15 Ways To Protect Your Business From A Cyber Attack!

DATALINK INTERACTIVE

Security Assessment

It's important to establish a baseline and to track progress on closing existing vulnerabilities.

Assessment Date:_____

Penetration Test Date:_____

Email Security

Secure your email. Most attacks originate through your email. We'll help you choose the package designed to reduce spam and your exposure to attacks.

Business | Advanced | Professional

Passwords and Policies

Apply security policies on your network. Limit USB drive usage, apply password complexity, enforce password rotation, screen timeouts, and logon hours

Apply Policies | Password Management

Security Updates

It's important to keep your systems up to date. Including Microsoft Windows and Office software. Also 3rd party software including Adobe, Java, and browsers.

Microsoft | 3rd Party

Security Awareness

Train your users – often! Teach them about data security, email attacks, data ownership, and your policies and procedures and randomly test for gaps.

Policies | Testing | Training

Endpoint Protection

The basics! Protect your endpoints against standard viruses and malware with managed software and DNS filtering. This is your first line of defense.

AV/Malware | DNS Filtering

Advanced Endpoint Detection & Response

Protect your endpoint data from advanced malware, viruses, and file-less and script based cyber attacks. And Ransomware with rollback technology.

Endpoint Detection & Response | File Integrity Monitor

SIEM/Log Management

(Security Incident & Event Management)

Use the power of big data and a 24/7/365 SOC to review all event and security logs to protect against threats and meet compliance needs.

30 Days | 90 Days | 365 Days

Dark Web Research

Knowing what passwords and accounts have been posed on the Dark Web allows you to proactively prevent a data breach or a ransomware attack.

Quarterly Review & Monitoring | Monthly Review & Monitoring

Mobile Device Security

Today's attacks attempt to steal credentials for access to your data any way they can. This includes tablets and phones. You can close this gap with MDS.

Company owned devices | BYOD devices and Policy

Multi-Factor Authentication

Utilize Multi-Factor Authentication whenever possible. Including on your network, company banking sites, and social media. It adds an additional layer even if your password is compromised.

Mobile phone push application | Token or FOB based

Encryption

Whenever its possible the goal is to encrypt company data at rest, in motion (think email and file sharing) and especially on mobile devices.

Mobile device | Endpoint | Server

Firewall

Turn on Web filtering and application aware filtering. Turn on Intrusion Prevention features. Send this log data to your managed SIEM. If your IT team doesn't know what these are, call today.

Application and web filtering | Intrusion Prevention

Backup

Whenever possible, implement encryption and follow the rule of 3. 3 copies of your data, Live, onsite backup, and offsite copies. Test your backups often, and if in doubt call us today.

Local backup with offsites | Local backups with offsites and virtual recovery

Cyber Insurance

If all else fails, protect your income and business with cyber damage and recovery insurance policies.