CYBERATTACK THREAT & PREVENTION

PROTECTING YOUR ORGANIZATION CAN BE EASY FOR YOU

LIGHTEDGE

CYBERATTACK THREAT AND PREVENTION

Protecting Your Organization Can Be Easy for You

According to The United States Department of Justice, cybercrime is one of the greatest threats facing our country and has enormous implications for our national security, economic prosperity and public safety.1

While companies of all sizes across the globe are at serious risk of having their vital financial, employee and customer data hacked, small- to medium-sized businesses are often targeted because their defenses aren't as strong as those of larger businesses. And cybercrime continues to grow at an increasingly dangerous rate—a 27.4 percent year-over-year increase. 2 Yet only 25 percent of organizations have a formal cyber incident response plan3 and many underestimate the capabilities of cyber criminals. In fact, it's estimated that only 1 of every 100 security compromises is even detected. In 2016 alone 64 billion data records were stolen.

Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.4 This is a substantial problem.

Organizations can't afford to let cyber criminals into their systems. Among respondents to the 2016 Global Economic Crime Survey, reputational damage was considered the most damaging impact of a cyber breach.5 Not only can a cyberattack cause irreparable harm to an organization's reputation, but the cost of a data breach in the United States could be a staggering $100 million.5 "The accelerating cost of cyber crime is now 23% more than last year, costing US organizations $11.7M on average."2

So, how do organizations lose so much money when they fall victim to a cyberattack? Business disruptions are the largest cost component of a cyberattack at 39 percent. The cost of business disruption includes diminished employee productivity and business process failures. The next most expensive consequence is information loss at 35 percent, followed by revenue loss at 21 percent. You also must take into consideration the loss of trust you'd experience from your key stakeholders and your customers.

Organizations require a more comprehensive, sophisticated, proactive and affordable solution than what's currently being used.

IS YOUR ORGANIZATION TAKING THE STEPS NEEDED FOR SECURITY?

- Do you have a comprehensive information security management system?
- Are you aware of the most recent global threats and vulnerabilities?
- Is there a risk management and mitigation plan in place?
- Are you prepared to act before a security incident occurs?
- In the event of an incident, would you be aware?

PROBLEM DEFINITION

If your organization isn't as secure as it could be, what can you do? The current market for security tools is hard to navigate. Forty-five major vendors offer 85 major security tools from which organizations can choose. Once the tools are purchased, you are left on your own to integrate and layer these tools, which are oftentimes incompatible with each other.

This problem is compounded by the fact that 83 percent of organizations report difficulty finding people with the security skills they need. This resource problem is even more severe in small- to medium-sized businesses. If an organization wanted to maintain the 24/7/365 security team needed to stay protected, it'd require at least seven full-time IT employees.

Another concern is that top senior executives don't have the time or the expertise to understand the threat of cybercrime and plan for emerging threats. In fact, PricewaterhouseCoopers reports that 71 percent of C-level executives get their security information only from cyber security websites and emails.5

Even organizations that fully understand the business value of security intelligence may be faced with budget, bandwidth and skills shortages, making them unable to deploy and manage the robust security intelligence solution they need. Security intelligence offers operational efficiency with better use of people, time and infrastructure. Organizations need the ability to centralize security tools and integrate data from their entire IT infrastructure—their existing network, firewall and endpoint devices. They need to improve their security posture without adding more operational and personnel costs or buying, maintaining and integrating multiple point products.

THE SECURITY SOLUTION

The need for a global, real-time solution to view emerging threats is apparent. This solution should integrate current and new security tools and use Big-Data analytics that combine and organize tens of millions of data points and deliver information that is not only consumable, but actionable. The solution also should provide a team of experts who will proactively assist in modifying and enhancing the organization's security profile.

LightEdge Solutions is partnering with CarbonHelix to deliver this powerful security solution: the Virtual Security Operations Center (vSOC powered by QRadar). Organizations benefit from its unified ecosystem that integrates best-in-class security solutions delivered through a single threat console. This solution provides comprehensive and centralized IT security intelligence. Because it's powered by IBM, it brings IBM's global security footprint to LightEdge's local market customers.

LightEdge is IBM's first vSOC partner in the Americas and delivers powerful security solutions to mid-tier businesses. Mid-tier businesses in regulated industries, those with global service delivery requirements and those whose IT service delivery is their business model should consider the LightEdge vSOC.

