15 Ways To Protect Your Organization From A Cyber Attack

APPLIED CONNECTIVE TECHNOLOGIES

☐ 

Advanced Malware Protection

Prevent ransomware and other malware attacks with advanced endpoint security. Traditional antivirus has proven ineffective. Consider an advanced managed AI-driven solution monitored 24/7 by our SOC (security operations center). Don't just stop breaches—prevent them.

☐ 

Email Security

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce threats and your exposure to attacks on your staff via email.

☐ 

Passwords

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

☐ 

Security Awareness

Train your users often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

DID YOU KNOW?

$4.35M is the average cost of a data breach today

82% of data breaches were attributed to human error or negligence

97% of breaches could've been prevented with today's technology

☐ 

Advanced EDR

Take endpoint protection to another level. Endpoint Detection and Response (EDR) is your failsafe for threats that bypass firewall and endpoint security services. Discover known and unknown elements of an attack. Today's EDR solutions complement your advanced malware protection by protecting against file-less and script-based threats and will reduce investigation and remediation time after an incident.

☐ 

Multi-Factor Authentication

Utilize multi-factor authentication whenever you can, including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

☐ 

Patch Management

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

☐ 

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

☐ 

SIEM/Log Management & SOC

(Security Incident & Event Management and Security Operations Center)

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements. SOC is critical.

☐ 

DNS Protection

Block malicious websites and filter out harmful or inappropriate content. DNS filtering ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks. Agent- or firewall-based coverage options should be considered.

☐ 

Mobile Device Security

Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

☐ 

Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM, and if your IT team doesn't know what these things are, give us a call!

☐ 

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email), and especially on mobile devices.

☐ 

Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.