Don’t Become a Headline

Protecting Your Company From Cyber Security Breaches

RCN BUSINESS

Don’t Become a Headline

Protecting Your Company From Cyber Security Breaches

TABLE OF CONTENTS

Don’t Become a Headline
Protecting Your Company From Cyber Security Breaches

INTRODUCTION

Before becoming a CIO, CTO, or IT director, you probably spent time as a project leader. Your team was responsible for running cable, managing databases, and providing desktop support. As the front-runner for each project, your focus was to carry out the strategic goals of the organization and manage the day-to-day activities.

That was before the hackers had your data in their sights.

Now they’re out to get you. It’s not a matter of “if” but “when” there will be a security breach. The CEO knows it, which is why you may find yourself talking, more and more, to C-level leadership about network maintenance and optimization.

The plague of ransomware, such as WannaCry, has cost companies billions of dollars in 2017. A variant called Petya was wiper malware disguised as ransomware. The creators of this far more destructive type of malware aren’t in it for financial gain. Their intent is system destruction on a massive scale to disrupt business and government operations. These advanced and persistent threats are what keep CIOs and IT directors awake at night. So, with cybercrimes growing at a faster rate than ever before, many companies must take a fresh look at current protection plans.

250%

The Q2 2017 “Proofpoint Quarterly Threat Report” shows that malicious message volume jumped 250 percent over the first-quarter. Emailed ransomware attacks continued to grow, accounting for 68 percent of all malicious messages containing malware.

While cloud computing offers layers of security for companies searching for ways to combat the mounting cost of cybercrime, a managed service provider (MSP) helps remove the complexities associated with managing mission critical applications.

REFERENCE: https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q217-threat-report.pdf

ELEVATED SECURITY RISKS

Mobile devices and ubiquitous Internet access have allowed business to expand in ways we couldn't have imagined 20 years ago. That growth and flexibility also gave us complex corporate structures, a distributed workforce, multiple internal departments, and huge databases full of confidential information.

So now we're sitting in a dangerous business intersection. Customers and vendors are concerned about the volume of data collected and how it is used, while attackers are getting better and faster at mounting malicious and costly cyberattacks. With the rise of IoT, cloud applications, and other evolving technologies, it is incumbent upon you to use cutting-edge protection measures to secure your network from malicious behavior.

An Inside Job

For IT, the task of maintaining and safeguarding an ever-growing amount of data is compounded by the proliferation of "bring your own device" (BYOD) usage. The obvious benefits include cost reductions and employee satisfaction. However, there are plenty of well-founded concerns about security and privacy because cyber criminals now target mobile devices knowing that employees walk around with access to customer data and company information in their pockets. Key stakeholders need to engage throughout organizations to adopt clear guidelines and best practices on how they use, store, and transfer data both inside and outside the business.

Although businesses are vulnerable to hackers who probe networks and break through firewalls, the biggest threat often comes from inside the company. Unsuspecting employees frequently fall for phishing scams. It's staggering how many people still click on links or open attachments in phishing emails.

According to the Q2 2017 "Proofpoint Quarterly Threat Report," there has been a recent increase in one-to-one attacks in which a single employee receives a spoofed email from a single executive.

ELEVATED SECURITY RISKS

Here are a few areas in which a company might drop the ball and expose itself to infiltration:

Timely Patching - Regularly applying security updates will significantly reduce the chances of being infected by malware. With IT teams often taxed to their limits, patches sometimes don’t get installed due to time constraints. Other times, there may be a concern that an update will cause a domino effect that breaks a currently working system.

Access Levels - As companies grow, employees often move into new roles or work on cross-functional teams. Over time, many end users have access to data they shouldn’t see because it’s not relevant to their job. If your employees have excessive data access, it might be time to implement the principle of least privilege. Under a least-privilege scenario, restricted user rights limit an employee's access to the resources aside from those needed to perform their regular job. The principle of least privilege can also apply to processes, systems, and devices, so they only have access to the resources required to perform an authorized activity.

Outbound Data - Egress filtering controls the traffic traveling from your network to the outside world. With proper filtering, you can restrict employees or systems from sending out protected data. Egress filtering also prevents attempts at network mapping. If nothing else, restricting outbound packets makes you a good neighbor on the Internet as part of a “do no harm” policy. Compromised systems sometimes play a role in criminal activities by behaving as a transit point for illegal traffic.

Budget Constraints - When money is tight, IT departments are often the first to feel the squeeze. So even if you’re aware of all the points raised in this paper, you will still be on thin ice if you don’t have the funds for proper anti-virus software, firewalls, and qualified in-house cyber security experts.

REFERENCE: https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q217-threat-report.pdf

MINIMIZING THE THREAT

At this point in the war against cyber criminals, most companies understand there is some level of threat. Unfortunately, even some large companies fail to comprehend the extent of that risk. Or they do understand their exposure but don't have the budget to address it with an in-house solution correctly.