The LightEdge vSOC delivers the collective knowledge trained threat analysts and complements LightEdge's current managed security solutions and works on any number of device types or brands. It is deployed and supported locally and provides:

- 24/7/365 log and event monitoring and threat analysis

- Secure, real-time communication with security analysts
- Cognitive event correlation and analysis
- Proactive alerts on emerging threats with recommended security policy changes
- Visibility and improved security policies
- Integration with a vast IBM security ecosystem
- Effective tools and reporting for PCI, HIPAA, PII and other compliance requirements
- Minimization of false positive alerts
- Additional monitoring of firewalls, AV, web, DNS, authentication platforms, and all other potential points of entry

The LightEdge vSOC is a proactive solution that enables policy changes, upgrades and intrusion protection. You can select security solutions tiers based on your organization's existing security profiles.

The solution also gives organizations a much-needed and highly valuable 24/7/365 virtual security partner with global reach, visibility and expertise that's necessary to protect themselves.

ARE YOU A PRIME CANDIDATE FOR VSOC?

All businesses should be locking down their critical data, but security is absolutely essential to organizations that fit the following descriptions:

- Must safeguard sensitive customer, patient or employee information
- Part of a highly regulated industry
- Required to meet global service delivery requirements
- Maintains intellectual property

BUSINESS BENEFITS

Organizations will benefit from the LightEdge vSOC's global footprint and worldview of the threat landscape. It monitors 130 countries and keeps 3,330 security experts on staff. Thirty-five billion events are managed and analyzed daily. The LightEdge vSOC offers 24/7/365 log and event monitoring threat analysis and secure, real-time communications with security experts who provide Watson-like cognitive event correlation. Actionable security information is presented in an easy-to-consume format and offers a combined presentation of actionable threat analysis.

The Virtual SOC Portal combines IBM's global security research (X-Force) with service-level data from devices across your networks to help you manage vulnerabilities discovered in your
systems. Even the most competent IT teams in mid-tier businesses do not have the resources to effectively cover 24/7, eyes- on-screens monitoring, response and management. Proper security administration requires round-the-clock support of a security team within IT.

Multiple technologies and/or devices bolted together create a challenge for interoperability and consistently successful results. The LightEdge vSOC, powered by QRadar, offers a single-pane solution.

Regulated, compliance-driven business mandates competency beyond that of many organizations and requires audit support and reporting resources that consume productivity. The preconfigured features and reporting available through the vSOC are ready-made for compliance, meeting the regulatory requirements for mainstream health and financial industries.

Security technologies remain complex while the threat environment evolves quickly, making it quite challenging to properly adapt and keep current. The LightEdge vSOC will reduce organization at risk for data security.

SUMMARY

In summary, the global threat of cyber criminals hacking into your organization's vital financial, employee and customer data is at an all-time high … and growing year after year. You face the potential loss of your organization's reputation and millions of dollars.

In this day, you need to have:

- A comprehensive information security management system,
- An awareness of the most recent global threats and vulnerabilities,
- A risk management and mitigation plan,
- The ability to act before a security incident occurs, and
- A way of knowing if an incident occurs.

LIGHTEDGE IS BRINGING YOU VSOC TO MEET ALL THESE NEEDS. IT:

- Collects and interprets your network, log and application data,
- Pulls in proven analytics and expert input from a global ecosystem,
- Provides real-time alerts and proactive policy requests,
- Offers simple monitoring through a single-pane-of-glass portal, and
- Grants 24/7/365 local support from LightEdge.

TAKE STEPS TO PROTECT YOUR ORGANIZATION NOW

As a C-level executive, it's imperative that you consider your organization's security practices and identify dangerous and costly gaps. If you're not sure where to start or simply don't have the time to do this, LightEdge Solutions can help. Contact us today at 877.771.3343 and we can review your security measures so you can close any gaps that leave your organization vulnerable to cyberattacks.

Sources:

1 United States Department of Justice, The Executive Office for United States Attorneys, viewed 5/5/2016

2 2017 Cost of Cyber Crime Study: Global, Ponemon Institute.

3 2016 Cyber Resilience Organization study conducted by Ponemon Institute and IBM

4 "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," Forbes, January 17, 2016.

4 2013 US State of Cybercrime Survey: PwC

5"Global Economic Crime Survey 2016, conducted by PricewaterhouseCoopers"