7 Cyber-security Best Practices Every Business Should Implement

During 2019, cyber criminals attacked thousands of businesses. Half of those attacks targeted small businesses, many of which rely on outdated systems and insufficient security. Those businesses lost millions of dollars, as well as the confidence of their customers. While cyber-attacks pose an increasingly serious threat, cyber-security best practices mitigate the danger.

Businesses that invest in cyber-security initiatives realize the benefits of protecting vital assets and maintaining critical business reputation. With the help of an experienced technology partner, use these seven steps to begin building the fortress you need to defend against cyber-crime.

1. Create an Acceptable Use Policy – and Enforce It!

Acceptable use policies (AUP) outline employee use of business-owned PCs, cell phones, software, internet access and email. For instance, a favorite tool of cyber-criminals involves duping employees into installing malicious software embedded in innocent-looking files or apps.

The AUP can whitelist admissible websites that employees can access with company-owned devices, enforcing the policy with content-filtering software and firewalls. The AUP should also include policies for network access by personal devices. Finally, it should cover lost or stolen devices, as well as outboarding procedures for employees who leave the organization.

2. Require Strong Passwords and Multi-Factor Authentication

Employees should get in the habit of using strong passwords that contain at least eight characters, mixed case, symbols and a number. In addition, requiring passcodes for cell phones will help prevent unauthorized persons from compromising a stolen device. Finally, enable multi-factor identification as an essential security measure.

3. Keep Your Systems Up to Date

Hackers exploit known vulnerabilities in common software programs such as Office 365. Consequently, you must protect your systems with a patch management strategy. Install security patches quickly for your servers, access points, desktops and laptops. Patch management can prove a daunting task, but managed services providers can help.

4. Insist on Reliable Backups

Your most important protection in the case of a ransomware attack lies in having access to clean, recent backups. Run frequent backups, test them and keep a copy of the backup offsite. Then, if cyber criminals, careless employees or natural disasters destroy your data, you can recover quickly, with minimal data loss.

5. Invest in a Quality Firewall and Monitoring

A firewall acts as the front-line defense against hackers, blocking everything you have not specifically allowed to enter or leave your network. For instance, you should block international access, as well as potential public domain access, in order to discourage overseas hackers.

Start with a quality firewall, such as a multi-function firewall from WatchGuard Technologies. Then practice vigilant firewall management and routinely update firewall policies to block or allow specific types of network traffic.

6. Perform Regular Security Audits

Cyber-security is not a "once and done" protection. New security factors enter the picture frequently, from changes in the supply chain to additional connected devices. Conduct regular network assessments and penetration testing. This will allow IT to map the location of all assets and address any vulnerabilities.

7. Train All Employees on Cyber-security Best Practices

According to a recent report from Verizon, 57 percent of all database breaches resulted from insider threats. From careless employees who ignore acceptable use policies to those who fail to recognize the signs of a phishing email, humans represent the primary security vulnerability. For example, an employee may infect the entire network by clicking a malicious link.

Make regular cyber-security training mandatory for all staff. Help them to understand the "why" of cyber-security best practices. Then ensure success with a layered approach, combining formal training with special events and just-in-time reminders. In the event that you lack internal resources to conduct training, consider engaging a third party to train your staff.

Expert Technology Partners Make Security Possible

The business security experts at eMazzanti Technologies can help you develop a comprehensive strategy to implement cyber-security best practices. Start with a free security and backup audit to assess your company's overall network health. We will look for data-loss and security loopholes and help you build a strategy to secure vital systems and keep business and customer data safe.