Network security is increasingly complex and dynamic, making it nearly impossible to manage for IT departments already overwhelmed with network administration, device support, and database management. As a result, security breaches that should be discovered in minutes often go unnoticed for weeks or months.

229 DAYS

Statistics in the most recent Ponemon report show that dwell time is an average of 229 days. In other words, nearly two-thirds of a year might pass between the time malware enters a company's network and when it is detected.

The gap is critical because the longer malicious software lingers, the greater the risk for significant damage.

In your efforts to reduce the risk of cyberattacks, trying to address the problem with a bigger budget and more staff might not be the answer. Without a team of experts dedicated to threat discovery and mitigation 24 hours a day, seven days a week, keeping cyberattacks at bay is like trying to hold back the tide. So maybe a better solution is to use your existing budget for a managed security solution that is more secure, efficient and cost-effective.

As they become more concerned about data vulnerabilities, C-level executives and leadership teams are supporting the move to third-party, cloud-based network security administration. A managed services provider enables a company to implement content filtering and define which devices connect to different parts of the network. Experts at RCN Business say cloud-based security solutions are new to a lot of executives and IT professionals. Once executives see the benefits, however, they understand the need to move past the old paradigm of on-premise hardware that requires hands-on maintenance.

REFERENCE: https://securityintelligence.com/media/2016-cost-data-breach-study/

WHAT TO LOOK FOR

In today's connected global economy, businesses are operating 24x7 and can't afford network downtime. Managed services provide better reliability, more uptime, and enhanced security while helping you control operating costs across your entire IT network.

Using a cloud-based managed services solution makes good business sense for a variety of reasons:

Monitoring and uptime - The concept of "business hours" is becoming more outdated with every new app and mobile device. Employees work flexible hours to fit their lifestyles, and they are often scattered across multiple time zones. That means there is no good time for the network to go down, either for routine maintenance or due to a malicious attack. Staffing a network center around the clock or having team members on call at night and during weekends is cost-prohibitive for most companies. Partnering with a managed services provider ensures continuous network monitoring and instant attention to outages, which should guarantee uptime in the range of 99.999 percent.

Peace of mind - A managed network infrastructure provides infinitely more security than most companies can maintain on their own. Your managed services provider protects your network from viruses, malware, spam, and inappropriate Web content.

Instant updates - Managed services providers implement constant, real-time security updates 24 hours a day, seven days a week, 365 days a year. A premise-based firewall cannot be updated to combat new threats as quickly as cloud-based security. Receiving instant updates can be especially beneficial for companies in the finance or healthcare industries, which need to control data access for regulatory or compliance reasons.

Industry experts - Companies with limited budgets don't have the luxury of hiring full-time experts across a range of networking and security disciplines. By partnering with a network management service provider, you have a virtual staff of certified IT network professionals who are up to date on the latest security threats and solutions.

Redundancy - A secure data center is designed to protect your information and prevent outages. However, you don't want to put your business in the hands of a partner with a single point of failure. In the unlikely event of a data center outage, your managed services provider should quickly failover to an alternate center to ensure business continuity.

WHAT TO LOOK FOR

The need for improved cyber security is increasing, and the threats grow and change at an alarming rate. Clearly, a possible best solution is prevention through a managed network provider. Beyond prevention, however, companies need swift breach detection and remediation to minimize the time criminals spend in their environment. The most efficient way to achieve those goals is through 24-hour monitoring and rapid restoration services administered by professionals who specialize in managed security. A qualified partner should offer industry-leading best practices in threat intelligence and security analytics to counteract malicious activity.

Cloud-Based Security - Select a managed services firm that is committed to protecting your data from hackers and malware, and that will notify you immediately if a potential breach is detected. Insist on a fully monitored and scalable Layer 3 and Layer 4 stateful firewall, DDoS protection, and cross-organization application visibility.

Comprehensive, Integrated Service - You're moving to a managed solution to control costs and simplify network administration, so look for a provider that offers an all-in-one suite of services that includes:

- Network management supported by expert monitoring 24x7x365
- Equipment management for any physical devices located in your facilities
- Cloud-based phone solution
- Managed router service to ensure reliable end-to-end network management and secure connectivity

Availability - By default, you expect your managed services provider to operate a staffed operations center all day every day. They should always be on top of things. But with that said, there might be times when you want to be proactive and contact your provider. Make sure you have the option of contacting them 24x7 on a direct line that doesn't send you into the void of a call center. Check the service level agreement to see if the guaranteed response time meets your expectations.

Best-in-Class - In the network solutions space, one good way to gauge service providers is through the annual "PCMag" Business Choice Awards. The awards highlight the broadband providers that score best overall with readers. Rankings also take into account reliability, value, and how likely readers are to recommend a vendor to colleagues and friends. "PCMag" readers consider service providers that make the cut to be clear favorites.

RCN BUSINESS

CONCLUSION

If you’re struggling to keep up with hardware and software demands, and your company’s network security is not optimized, then a managed service provider can be a lifesaver. To learn more about how to secure your company’s data at the network level, schedule a free consultation with an RCN Business representative.