CYBERSECURITY STATISTICS TO DRIVE SECURITY ENHANCEMENTS NOW

A cyberattack is a scary event. It can shut down your business, cripple government agencies and incapacitate hospitals and other healthcare providers.

Here are seven cybersecurity statistics and recommendations that will get you thinking about new ways to enhance your IT security posture.

7 Scary Cybersecurity Statistics and Recommendations to Improve Security

1

43% OF SECURITY BREACHES AFFECT SMBs

In 2020, small and medium-sized businesses will continue to be primary targets of cyberattacks. Many businesses struggle with IT budget constraints and lack proper cybersecurity resources, which hackers routinely take advantage of.

Source: *2019 Data Breach Investigation Report, Verizon*

Recommendation: Automate patch management to stay up to date with security patches. In the Kaseya 2019 State of IT Operations survey, only 42% of organizations had, or planned to have, automated patching.

2

29% OF BREACHES IN 2018 INVOLVED THE USE OF STOLEN CREDENTIALS

Compromised passwords are a major threat to businesses. Passwords can be hacked with brute force attacks, stolen through email phishing scams and purchased on the dark web.

Source: *2019 Data Breach Investigation Report, Verizon*

Recommendation: Tighten your password security protocols and implement authentication methods like two-factor authentication (2FA) and single sign-on (SSO) for enhanced security. Organizations also need dark web monitoring to proactively check whether their compromised credentials are being shared on the dark web. With dark web monitoring, organizations can take steps to prevent a data breach from occurring.

3

3.5 MILLION UNFILLED CYBERSECURITY JOBS PREDICTED BY 2021

The cybersecurity skill gap is a major threat to organizations. 53% of organizations report a problematic shortage of cybersecurity skills.

Source: *Cybersecurity Jobs Report, Cybersecurity Ventures*

Recommendation: Address the skill gap by implementing cybersecurity training or partner with academic institutions to nurture cybersecurity talent.

4

ON AVERAGE, SMALL COMPANIES LOSE OVER $100,000 PER RANSOMWARE INCIDENT

Ransomware has been on the rise over the past couple of years, knocking out some city services and forcing others to revert to paper records. The effects of a ransomware attack can be very damaging to small or midsize businesses and the expensive nature of these attacks can be attributed to costs associated with downtime and recovery.

Source: *Second Annual State of Ransomware Report, Osterman Research*

Recommendation: Implement a reliable Backup and Disaster Recovery (BDR) solution that automatically tests backups to ensure recovery. Choose a BDR solution that is integrated with your endpoint management tool.

5

32% OF DATA BREACHES IN 2018 INVOLVED PHISHING ACTIVITY

Phishing featured in 78% of cyber espionage incidents in 2019. Phishing is a method of gathering personal information, including login credentials, through the use of deceptive e-mails to get unsuspecting recipients to click on malicious links.

Source: *2019 Data Breach Investigations Report, Verizon*

Recommendation: Organizations can avoid phishing attacks by training their employees to identify phishing emails and to report any phishing activity. Tools are available to help with this type of cybersecurity training. Tools are also available to help identify and quarantine phishing emails.

6

8 OF THE 10 MOST EXPLOITED SOFTWARE VULNERABILITIES LAST YEAR INVOLVED MICROSOFT PRODUCTS

The most exploited vulnerability in 2019 involved Adobe Flash Player while there were four for Internet Explorer and three for Microsoft Office.

Source: *Criminal Underground Continues to Target Microsoft Products in Top 2019 Vulnerabilities List, Recorded Future*

Recommendation: Be sure to have an automated patching process in place that covers Windows and macOS operating systems, browsers and third-party applications.

7

THE AVERAGE COST OF A DATA BREACH WAS $3.92 MILLION IN 2019

Data breaches are extremely costly. The U.S. incurs the highest average data breach cost at about $8.2 million.

Source: *Cost of a Data Breach Report 2019, Ponemon Institute*

Recommendation: Use an endpoint management solution that integrates antivirus, backup and patch management in a single console.

The above statistics show that cyberattacks and data breaches can be a huge threat to your business. It is critical for your organization to establish a strategy to mitigate security risks. Even if you are a small business with a limited budget, you can achieve enterprise-level security with Kaseya VSA.

Kaseya VSA is a remote monitoring and endpoint management solution that allows you to manage and secure your entire IT. To learn more about Kaseya VSA request a demo here.

Kaseya®