Preparing for Cybersecurity Threats You'll Face - Not If But When

Luis Simonet
NXTsoft CISO

Preparing for Cybersecurity Threats

- The fact is while companies may now be aware of the risks they are facing hackers continue to stay a step ahead, identifying newer vulnerabilities to exploit and finding more effective strategies for getting what they want. In fact, we often say it's not so much a matter of if you will be attacked, but rather when.

- The risk and severity of cyber-attacks have clearly grown over the past few years.
- The advancement of technology and the wide use of digital media is making attackers smarter by the day. As technology continues to develop and evolve, businesses need to keep up and protect themselves by preparing for a cyber attack.
- These cybercriminals take advantage of individuals and firms who pay less heed to cybersecurity.
- We frequently see news related to cybersecurity threats like ransomware, phishing, or IoT-based attacks.
- The best practice in cybersecurity is staying ahead of threats rather than managing them later. With cyber attacks on the rise, it's no longer sufficient to simply react and clean up the mess that occurs. Businesses need to shift from reactive to proactive. That's why businesses need to consider what steps are necessary when preparing for cyber-attacks.

- You should know and prepare for the top cybersecurity threats that organizations will face in 2020.

But, First let’s look at some of the Threats to Be Aware

- **Cloud Vulnerability**
  - The adoption of the cloud is creating new challenges.
  - The Oracle and KPMG Cloud Threat Report 2019 reveals that cloud vulnerability is and will continue to be one of the biggest cybersecurity challenges faced by organizations.
  - Cloud Services have become more business-critical. Organizations are leveraging cloud applications and storing sensitive data; ePHI, PII, CDE, etc.
  - The Use of Cloud Services Continues to Grow; confidence has increase
  - Cloud Security is a Confusing Shared Responsibility between CSP and customer.
  - Visibility is more cloudy
- Tips:
  - Before you start; create and document a design and scope:
  - Governance
  - Risk Assessment
  - Compliance
  - Responsibilities Matrix: CSP/Customer/Third-Party

- **Social Engineering Attacks**
  - Social engineering attacks like phishing have always been used by attackers to trick victims into surrendering sensitive information like login details and credit card information. Though most organizations are enhancing their email security to block phishing attacks, cybercriminals are coming up with more sophisticated phishing attacks.
  - The vast majority of cyber-attacks deploy social engineering methods. They exploit fear and uncertainty to trick users.
  - No surprise; Due to the COVID-19 pandemic an uptick in sophisticated phishing email attacks by cyber-criminals has emerged.
  - Users isolation and home-based networks

IoT-Based Attacks

- The number of internet-connected “smart” devices in homes and businesses are starting to increase. The problem is that not all of these smart devices have strong security and are creating openings for attackers. Cyber-criminals target IoT devices specifically because they are often overlooked when it comes to applying security patches, which makes them easier to compromise.

Tips:

- Keep inventory of all internet-connected devices on your network
- Keep firmware for these devices up-to-date
- Change defaults settings: user/password
- Enable security: do not try to make it easier for users

Ransomware

- Systems get infected, data is encrypted, ransom note
- Ransomware is been around for several years, but still popular and a big risk**.**

Tips

There are a few strategies for dealing with ransomware. The first is to use strong perimeter security, such as firewalls/IPS, to prevent malware from being uploaded to your systems. Second, individual workstations should have a good End Point Protection software. Having a business continuity/disaster recovery plan in place that includes an offsite backup of all of your most important business data can help to protect your business against loss.

Internal Attacks

- The biggest risk to any organization’s cybersecurity program is from the employees who use network resources on a daily basis.
- The level of access that employees have make them capable of inflicting great harm if they choose to abuse their access privileges for personal gain or if they accidentally allow their user accounts to be compromised by attackers, or unknowingly download dangerous malware onto their workstations.

Tips:

Implement least privilege to limit what systems and IT resources any user can access to the minimum required for their job.
Implement RBAC
Employee termination checklist and process
Monitoring and review

Security Gaps

- According to data from the 2019 Verizon Data Breach Investigation Report, the majority of cyberattacks (52%) featured “hacking.” Hacking can be defined as direct intrusion attempts made by people outside of your organization attempting to bypass your perimeter network security in some fashion.
  - Old unattended systems
  - Unpatched vulnerabilities
  - Missing implementation across the organization
  - Misconfigurations
  - Rouge devices on the network

Now Let's outline some key steps you can take when preparing your organization for a cyber attack

Hack yourself

Before you can begin taking steps to protect your business from cyber threats, you need to figure out where your vulnerabilities are. Conducting a security audit can highlight areas for improvement for your business. Once you know where your company excels in security and where you could improve, you can begin taking concrete steps to improve your security and help protect your business against potential cyber attacks.

Provide cyber awareness security training to employees

The majority of cyber-attacks are trace back to a negligent employee or contractor as being the root cause. Because of this, it's especially important that you educate your employees about the risks of cyber attacks and some of the potential tactics hackers can use to access company data. A business should develop a cyber security policy that works for them and the type of data they collect and store. Then you can incorporate the policy into your employee handbook and training. Cyber security training ***should not*** be just a one time a year event.

Make use of good cyber hygiene and controls

- Create and maintain an acceptable use policy
    - Require employees to acknowledge reading and understanding on an annual basis
    - No public WiFi
    - Do not connect to unknown networks
    - Do not share credentials
    - Quickly report suspicious activities or possible breaches
    - Careful use of USB drives
- Put other policies in place to guide your employees

- **Utilize technical safeguards**
  Secure your devices and Network. While preparing for a cyber attack, you can further protect your business by ensuring your company has the most up-to-date technology to protect against a potential breach.
    - Multi-Factor Authentication (MFA)
    - NGFW
    - EPP/EDR
    - IPS/IDS
    - Monitoring: SIEM, RMM
    - Scanners
    - Data encryption: at rest and in transit
    - Others

    Note: Your efforts to protect your company's data shouldn't end at the office. With work from home programs becoming increasingly common, it's also crucial to ensure any devices your employees are using remotely are protected.

Have a strong backup policy.

- Isolated network
- Offsite – Cloud
- Multiple times in a day

Create, maintain and test your incident response plan

Even after taking every possible precaution, a cyber attack could still occur. That's why it's important to have an incident response plan in place. That way, if your business suffers from a cyber breach, you'll know exactly what to do.

- **Get cyber insurance**
- **Get updates on the latest risks**

Summing Up

Cybercriminals are constantly looking for fresh exploits and producing advanced strategies to defraud organizations. Considering this fact, organizations should be mindful of not just the ever-growing number of vulnerabilities but also of the cybersecurity threats that are coming.

Questions