# Advice and Guidance Around Cyber Security for SMEs

The following pages discuss several processes and technology solutions that organisations should implement to help protect them against a cyber attack or data loss.  Of course, nothing can be 100% guaranteed, but by adding layers of security and processes, you will vastly reduce the risk of becoming a victim of a cyber attack and the associated issues this causes.

# Passwords and Two Factor Authentication

Securing access to systems with a username and password has been commonplace for decades now. Known as single-factor authentication, the requirement of a username/password combination to allow access to a system is of course essential for information security within every organisation.

Every organisation should have a password policy in place to enforce specific requirements for length, complexity and history, but you should also publish guidance for users for their password hygiene.

This may include:

- How to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet)
- Not to choose common passwords — this could be implemented by technical means, using a password blacklist
- Not to use the same password anywhere else, at work or at home
- Where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
- If they may use password management software — if so, which software and how

A business may have several different applications or platforms, each with their own authentication systems, meaning employees must remember multiple username and passwords for these platforms. Alongside this, everyone now has multiple personal accounts for various services such as email, social media and online shopping.

Even with the appropriate guidance, it is well known that people will generally reuse passwords across multiple accounts; business and personal which of course creates a security concern. In addition, there has been widespread data breaches which have put millions of username/password combinations for sale on the dark web, which of course makes passwords much less secure and puts business systems at risk of attack.

With the huge shift to cloud computing over recent years, many organisations now have large parts of their IT infrastructure hosted within the cloud, making them very accessible. This accessibility brings additional security concerns as these cloud-based systems are prone to brute force attacks. The systems themselves are not necessarily insecure, but the use of weak passwords from their users has vastly increased successful brute force attempts and therefore data breaches.

To combat this, an additional layer of authentication security is required in the form of two factor authentication. Instead of trying to enforce better password hygiene practices amongst employees, adding an additional layer of authentication security in combination with their password provides a much stronger authentication system. This second form of authentication is generally in the form of something you have and may be a physical smart card or a USB security key, but more often, a code which generally has a shelf life of around 30 seconds. These codes can be delivered via physical tokens, or more commonly now, via a mobile app. Some apps even provide “push” technology where you simply click and Allow or Deny button from your phone.

Nowadays you will struggle to find a business or personal cloud platform that does not offer 2FA as part of its authentication platform. This is generally included at no extra cost as the cloud platform provider wants to ensure their environments are considered safe and secure and some will enforce 2FA is enabled.

# Email Security

Email is a core component of everyday working life within organisations and is a great way to communicate with anyone from around the globe. Email however is one of the main sources for an attacker to successfully compromise a network. Email attachments that contain malware and links that send you to a malware infested website are all common ways that an attacker will gain entry. There are also more and more sophisticated ways that attackers develop and use phishing techniques to socially engineer their way into a network.

There are of course ways in which you can secure your email environment to reduce the likelihood of your network being compromised.

## Email Security Solutions

For many years, business have implemented anti-spam technology to help protect against email users receiving large amounts of unwanted or spam email. These were an essential component to filter out all the rubbish you didn't want to see and would generally use list, key word search and heuristic search to filter out the spam. There would then generally be anti-virus engines built into these solutions to protect against virus infections to the email environment.

Many businesses these days will use a completely hosted email solution such as Microsoft 365 or Google G Suite. As a standard, these all have built in traditional spam filtering as part of that service, giving you the minimum email security any business should have in place. There are then additional subscription services that can be purchased to further extend this.

Implementing additional email protection solutions that provide these types of protection is something all business should undertake:

- Use AI to learn how people communicate within your organisation and therefore can stop spear phishing attacks
- Scans the content of attachments to ensure no malware is present
- Checks links within emails to ensure they're legitimate and are not redirecting to malicious websites

## Awareness Training

As well as using technology to help prevent an attacker from successfully compromising your network, all users should be provided with Cyber Security awareness training to help them understand how email based threats operate and how they can be avoided. As discussed, phishing techniques have become very sophisticated using AI to mimic how people communicate with their colleagues, clients and suppliers and as these emails can be received from legitimate, registered email domains, everyone needs to have a good understanding of what to look for.

Training employees how to identify and handle suspicious email, including how to report this content to the relevant IT teams within your organisation. There are now many platforms that provide this type of service, generally delivered via video training in bite size chunks so that employees can easily understand and re-visit if required. It should be noted that any training should not be a one-off and should be undertaken on a regular basis to ensure everyone always has it in their mind.

In addition, phishing simulation tools can be used to create test content that an organisation can send to all employees to see how they respond once they've had their training and identify any individuals that may need some additional training.

## Email Reputation

In order to protect an organisations email domain reputation, there are several measures that should be put into place to help with this. These are fairly simple measures that provide controls and validation for a recipient mail server ensuring they know that email received is genuine and that helps protect email senders and recipients from spam, spoofing, and phishing, alongside protection the reputation of your email domain. There are three main standards of protection that be put into place:

- **SPF** (Sender Policy Framework). This is a DNS record added for each email domain used and defines a list of authorised email servers for the domain, so that receiving email servers can check the source of incoming email against the SPF list.
- **DKIM** (Domain Keys Identified Mail). DKIM will sign emails to prove they came from your organisation. It authenticates email is genuine via a digital signature and makes it easier to identify spoofed emails. The sending email server signs the email with the a private key and the receiving mail server uses the public key in the to verify the signature.
- **DMARC** (Domain-based Message Authentication, Reporting, and Conformance). This allows an organisation to publish a policy that defines its email authentication practices and provides instructions to receiving mail servers for how to enforce them. Both SPF and DKIM are required to implement DMARC.

# Endpoint Protection

Protecting endpoints with an anti-virus solution has been a requirement for decades and we're all used to seeing anti-virus installed to our devices. Traditional anti-virus clients were signature based, meaning that they would monitor for known virus types and behaviours, with these signatures being regularly updated to ensure protection against new and emerging threats.

In modern times, there are many more sophisticated threats that can cause huge disruption, system downtime and data loss. A lot of these may use legitimate processes or actions in a malicious way. For example, we've all heard of crypto-locker which uses the legitimate action of encryption, but in a malicious way to lock you out of your data.

New technology has emerged in recent times to extend what a traditional anti-virus provides. Know as an EDR (Endpoint Detection and Response), this will look at behaviours and activity on endpoints and record these to a central repository for additional analysis and investigation. The EDR will stop suspicious processes from executing or stop legitimate processes running if the EDR detects they are being use maliciously.

This additional later of protection will become the norm in the not so distant future and there are already many security software companies with EDR offerings.

# Cyber Essentials

The Cyber Essentials scheme is a framework devised by the government to adopt good practice in information security and contains a set of security standards which organisations can be assessed and certified against.

The framework identifies the security controls that an organisation must have in place in order to meet the requirements of Cyber Essentials and be awarded the accreditation. By achieving this, you will have confidence that data is kept safe and that you're protecting your organisation from the risk of internet based threats.

The scheme focuses on the following five essential mitigation strategies:

- Boundary Firewalls and Internet Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management

By completing this accreditation, it will provide your clients with the assurance that you're practicing robust Cyber Security measures to mitigate against data loss or cyber-attacks. It will also demonstrate that your data is adequately protected and that they take cyber security seriously.