2022

CYBER SECURITY

CNP TECHNOLOGIES

TABLE OF CONTENTS

03-05

THE CYBERSECURITY CHECKLIST

25 Cybersecurity Best Practices

06-07

PATCHING BEST PRACTICES

4 Steps to an Effective Patch Management Process

08-10

CYBER INSURANCE

The Cost of Not Having Cyber Insurance

6 Ways to Lower your Risk

11-15

PREDICTIONS

6 Predictions for Cybersecurity in 2022

8 Steps to Secure Your Business Now and in the Future

CHECKLIST:

25 BEST PRACTICES FOR CYBERSECURITY

In Partnership with FORESITE

- Remove local administrator access for all users – Local admin access by users is a high risk if user credentials get compromised.

- Limit user's access to only the data/systems needed for their role – Make sure there are no shares or privileges for user's accounts to data that they do not need. "Least privilege access" decreases the ability of an attacker to gain access to all data by compromising a single user's credentials.

- Do not allow anonymous access to anything – Scan your network to enumerate all shares. Add permissions to any with anonymous access and remove any default logons from devices (i.e. admin/admin).

- Use secondary accounts for all admin access – When admins use these accounts for daily use the admin accounts are exposed to increased risk of credential theft. Keep the usage at a minimum.

- Use long, non-string passwords for all admin and service accounts – Administrator accounts and service accounts are primary targets of threat actors. Make them difficult with a password management tool to maintain the complex passwords.

- Terminate sessions after a period of inactivity – Session stealing is a common practice. Don't expose these sessions any longer than necessary.

- Only allow remote access through encrypted channels – Use Multi-Factor Authentication (MFA). Remote access is a huge threat vector and requires additional technical controls.

- Do not expose RDP to the internet – RDP weaknesses and vulnerabilities are well known and easy to exploit.

CHECKLIST

- Use some form of wired network access controls – Basic MAC address filtering adds an extra layer of security by checking the device address against an approved list.

- Separate the Guest wireless from Production – Guests should never be allowed on the production network.

- Use WPA-2 enterprise with authentication for production wireless access – A passphrase is not enough as the wireless usually extends beyond the walls.

- Stop using USB storage except where absolutely required – USB storage is a method used to infect with malware and increases risk of data leaks.

- Ensure all systems stay patched – All applications and devices such as firewalls; not just Windows patches.

- Use a modern antivirus – Next-gen AV can respond to behavioral threats, not just a database of known virus signatures.

- Review everything that you are allowing through the firewall on the internet – Networks can allow things on the internet via the firewall that open them up to threats. Make sure you know what is allowed and why, and make sure the firewall is patched regularly.

- Provide security awareness training for all users – Users often can be a weak point. Make sure they understand the risks, the latest threat tactics, and what to do if they receive a suspicious request.

- Preserve critical logs – Logs should be shipped off critical servers and devices and preserved in case they are needed for incident investigation.

- Implement spam filtering – Email is a major threat vector. Spam filters can flag and block suspicious messages.

CHECKLIST

- Implement physical security for critical systems – All critical and sensitive servers and network equipment should have limited physical access.
- Visitors should always be escorted.
- Password hygiene – Train users not to save passwords in cleartext files. Use at least 12-character complex passwords and force scheduled changes.
- Multi-Factor Authentication – Use MFA for any access coming from the internet, including VPN, webmail, and cloud services.
- Destroy any data device before disposing – Shred hard drives, destroy removable media, and render the data unrecoverable.
- Remove user access to anything and everything after terminations – A process should be in place to remove access when people leave the organization, including 3rd party vendors that have system access.
- Plan for worst case scenarios – Make sure you know what to do if there is an incident such as ransomware or business email compromise. Have resources in place before you need them to speed up response.
- Scan for vulnerabilities – Scan all internal and external devices on your network as often as possible to detect and remediate known vulnerabilities.

PATCHING
BEST PRACTICES

When working with Windows and 3rd party applications, it can be difficult to stay on top of all vulnerabilities that could lead to potential security issues. The best way to prevent any holes or vulnerabilities is to find the weak spots and use secure patches to reinforce areas of concern.

