LUNAVI

ARE YOU READY OR AT RISK?

LEARN HOW TO GUARD AGAINST TODAY'S TOP CYBERSECURITY THREATS

LUNAVI

Among all the business changes and challenges brought on by the pandemic over the past year, one of the most significant was a dramatic increase in the volume and variety of cybersecurity threats.

Shifts in how and where employees work have created new points of vulnerability that cybercriminals are all too eager to exploit, from remote working to increased use of digital devices. And the cost of these vulnerabilities is already adding up, with global losses from cybercrime exceeding $1 trillion in 2020 alone.

But knowledge is power when it comes to protecting your organization. Read on to learn about today's top cyber risks and the proven solutions you can put in place now to help safeguard against them.

The FBI reports a 4x increase in cybersecurity complaints since the start of the pandemic.

Microsoft reports that pandemic-related phishing and social engineering attacks have skyrocketed to 30,000 a day in the U.S.

LUNAVI

Risk #1

Phishing

These deceptive e-mails and websites can trick unsuspecting employees into revealing passwords, account details, and other valuable info that they can then use to breach systems, access accounts, and compromise data.

Spear phishing attacks account for 95% of breaches in enterprise networks, according to Cisco.

Phishing attempts soared by 667% in March 2020.

Best Defenses

Business-class email service system with advanced security:
Ensures protection features are built into your email service to detect and isolate malicious phishing email

Identification and access management (IAM) platform:
Provides multi-factor authentication to guard against unauthorized account and system access

Employee education:
Teach staff to recognize phishing attempts and report suspected encounters

Ransomware

Risk #2

Ransomware attacks have risen 800% during the pandemic. As of September 2020, 1 in 4 remediated cyberattacks were linked to ransomware.

Average cost to fix the data encryption damage: $1.45 million.

Cybersecurity ventures predict that a business will fall victim to ransomware every 11 seconds in 2021.

A type of malware that encrypts a person or organization's files, often preventing them from accessing them unless a ransom is paid. It's typically unleashed in a device or system via email phishing, social media phishing, or exploit kits (automated programs).

Best Defenses

Cybersecurity hygiene housecleaning:
Focuses on getting software and systems up to date, ensuring security tools are working as intended and deploying effective access controls to reduce risk, including MFA.

A comprehensive endpoint protection solution:
Leverages automation to continuously scan for vulnerabilities, identify suspicious activity and links, and automate investigation and response.

Comprehensive backup and DR plan:
Leverages cloud solutions to protect your information and allow you speedy recovery if the unfortunate should happen.

Work-from-Home Vulnerabilities

Risk #3

Almost half (48%) of recently surveyed workers in the U.S. said they were hit by targeted phishing emails, phone calls, or texts during the first six months of remote work.

9% of those workers said that they were hit by one or more such attack each week.

A lack of network perimeter security can lower cybersecurity defenses for remote workers, enabling cybercriminals to exploit new avenues of vulnerability, including cloud-based services, improperly secured VPNs, and unpatched assets.

Best Defenses

Be proactive: Perform regularly scheduled vulnerability scanning and patching, and monitor for suspicious activity.

Employ strong IAM controls: Treat identity as the primary security perimeter. This includes maintaining an active directory platform, enforcing multi-factor verification, maintaining strict password management, and controlling locations where resources are located.

Fortify security with multiple protection layers: Adopt a Secure Access Service Edge (SASE) approach to secure access, taking advantage of firewall as a service (FWaaS), secure web gateway (SWG), zero-trust network access (ZTNA), and a medley of threat detection functions.

Empower IT: Equip IT teams with remote monitoring and endpoint management tools that can actively monitor for suspicious activity, and automatically patch endpoints to help keep them secure.

Risk #4

Cloud-based Threats

With the recent rise in cloud computing due to the pandemic, many companies may have rushed to migrate their tools and operations without ensuring they have sufficient security to protect against online risks such as cloud app vulnerabilities, incomplete data deletion, and misconfigurations in cloud storage.

In a recent survey, organizations named misconfiguration (68%), unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%) as their top cloud security concerns.

Best Defenses

Establish thorough cloud governance policies: Track what cloud apps your organization uses and help secure them with capabilities like single sign-on and conditional access to the cloud via app security and Active Directory services.

Leverage security-focused technology and services: Use these resources to discover shadow IT, monitor and control user actions, and ensure appropriate in-app permissions.

Move at cloud speed to defend against attacks: Implement cloud native security orchestration automation and response (SOAR) capabilities to take immediate action around identified threats.

Risk #5

Internet of Things (IoT)

Comprising a vast and growing universe of devices and equipment (possibly 35 billion IoT devices worldwide by the end of 2021), IoT encompasses everything from edge computing devices to home appliances, wearable technology and cars. And, since most IoT devices lack the processing power for even basic protection like encryption, they present a wealth of new potential entry points for hackers.

Since the coronavirus hit, McAfee device monitoring has shown a 22% increase in the number of connected home devices globally and a 60% increase in the U.S.

According to The McKinsey Global Institute, 127 new devices connect to the Internet every second.

Gartner predicts that by 2022, IoT security attacks due to lack of insight into edge and third-party device providers will increase by 35%.

Best Defenses

Know your IoT landscape:
A significant part of cyber-securing IoT involves understanding what is connected in the IoT landscape, knowing how to best protect the most important assets, and effectively mitigating and remediating security incidents and breaches.

Secure connectivity between devices and the cloud:
Do a vulnerability assessment of all devices connected to your network (on-prem and remote), maintain a list of approved IoT devices, and enforce cybersecurity policies to block unsecure new devices from networks.

Secure provisioning of devices:
Compartmentalize IoT devices to minimize attack surfaces, scan all software for network and app vulnerabilities, and update and patch both networks and devices

Secure data in the cloud:
Take measures to secure or even encrypt data during processing and in storage.

Keep your guard up:
Continuously monitor for IoT threats, anomalies, and unauthorized devices.

LUNAVI

Ready or not, cybersecurity risks are out there and pose a significant threat to your organization, your customers and your peace of mind.

At Lunavi, we can help you put the right defenses in place to fortify and protect your organization from critical vulnerabilities today and in the future. Learn more at Lunavi.com.

LEARN MORE

SOURCES

https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats

https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

https://www.securitymagazine.com/articles/94343-five-cyber-threats-to-watch-in-2021

https://www.techrepublic.com/article/how-remote-working-poses-security-risks-for-your-organization/

https://securityintelligence.com/articles/iot-threats-look-out-2021/

https://www.gurufocus.com/news/1206905/check-points-2020-cloud-security-report-highlights-enterprise-security-concerns-and-challenges-in-public-clouds

https://www.mcafee.com/blogs/consumer/consumer-threat-notices/top-security-threats-to-look-out-for-in-2021/

https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/?sh=68ccbb945d50

https://www.tietoevry.com/en/blog/2021/01/three-ways-to-enhance-edge-iot-security/

About Lunavi

As a leading managed service provider and consulting firm, Lunavi is focused on helping customers advance their digital transformation goals by modernizing business applications, migrating solutions to the cloud, designing hybrid cloud solutions, and applying Agile and DevOps engineering practices to build new, innovative solutions. Our portfolio of services is designed to provide continuous improvement along each step of the IT journey to maximize business value and success. We are a Microsoft Gold Partner and Azure Expert MSP, offering deep expertise in the Microsoft ecosystem of enterprise IT software and services. Visit us at www.lunavi.com to learn more and follow us on LinkedIn, Facebook, and Twitter.

LUNAVI