

# Protect your Business from a CYBERATTACK!



## Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?



## Spam Email

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



## Passwords & Policies

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



## Multi-Factor Authentication

Utilise Multi-factor Authentication whenever you can, including; on your network, banking websites, online stores and social media. It adds an additional layer of protection to ensure your accounts & data stay protected.

## Did you know?

**1 in 5** Small businesses will suffer a cyber attack this year.

**81%** of all breaches happen to small and medium sized businesses.

**97%** of breaches could have been prevented with today's technology.



## Advanced Endpoint Detection & Response

Protect your computers data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology protects against file-less and script-based threats and can roll back ransomware attacks.



## 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.



## Computer Updates

Keep Microsoft, Adobe, Java and other 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 leaked on the Dark Web will allow you to proactively prevent data breaches. We'll scan the Dark web and take action to protect your business from leaked accounts.



## SIEM/Log Management (Security Incident & Event Management)

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.



## Web Gateway Security

Internet Security is a race against time. Cloud-based security detects web and email threats as they emerge on the internet and blocks them on your network within seconds. Ensuring your users are always protected.



## Mobile Device Security

Today's cybercriminals attempt to steal data or access your network by way of your employees' phones and tablets. They are counting on you to neglect this part of your security, Mobile Device Security closes this gap.



## Firewall

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



## Encryption

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



## 3, 2, 1 Backup

Backup Local, Backup to the cloud, have an offline backup for each month of the year. Test your backups often. And if you do not know your business backup police or if they are working? Speak with us today!