnel, Mr. Jaeger says. The team needs to include representatives from the company's business operations, media and general counsel functions.

Ordinary contact information needs to be assembled—in a safe, offline place—and kept updated for moves and transfers, not only of your internal team but of your external cyber-security partners, including law enforcement, as well.

Have every aspect worked out in advance, such as "getting a call center to notify a million people that you lost their data," Mr. Collins says, or "what you are going to tell the reporter who calls to ask for a statement."

Such "war games" identify gaps in planning or personnel, and help team members feel more confident and be more effective when the real crisis happens. "War-gaming exercises help people learn about managing emotion and communications, and doing the right things at the right times," Mr. Nicolas says. "In the end, it's traditional crisis management."

Attackers try to have resilience. "They have multiple points from which to operate if one goes down. They try to increase their points of presence by moving laterally or creating back doors in your system," says Ms. Ablon of the RAND Corp.

That's a lesson companies need to take from their attackers. "How do I operate through a breach with minimal business impact? How do I deal with a loss of reputation? It's not just about operating through the network," she says. "Resilience is crucial."

Related articles

December 1, 2014
Risk Talk A strategic approach to cyber risk

December 1, 2014
Interconnected risks in a digital economy

Subscribe to our newsletter

Related Topics

› **Cyber risk**