According to Forrester's State of Application Security Report, application vulnerabilities are the most common external attack method, making patch management critical to your company's overall security. In fact, according to the Ponemon Institute, 57% of cyberattack victims report that their breaches could have been prevented by installing an available patch and even more chilling, **34% of those victims knew of the vulnerability, but hadn't taken action.**

Why? Perhaps it's the sheer volume of vulnerabilities that arise each year.

Info Security Magazine reported that **more than 18,000 Common Vulnerabilities and Exposures (CVEs) were published last year alone.** That's an **average of around 50 CVEs a day**! As technology continues to move more quickly, it's expected so will potential vulnerabilities. With so many gaps in such a dynamic landscape, it can feel impossible to stay on top of making sure your applications are safe from attacks.

Beyond the sheer volume of constant new vulnerabilities, patching can be time consuming. A patch needs be tested first to make sure it 1. Works to eliminate the vulnerability and 2. Doesn't adversely affect your installed software. **In fact, 74% of companies say they simply can't patch fast enough because the average time to patch is 102 days according to Ponemon.**

4 STEPS TO AN EFFECTIVE PATCH MANAGEMENT PROCESS

Patching is important so you can ensure your company and customer data is secure against ransomware and other malware, which can take advantage of application vulnerabilities to hack your system.

So, what can you do to make sure you have an effective patch management process?

1. **Assessment:** The first step is to discover, assess and categorize. This means making sure you have a full inventory of all devices, applications, operating systems, etc
2. **Establish Policy and Process:** Once you have your inventory, it is critical to have a patching policy established. This can include what you will patch, when, and under what conditions. It's also key to set up an overall patch process such as monitoring vulnerabilities and patch release schedules and timelines for testing and maintenance.
3. **Take Action:** Follow your outlined policy and processes established above in order to 1. Test patches, 2. Roll out the tested patches, and 3. Report to track your patch management and compliance.
4. **Rinse and Repeat:** Review your results continuously as you repeat your process to look for areas in which you can improve in order to best stay on top of emerging vulnerabilities and released patches.

While patching may be time-consuming and difficult, it is a critical aspect to making sure your organization is safe and secure from cyberattacks. If you have concerns about increasing cyber threats and potential vulnerabilities in your applications, please reach out to our expert cybersecurity advisors. We can provide an assessment of your current patching process and see where there may be gaps before you become one of the 57% who experience a data breach due to poor patch management.

CYBER INSURANCE

According to a survey of nearly 3,000 risk management professionals, COVID-19 continues to be viewed as a top business risk for 2021 alongside Cyber Incidents **(both at 40% of those surveyed)** and comes in second only to **Business Interruption (41%)**. While cyber incidents have been a growing concern for years, the pandemic has increased the risks due to increased reliance on remote technology, as well as the speed with which new technology was adopted.

Due to the surge in these risks, cyber insurance premiums, which now total around $5 billion annually, have drastically increased and are expected to continue to **increase 20 to 30% per year on average.** A few reasons for these increased premiums are as follows:

- **COVID-19:** The pandemic has turned the world upside down in many ways, including how businesses and workforces operate. With many employees going remote, devices were exposed to less secure networks, leading to an increase in cyber incidents.
- **Ransomware:** Ransomware continues to increase exponentially as criminals find easier ways into unprotected systems. With the threat of ransomware increasing, cyber insurance companies must respond with higher premiums to offset the increased probability a client may become a victim of a ransomware attack.
- **Email Compromise:** Over 90% of successful cyberattacks start with an email. As phishing increases and cyber criminals become better at getting employees to click or respond to phishing emails, cyber incidents will continue to proliferate, causing cyber insurance rates to increase.
- **Changes to regulations:** Compliance demands continue to grow as industry regulations, privacy, notification laws, and notification requirements change and increase leading to more reported incidents and higher premiums.

THE COSTS OF NOT HAVING CYBER INSURANCE

Cyber Insurance is critical to your business and continues to be as threats grow in number and sophistication. Here are just a few reasons why it's so important you protect your company with substantial coverage:

RANSOM COSTS

After a ransomware attack, some companies choose to pay the ransom in hopes of restoring their data...however, **paying the ransom results in only a 30% chance of data and systems being recovered**.

DATA RECOVERY

With only a 30% chance of data and systems being recovered after paying the ransom, you may never be able to recover the data lost in a ransomware attack or other incident involving a loss of data.

