5 Cybersecurity Quick Wins

Devolutions

HERE ARE 5 QUICK-WIN SUGGESTIONS THAT YIELD NEAR-TERM, HIGH-IMPACT RESULTS

One of the defining features of cybersecurity is that it is an ongoing (read: endless) commitment vs. a one-time event. Despite this, many IT security professionals are under extreme pressure to produce some “quick wins” and prove that investments and resources are being put to good use.

If you are facing this scenario, or if you need to dramatically improve your organization’s cybersecurity posture in a relatively short period of time, **here are 5 quick-win suggestions that yield near-term, high-impact results:**

1. IMPLEMENT TWO-FACTOR AUTHENTICATION (2FA)

Compromised credentials are commonly used to log into client networks through remote access systems, such as VDI, VPN, Web Access, Outlook, and so on. And because the activity seems normal, threat detection alarms fail to go off.

Implementing 2FA – which combines something users know (username + password) with something they have (device) or something they are (biometric) – adds a vital additional layer of authentication. Granted, 2FA is not bulletproof. However, **it is a step in the right direction**, and depending on the number of users in your organization, it can be implemented within hours or days.

Learn More: For our comparative review of the most popular 2FA solutions (now updated with FreeOTP, Authenticator Plus, and SoundLogin), click here.

2. ESTABLISH A STRONG PASSWORD POLICY

Weak passwords continue to be the number one security risk. That's where establishing a strong password policy can make the difference between a costly hack and staying out of harm's way. **Here are several best practices:**

- Prevent users from choosing passwords they have selected in the past.
- Enforce a minimum password age. This prevents users from circumventing the password system by creating a new password, and then changing it back to an old one.
- Set a maximum password age policy. Note that recent NIST guidelines advise organizations to dial down the frequency at which users must change passwords, since studies show that they tend to replace strong old passwords with weaker passwords.
- Enforce a minimum password length standard. According to research by BetterBuys.com, **a password that is 7 characters or less can be hacked in milliseconds**. However, a password that is 11 characters long takes a decade to hack, and a password that is 12-characters long takes 200 years to hack.
- Ensure all passwords meet minimum complexity standards.
- Reset the local administrator password every 180 days and reset the service account password at least once a year.

- **Protect domain administrator accounts with strong passphrases** that have a minimum of 15 characters.

- Implement a password audit policy that allows you to track all password changes.

- Create email notifications that remind users when it's time to change their passwords before they expire.

- **Store passwords using reversible encryption** for all users. Note that this should only be enabled on a per-user basis, and only to meet a user's actual needs.

Learn More: For more advice on all of the password management best practices highlighted above, click here.

3. IMPLEMENT PRIVILEGED ACCESS MANAGEMENT

Mismanaging access to privileged accounts is something that 65% of organizations are guilty of doing, which can lead to security breaches, regulatory penalties, customer churn, lawsuits and lasting reputation damage. In some cases, it can even lead to extinction: a study by the National Cyber Security Alliance found that 60% of SMBs go out of business within six months of being victimized by a major cyber attack. **Here are a few best practices for implementing a robust PAM system to consider:**

- **Identify and analyze all privileged accounts and end users to ensure that access is appropriate**, that it aligns with acceptable risk levels, and that it complies with regulatory requirements.

- Ensure access to privileged accounts complies with the principle of least privilege (POLP).

- Constantly **monitor all privileged account usage and enforce strict controls** for sharing credentials.

- **Implement high-trust authentication methods for privileged access** and leverage suitable PAM tools and technologies.

- Augment and extend privileged identity management with access governance controls to meet ongoing compliance needs.

Learn More: For more advice on all of the PAM best practices highlighted above, click here.

4. CREATE A CULTURE OF SECURITY AWARENESS

As noted above, implementing a strong password policy is critical to ensuring that users are part of the solution instead of the problem. However, **it is important to go further by educating them** — through presentations, videos, emails, or any other suitable methods — about risks such as email phishing and even online shopping. It is also wise to have users enroll in free online cyber security training so they grasp the fundamentals.

Learn More: For advice on how to educate your users and create a culture of security awareness, click here.

5. IMPLEMENT PATCH AND VULNERABILITY MANAGEMENT

It is critical for all computer systems and mobile devices that interface with your business data to have the latest patches and updates. **Here are the best practices in this area:**

- **Use a good discover service that uses a mix of active and passive discovery features**, and has the capacity to identify physical, virtual, and on/off-premise systems that access your network.

- **Make sure to include Mac systems and devices in the discovery process;** research shows that MacOS may be more vulnerable to cyber threats than many people believe.

- Patch applications are not just operating systems; as many as 80% of software vulnerabilities derive from non-Microsoft apps running on Windows.

- **Patch off-premise devices and not just on-premise devices;** remote and mobile workers can be hit by zero-day exploits, which migrate to the corporate network when they connect back on the network or to VPN.

- Create a process to patch weekly; different vendors have various patching release cycles, and trying to keep up with their schedules is not just an administrative burden, but it can lead to gaps.

- **Deploy a flexible architecture that allows both agentless and agent support for servers.**

- Mitigate exceptions accordingly by (for example) locking down user permissions, applying whitelisting, and so on.

Learn More: For additional advice on all of these patch and vulnerability management best practices, click here.

ADVICE FROM OUR CSO MARTIN LEMAY:

Some of the controls presented in this paper might seem costly for some organizations. My advice is to prioritize your investment according to your risk profile. Threats are different from one organization to another. Quick wins presented in this article might not necessarily apply “as-is” to your organization. However, they tend to be common controls that offer the best cost-benefit ratio. Perform a risk assessment and invest in what you are actually trying to protect.

LOOKING AHEAD

The cyber threat landscape is getting worse — not just because user and corporate data is becoming a more valuable commodity, but because hackers are using more sophisticated tools and tactics. These aren’t the script kiddies of old who were intent on destroying machines and wreaking havoc. Today’s hackers are motivated by money, and they are surprisingly well-organized and highly funded.

The 5 quick wins described above **will help you clearly and measurably strengthen your organization’s cybersecurity in the near-term**, so that you can minimize your chances of getting hacked, as you strive to stay a step or two ahead of the bad guys.