Effective Incident Response Planning Could Save You Millions

As Companies like Equifax, Verizon Wireless, and Anthem know all too well, it's not a matter of if, but when there will be a breach. Are you prepared for when you're attacked?

Today's Realities:

- The average cost of a breach? $3.62 million*
- It takes 214 days on average to detect a breach—and another 77 days to adequately respond*
- Companies must shift from check-box compliance to incident response-based defenses

*2017 Ponemon Cost of Data Breach Incident Report

AWN CyberSoc for IR:

- Leverages people, processes and technology
- Combines human and machine intelligence for real-time continuous monitoring and threat detection
- Managed detection and response to swiftly address detected threats
- AWN Concierge Security Engineer with comprehensive security and IR expertise

Cybersecurity professionals fight a never-ending battle as the digital threat landscape evolves with new viruses, malware, ransomware and phishing exploits growing exponentially. And with the average cost of a breach at $3.62 million according to a 2017 study by Ponemon Institute, it's a very costly battle indeed.

Even companies in full compliance of industry regulations get exploited. In truth, seeking to become impenetrable is admirable but entirely unrealistic. Technology can only do so much, and companies reliant exclusively on technology develop a false sense of cybersecurity. Now is the time to shift from "check box compliance" to risk-based security defenses that rely on incident response (IR).

✓ What's at Stake

The companies that successfully navigate today's treacherous cyber-terrain are those that implement sound strategies for incident detection and response. A foundational mindset for effective defense begins by understanding that attacks and breaches are bound to happen–just ask Equifax, Verizon Wireless and Anthem, which all suffered major breaches that marred their reputations, lost the public's trust, and sunk their bottom lines.

The 2017 Ponemon Report estimates that the mean time to identify (MTTI) a malicious and criminal attack is around 214 days, and the mean time to contain it is around 77 days. The report concludes that companies can lower their cost of handling security breaches by investing in IR tools that speed up the time to identify and contain cyberattacks. That's why organizations need to be forward-thinking in their approach to cybersecurity, especially when it comes to incident response. You must develop plans to mitigate the inevitable threats and attacks still to come, and consider how to do so in the context of business continuity.

Across industries, IT security leaders recognize the need to refocus the majority of their efforts from prevention and compliance to incident response. In fact, Gartner predicts that “by 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches.” That budget figure was in single digits as recently as 2014.

Implementing Best Practices for IR

Having a robust incident response plan requires trained professionals who can lead a response to incidents, processes that use best-in-class threat intelligence to provide additional context, and a scalable technology that can eradicate noise and identify a prioritized set of incidents.

People:

Having a robust incident response plan of action requires having the right team, which involves a more holistic approach than simply relying on the technical expertise of IT.

Company executives and department heads must lend their inquiry, knowledge and expertise as to what effect a breach or major incident might have on company stakeholders—including partners, customers, suppliers, as well as legal counsel and regulators. An open, ongoing dialogue must exist between security experts and top organizational stakeholders as to what incident response systems are currently in place and what others should be considered in the future. In addition, an effective IR plan must take into account what information gets communicated and to what parties in the event of a compromise. This will include, in some cases, government officials and the general public.

Most of all, organizations need to become more “people-centric” and not rely solely on technology to protect their assets. All employees must employ good cybersecurity practices in the work they do and the information they share. And IR defense plans must enlist security experts, who can quickly and accurately interpret the data and information that machine-learning technology provides to make decisions based on the best interests of the organization.

Processes:

Thwarting or mitigating cyberattacks demands precise processes for detection and response. After developing an IR plan, companies need to ensure that the plan delivers the desired outcomes once implemented. This means trial runs to determine how prepared you are, including threat simulation exercises in safe settings to gauge how effectively your IR strategy works in critical attack scenarios.

In transitioning cybersecurity strategies from those centered solely on prevention into ones more focused on detection and response–and better business outcomes, defense teams should evaluate how information flows through all various endpoints, in-house infrastructure and third-party cloud systems. This provides a strong sense of which areas are likely targets of incoming threats, as well as whom will be affected and the impact that might have.

IR processes require constant attention and re-evaluation to ensure that strategies are working and that no steps in the process fall through the cracks. In the case of Equifax, its 48-hour policy of installing software patches was all for naught when–two months after receiving a notice to patch a known vulnerability–it was hacked and the social security numbers and other sensitive data belonging to more than 140 million Americans was breached.

Technology:

You need robust prevention technologies, such as next-generation firewalls, intrusion prevent/detection solutions, web and email gateways, and vulnerability scanning tools to detect threats. In addition, you need a scalable security information and event management (SIEM) platform that can provide 360-degree visibility and continuous monitoring of anomalous activity across your on-premises and cloud-based infrastructure.

Organizations will always require technology that can effectively monitor, detect, and respond to the growing multitude of cyber threats. Yet, human security experts must play an equally critical role in any IR strategy. If your team lacks such experts, you may not have the necessary capacity to lead a successful threat response, even if your systems prove effective in monitoring and detecting what takes place.

✓ SOC-as-a-Service for Comprehensive IR

For mid-size enterprises, combining the essential attributes for effective incident response–people, processes, and technology–can seem unattainable because of cost and required expertise. To build an in-house security operations center (SOC) with advanced technology capabilities manned by a team of experts is beyond many firms' budgets and resource capabilities.

Arctic Wolf Networks (AWN) has the solution in its SOC-as-a-service. The AWN CyberSOC™ leverages people, processes and technology. It extends the capabilities of your IT team without requiring additional investments in hardware, software or staff. It combines human and machine intelligence to continuously monitor and analyze millions of events in real time, providing 24x7 threat detection.

In addition, Arctic Wolf offers an IR simulation advisory service that enables you to assess your IR readiness with the guidance of our security experts who run our SOC-as-a-service. We review your current IR plan and customize it to your needs. We also run through live table-top exercises, and make recommendations on how to rapidly respond to a set of cyber threats, while addressing regulatory requirements that apply to your industry.

To ensure better business outcomes, Arctic Wolf provides the industry-leading SOC-as-a-service with managed detection and response (MDR) that enables you to swiftly address detected threats. Your dedicated AWN concierge security engineer (CSE) recommends remediation actions by evaluating logs and data to proactively hunt down threats. The CSE serves as a trusted advisor and an extended member of your IT team.

With a SOC-as-a-service like the AWN CyberSOC™, you can rest assured in your incident response capabilities and the knowledge that–although attacks are inevitable–you won't become the next Anthem, Verizon Wireless or Equifax.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com