COMPLIANCE FEES

Compliance is not only difficult to navigate, it can also be expensive. Ransomware will cost you a pretty penny on compliance as well.

LEGAL FEES

The costs of legal fees related to cyber incidents and the fees associated can cause irreparable financial damage to a business.

6 WAYS LOWER YOUR RISK AND MITIGATE CYBER INSURANCE COSTS

Despite the growing cost of cyber insurance, and the necessity of robust coverage, there are some key methods and best practices to reduce your liability:

1. **Use enterprise-level antivirus:** Enterprise-level, next generation antivirus solutions combine various technologies such as behavior analysis, artificial intelligence (AI), machine learning, live monitoring, and intention monitoring to find threats, instead of just scanning for signatures. Traditional consumer-level antivirus can’t fully protect your data and systems.
2. **Conduct regular penetration testing:** Regularly check your entire system for vulnerabilities, exposed endpoints, software weaknesses, necessary updates, and any flaw that a hacker could potentially exploit. If any issues are found, you can quickly resolve them before your business is exposed.
3. **Adopt a data recovery and backup solution:** If your data becomes corrupted due to a security incident, a comprehensive data backup and recovery solution will keep your business moving forward. Your chosen solution should also be tested regularly to ensure that you are able to recover your data if an incident were to occur.
4. **Patch management:** Many cybersecurity incidents have been the result of unpatched software. **In fact, 57% of cyberattack victims report their breaches could have been prevented by installing an available patch.** Patches secure any weak spots or vulnerabilities that have emerged, leaving you open to ransomware or malware attacks.
5. **Make sure your website is secure:** Always use a trustworthy provider for website hosting and regularly conduct audits to ensure there are no vulnerabilities that could leave your company and data open to cyberattacks.
6. **Notify and train employees:** Keep your employees up to date on the latest threats and trends in cybercrime so they can stay vigilant to not fall victim to suspicious emails and other vulnerabilities.

Cyber insurance can feel like a daunting expense, but the potential loss of data and coinciding expense of not having comprehensive coverage can be worse. CNP can help you prepare for the growing threat landscape while recommending insurance partners that can ensure your organization can recover.

CYBER SECURITY

PREDICTIONS

2022 AND BEYOND

CYBERSECURITY PREDICTIONS

Cybercriminals show no signs of slowing down. As our daily lives and work increasingly integrate with technology, cybercrime is only going to get stronger, smarter, and have farther reaching consequences. Knowing what to prepare for in advance can help to tie up those loose edges and take a strong stance against the risk:

1

CRIME-AS-A-SERVICE

Believe it or not, there are cybercrime companies set up on the dark web to sell ransomware, malware, and other cybercrime technologies as a service to the highest bidders. Expect to see this trend continue and protect yourself against phishing schemes, spoofing, botnets, data breaches, as well as your typical trojans and malware. Bad actors will include adversarial governments, political actors and anarchists, and those seeking a big payout (ransomware). This puts government, utilities, healthcare, transportation, and other critical businesses and services at increased risk.

2

SATELLITE ATTACKS

Satellites are filling the skies, with everyone from Elon Musk to Amazon jumping on the bandwagon. It stands to reason that hackers will soon follow, opening up a whole new attack surface that many may not have considered. ICARUS, for example, is a proof-of-concept DDoS that can use satellites to attack from various locations. Targets of this new form of cybercrime will include companies relying on satellite-based connectivity to operate, deliver connectivity to remote locations, or provide services to customers on the move, such as the transportation sector

3

LINUX VULNERABLE TOO

Historically, the hacker community has mostly ignored Linux, but this is starting to change. For instance, Vermillion Strike can target and remote access Linux systems in stealth, as to not be detected. A vast majority of back-end systems and networks are still Linux based. Also, Windows 11 has Linux integrations. It’s imperative to consider this in your security measures. Protect for every operating system and platform in use, even if it didn’t seem necessary before.

4

CONTINUED MICROSOFT FLAWS

As mentioned previously, Microsoft vulnerabilities continue to be an issue and will be for the foreseeable future. Patching and maintenance is imperative, but don’t allow that to be your only line of defense. A thorough and robust security plan outside of the realm of Microsoft is critical to your defense, as are consistent testing, logging, and recalibrating accordingly.

