winxnet

Top Five IT Security Best Practices for Small and Mid-Sized Businesses

In today's world, IT security is no longer optional. It is imperative that organizations create a culture of security and enforce IT governance to make sure their business stays secure. According to the Verizon 2015 Data Breach Investigations Report, 99% of breaches led to compromise within days or less with 85% leading to data exfiltration in the same time. This report also states that 85% of breaches took weeks or more to discover and 84% of data records were stolen as a result of stolen login credentials.

How can an organization assess whether or not it is secure? Here are the top ways to assess risk:

1. **Physical -** It is extremely important that your organization enforces and creates a secure location. Locked buildings and doors, access to secure computing areas are controlled and audited. Servers are in a secured data closet that only necessary personnel have access to. Although this may seem trivial, it can be surprising how many businesses are not physically secure.

2. **Logistical/ Administrative -** In order to create a culture of security, it is extremely important to enforce IT Governance at your organization. Designate a security officer to enforce the security rules and best practices. Hold frequent staff training sessions to make sure your employees are aware of how to stay secure. Create recurring assessment and easurement of security success and efforts to try and improve security understanding from employees.

3. **Technology -** First, it is crucial to understand that there is no single technology solution. With today's fast-paced environment, Mobile Device Management is now essential and all mobile devices must have physical locks, encryption on all devices as well as a mobile wipe. Password management is also very important and organizations must inform employees about the length, complexity, duration and storage of a password as well as the best practices for managing those passwords.

4. **Procedural -** Documented policies and procedures are necessary to stay secure. These procedures help govern staff activity related to security and create guidelines that help employees know what to do and what not to do.

5. **Organizational -** Leadership must enforce organizational security. Consistent and measurable review of organizational policies and requisite updates must be put into practice and regulated at a frequent basis.

Read on to learn about the top 10 IT security best practices your business needs to consider to minimize risk and protect your data. If you don't feel like your organization is where you need to be from a security perspective, then click here to request a free cybersecurity assessment from a Winxnet expert.

Top 10 Security Controls for Organizations

winxnet

1. Awareness Training

Periodic security awareness training is by far the most effective measure to put in place that will reduce your company's susceptibility to phishing and other types of cyber-attacks. Most compromises start with a click of a mouse so be sure that your IT provider or staff take the time to educate your organization about security.

2. Outsourcing

Security specialists are in high demand, which makes it hard for smaller companies that do not even need a full-time expert. With more options in the marketplace, delegating some of your company's security functions to a reputable vendor that specializes in information security makes the task of staying secure more manageable.

3. Social Engineering Testing

With user-based attacks leading the charts, there is no better control to augment and test your awareness training program than with social engineering testing. A well-executed test will allow your organization to reveal any potential weak spots and test the efficiency of your training program.

4. Backups

Equipment failure is still the number one non-malicious cause of downtime. It is important to frequently check your backup solutions and enforce centralized file storage. Your organization must test backups periodically to make sure that everything is running properly.

5. Updates

Software vulnerabilities are still widely exploited by hackers as means of gaining unauthorized access. Automatic updates are crucial and any device that's connected to your network needs to be updated on a frequent basis.

6. Antivirus

Malware is software that is intended to compromise computer systems and is a top malicious technical threat, frequently augmenting social engineering attacks. Antivirus solutions can help minimize the potential impact of malware attacks and this protection is imperative to stay secure.

7. Filtering

Hackers need to get data and code across your firewall. Tight control of what data is allowed in and out of your network will make those tasks more challenging for attackers. For a basic and inexpensive level, you can set web browser filters and will control what you can and cannot access. With a centralized solution you can set company-wide filters so your employees aren't able to access malicious sites.

8. Authentication

Stolen credentials are another leading method of getting into your systems. Using strong passwords and changing them periodically will help you stay more secure. A reputable password management tool will also help avoid password reuse. Where possible, use multifactor authentication mechanisms for more critical data.

9. Encryption

All mobile devices need to be encrypted as a first line of defense against the exposure caused by a lost or stolen device.

10. Security Monitoring/ Detection

A security incident is a matter of when, not if. This is where proper monitoring and detection is crucial for not letting an incident develop into a full-blown breach. Whether home-based or outsources, a good intrusion detection system will help you know when your action is required.