ARTICLE

You've Been Breached. When Do You Engage a Third Party?

Pride Comes Before the Fall

We've all experienced that dreaded feeling: I just can't do it myself. It hurts to admit. You realize the time spent trying to remediate the problem is lost and things are worse than when they started. Unfortunately, when it comes to cybersecurity and incident response, there isn't the luxury of time to learn from mistakes.

However, with a well-developed and up-to-date incident response plan, organizations can clearly define internal roles and responsibilities and determine where a third party can extend capabilities. In addition, an incident response plan can reduce the overall cost of an incident. In a 2014 Ponemon study, the average cost for each lost or stolen record was $201, but with a formal incident response plan already in place, the average cost of a data breach was reduced as much as $17 per record[1].

How do you determine when to engage a third party?

Answering the following three critical questions for response readiness will help define who, what, when and where a third party should be engaged.

According to IT and IT security practitioners in the United States and EMEA who are involved in handling security and incident response for their company:

55% say their security team lacks the sufficient skills to effectively investigate and remediate sophisticated cyber attacks and compromises[1]

38% say it could take a year to know the root cause of a cyber attack[1]

41% say their organizations will never know with certainty the root cause[1]

According to U.S. executives surveyed on how they are prepared to respond to a data breach:

30% say their organizations are effective or very effective in developing and executing a data breach plan[2]

78% say they have no set time to update and review the plan or haven't updated and reviewed since inception[2]

41% say they disagree or strongly disagree that their organization understands what needs to be done following a material data breach to prevent negative public opinion, blog posts and media reports[2]

[1] *Threat Intelligence & Incident Response: A Study of U.S. & EMEA Organizations.* February, 2014
[2] Ponemon Institute Study: *Is Your Company Ready for a Big Data Breach?* September, 2014

Do You Have the Expertise to Address the Full Scope of the Threat?

Security leaders must evaluate the functional requirements (people, process and technology) in place to quickly and effectively resolve an incident.

1 Is Our Incident Response Plan in Place and up to the Task?

- First and foremost, if your organization doesn't have an incident response plan in place, nothing else really matters.
- Secondly, your plan must be current to reflect personnel, leadership and overall organizational changes.
- Third, your plan must accurately reflect your team's capabilities to respond to various types of breaches, and address the skillsets required for all phases of the incident response workflow.
- Fourth, the plan must be current to reflect the latest intelligence and tradecraft used by attackers.
- Lastly, the plan must be tested to look for gaps.

2 Do You Have the Expertise to Address the Full Scope of the Threat, Eradicate it, and Determine the Extent of the Compromise?

- Security leaders must evaluate the functional requirements (people, process and technology) in place to quickly and effectively resolve an incident through each phase.
- Given the increasing sophistication of advanced threat actors, incident responders must have institutional knowledge on the tactics, techniques and procedures (TTP) used by threat actors.

3 Is Any Personal, Private or Privileged Information at Risk?

- This question literally cuts to the chase for any security leader trying to determine how to move forward when a security breach occurs. For organizations with large amounts of intellectual property, credit card information, and customer, patient or employee records, a security breach can quickly grow in its potential impact by orders of magnitude and easily eclipse the expertise of the incident response team and overall IT organization.

By formally outlining the incident response plan and understanding internal capabilities, organizations can clearly define when and in what situation third party involvement is needed. Additionally, by clearly outlining the details, organizations can negotiate incident response retainers with third parties to minimize reactive costs and improve readiness response times. Below are two examples of organizations that had a well-planned out incident response plan that identified when third parties were engaged and activated incident response retainers that dramatically decreased remediation efforts.

A Point of Sale Exposure

A Fortune 100 technology service provider self-discovered that multiple kiosks used by customers to pay bills had been compromised by malware. Recognizing a gap in expertise to quickly remediate the issue, the security team initiated a third party incident response retainer with SecureWorks. Initial analysis from a forensic team quickly revealed that 20 precent of the client's 200+ systems were in some form compromised and included keyloggers, memory scrapers as well as command and control mechanisms. Leveraging key intelligence capabilities the forensic team was able to decrease response time to days by creating a custom tool that rapidly and collectively queried multiple malware identification systems for the malicious files, defined specific steps to remediate and provided guidance on alerting the institutions affected.

Spamming Spirals out of Control

IT personnel at a £2 billion insurer noticed an employee's account sending spam emails to the entire company without the employee's knowledge. Forty-eight hours later, with more than 150 infected workstations and successive waves of spam, the IT team realized they were losing the fight. The company initiated an incident response retainer with SecureWorks and the responders were quickly able to identify the threat and understand the full infection chain. Detecting infected systems, disrupting beaconing to Command and Control infrastructure and ultimately wiping out the malware became straightforward after utilizing SecureWorks' unique capabilities and intelligence resources. Additionally, responders made several recommendations to the customer's IT team and user education on dealing with suspicious files.

Next Steps

Based on direct experience working with customers who have experienced security incidents, our SecureWorks Counter Threat Unit™ research team has developed a set of ten recommended best practices to help minimize the duration and impact of a security breach. This white paper also includes 18 additional recommendations regarding technical issues, configuration and processes.

Conclusion

While all companies are unique, the need for a comprehensive incident management plan is not. With breaches becoming more common and the results more public facing, readiness is key. Mitigating risk boils down to identifying your strengths and gaps and determining when a third party can extend the capabilities of incident response teams to rapidly reduce response times and operational effort.

より詳細な内容に関しては下記のメールアドレスにご連絡ください
SWRX_PreSales@Dell.com
代表03-6893-2317
www.secureworks.jp/
SecureWorks Japan株式会社