5

REMOTE AND HYBRID THREATS

Remote and hybrid work has become the new normal for many businesses, especially those which already rely heavily on technology. This presents a brand-new challenge for security, however convenient it might seem to work from home. Employees are now moving away from secure company infrastructure into home network environments, and they might not have the IT credentials or the outside knowledge to secure their environment effectively. It’s a huge vulnerability that might not have existed before. Supplying employees with secure technology and devices, monitoring and logging network activities and credentials, testing home and company networks, training for digital safety, and utilizing security software and insurance is not optional anymore, if it ever was.

6

CRYPTO CRIME

Cryptocurrency and digital transactions have been targets for digital thieves from the start. But as crypto gains in popularity with Web3, NFTs, the Metaverse, and digital banking moving to mainstream, current security technologies like encryption and multi-factor authentication won’t be enough. Digital wallets are already being targeted at scale with fake gift card generators, fake cryptocurrency apps, fake digital wallets, and trojans like ElectroRAT. Increasing cybersecurity awareness and training, implementing stricter security policies, and utilizing security tools outside of the basic encryption technologies are going to be more important than ever.

8 STEPS TO SECURE YOUR BUSINESS NOW AND IN THE FUTURE

Now that we've shared a checklist for the current threat landscape, some patching best practices, how cyber insurance is effecting business and we've looked at what the future might hold, let's talk about continued preparation for today and into tomorrow: What steps can you start taking right now to prepare and secure your business for what the future holds?

1

Unified Security Products: Modern security defense requires a comprehensive approach, with integrated software and devices designed to interoperate as a unified solution in all locations where you do business. This leads to the next point:

2

Encompassing Protection: You need to protect every user, every device that accesses company resources, and every application in company use, including remote or on the move work. Follow and protect every data point and every transaction end to end.

3

Strong Policies: Ensure that security policies are enforced and followed at all times by everyone, everywhere they go, including outside of work. Conduct digital safety training as a requirement for all employees on a repeated and frequent basis. Remember, the Colonial Pipeline incident happened because an employee used a company password outside of work for an unrelated and unsecured account. It's the little things that slip by that will get you.

4

Patch and Update: Keep your software current with the latest patches and releases as soon as they are available. This includes mobile devices, servers, and any device accessing company infrastructure, even if it seems irrelevant.

5 **Strong Filters:** Take a security-first approach to bringing on any new software or devices. Research them thoroughly: how often are they updated? How strong are their security features? How many other dependencies will they bring with them and what are those dependencies? How thorough is their SBOM? Protect your network and any endpoints before onboarding, log the details of the process, and keep a record of the SBOM on hand.

6 **Behavioral Analytics:** Preparing for, discovering, and blocking attacks in the early stages through behavioral analytics can significantly increase your chance of stopping a threat before it does too much damage or spreads through your entire system. It might even detect an issue before the damage starts. Monitoring your systems, building a threat aware environment, and probing for strange activity constantly will do wonders for your attack prevention.

7 **Real-time Protection:** Your security toolset needs to be robust with machine learning, use of threat feeds and attack profiles, real-time capabilities, 24x7 monitoring, security insurance, and ability to detect and protect against both known and unknown threat factors.

8 **Scalability:** Your security protocols and toolset need to be able to grow with your business, keeping you secure through every stage of your company evolution. Experiencing a security breach because you expanded your offerings or opened a new location could be the end to your business growth cycle. The ability to protect every endpoint, even through a stage of expansion, is imperative to your data security and digital safety.

While this book might be a good start...

...we know we haven't been able to cover close to everything you might need to protect your business in 2022, which is why having cybersecurity experts on your side is so important. Information about cybersecurity is constantly changing as new threats emerge everyday and our goal is to keep your business, employees, and clients safe.

From data protection, recovery, and business continuity to network security and email protection, CNP has over two decades of experience helping clients across the United States from our HQ in Charlotte, NC.

If you have questions or concerns, our expert engineers are always here to answer any of your questions. For more information or to get an assessment of your business and security needs, contact us at info@cnp.net or give us a call at (888) 973-3737.

www.cnp.net

CNP

TECHNOLOGIES