redsquid.

Cyber Security **Check List.**

Overview.

The threat landscapee has changed dramatically over the last years, and the cyber criminals are now tagerting small and large businesses alike.

Although, no business can ever be 100% secure, there is a lot you can do to stay as safe as possible.

In this list we have included the cyber security policies that any business should follow, split between the basics, the advanced and Microsoft 365 security.

By following these, your business will be able to operate safely, while protecting your information and data.

Let’s get started!

The Basics.

Patch Management

Patch management refers to the installation of updates to core operating systems and common software. Core operating systems include but are not limited to Microsoft Windows, Windows Server and Apple macOS (OSX). Common software includes things like Acrobat Reader, Google Chrome and Microsoft Office. When we are talking about security, we focus on the timely manner in which security patches are rolled out. It is recommended that security patches are rolled out within 14 days of release. A good patch management solution will ensure that patches are rolled out automatically within this time frame, and if there are errors, these are proactively resolved by your managed service provider.

Support OS

Every device has an operating system, or OS for short. Once a devices operating system is considered end of life by the vendor, security updates are no longer being released. This means that devices that have reached 'end of life' are a big security to your organisation. Therefore, you must ensure that these devices are upgraded, updated or decommissioned before they become end of life.

Next Generation Antivirus

Antivirus is essential for all Windows endpoints, and every business should have a business-grade, centrally managed antivirus solution installed. There is some debate as to whether Apple OSX, iOS (iPhones) and Android require antivirus, and this decision will ultimately depend on your business strategy, operations and attitude towards security.

Antivirus software has undergone heavy development over the last 36 months, to allow it to cope with modern threats. As a result, a new type of antivirus has emerged, which has been coined 'next-generation'. Over time this will eventually become the standard.
Traditional antivirus works by comparing programs and process to a signature file, that is updated every day. If a program or process matches one that is in the antivirus solutions signature file, then the item is blocked from running.
How is next-generation antivirus different? Next-generation antivirus goes a few steps further. A program or process is compared to the signature file and a cloud database, containing real-time data from around the world. Not only that, but most next-generation antivirus solutions include application white listing. This applies a principle of "guilty until proven innocent". If a program or process is not recognised and not included in the signature file, it will be blocked.

This provides a high level of protection which is recommended in today's environment.

The Basics.

Firmware

Firmware is the name given to the software that is stored on a hardware device. Every piece of technology has firmware. Firmware can be updated to improve performance, reliability and security. Therefore, firmware on key equipment must be kept up to date. Key equipment includes but is not limited to routers, firewalls, servers, clients computers, wireless access points, printers and even IoT devices.
Typically, firmware updates cannot be automated and will require an IT administrator to apply it safely.

Remote Access

Remote access is now an essential part of a businesses IT agility solution. Traditional VPNs (Virtual Private Networks) were used to facilitate remote access, but modern solutions, such as M365 do not require a VPN to be initiated. Whatever your remote access method, ensure that for a VPN L2TP or SSL is in use, and for direct connections, SSL is applied. For any questions about remote access, your managed service provider will be able to provide you with information for the best solution for your business needs.

Network Publishing

Network publishing (also described as port forwarding or IP routing) refers to the access of an on-premise service via the internet. If you have an on-premise server and this is accessed remotely, then you have network publishing in place. There are many other examples of network publishing, such as remote access to firewalls, routers, switches and client computers. Ensure that your managed service provider reviews your network publishing regularly and that only necessary services are published, and where possible, restricted by user, location or IP address.

Password Policy

Password policies should be enforced by your systems and always following your written company policies.
Many user don't realise the importance of having safe passwords. Too often we find that short passwords including birthdays of children's names are still a favourite! But did you know that a password in 8 or less characters can be hacked in less than a minute?
Users should be trained to understand what constitutes a secure password and what does not. There is some debate over the specifics of a complex password, but some guidelines are 8 characters minimum, contains numbers, special characters and no complete dictionary words or names. Finally, we will not recommend regularly forced password resets (password expiry), but the reasons behind this are outside the scope of this checklist.

The Basics.

Usernames

Many devices and operating systems come installed with an easily guessable username such as admin or administrator. As convenient as it might be, these are simply just too insecure to use. A policy should be in place to change these usernames before the device is implemented. Furthermore, usernames for individuals should never be in a first name format. A good policy is to have a First name, Surname or email address format. For shared accounts such as sales, scanner or hotdesk, a company name prefix is recommended, such as CompanynameSales.

User Purge

You should regularly review the users who have access to your systems and disable accounts that no longer require access.

SPF/Reverse DNS/DMARC/DKIM

These technologies help ensure that your email domain is not spoofed. Without these technologies in place, it is easy for a threat actor to send an email from your company's email domain name. Check with your managed service provider that these technologies are in place for all domain names.

Email Forwards

When a threat actor gains access to a mailbox, they often put a rule in place to BCC themselves into all incoming and outgoing email communication. These rules are discrete and not often noticed by the managed service provider or end-user. These rules allow the threat actor to run a password reset against the account or wait for an opportunity to make money or infect the system. Ask your managed service provider to disable the ability for end-users to set their own automatic forwards and have this functionality restricted to IT administrators.

Review File Access

Regularly review the permissions on any location that stores files. This could be network shares on a server or document libraries and team sites within M365.

The Basics.

Wireless

When connecting to a wireless network, different security technologies are running in the background. Therefore, you should ask your managed service provider to ensure that your wireless access points use WPA2 technology for full security.

Removeable Data Storage and Auto Run

Data exfiltration refers to data leaving the business IT estate, when it was not supposed to. Where your business' operations allow it, always ensure that removable data storage, and autorun of removable storage, is blocked.

Screen Locking

After a period of inactivity, your computer should display the password screen (lock screen) ask for a password to continue operating. It is recommended that screens lock after 10 minutes of inactivity. This helps prevents unauthorised physical access.

Physical Security

After a period of inactivity, your computer should display the password screen (lock screen) asking for a password to continue operating. It is recommended that screens lock after maximum 10 minutes of inactivity. This helps prevents unauthorised physical access to your devices. Depending on where you work from the inactivity time should be even shorter, eg. if you are working out of public or shared work environments.

MFA (Multi-Factor Authentication)

One-factor authentication is something that a person knows, such as a password. Two-factor authentication is something that the person knows and something they have with them, such as a smartphone. Three-factor authentication is something that they know, something they have on them, and something that is part of them, such as a fingerprint or retina scan. Multifactor authentication refers to technologies that do not just require a password. A secure business uses 2FA or MFA at a minimum. M365 makes MFA easy and transparent to the user. Implementing MFA gives a significant increase in security, check with your managed service provider to see if MFA is implemented.

The Basics.

Endpoint Encryption

The term encryption is used broadly and means different thing depending on the hardware, software and process that it applieds to. Broadly speaking, encryption scrambles data so that only the intended recipient can read it. When we refer to endpoint encryption, we describe the process by which data on a hard drive cannot be accessed without a password or decryption key. Without encryption applied it is very easy to physically remove the hard drive from any device (computer, server, smart phone or tablet) and without knowing the password, access the data. Most smartphones and tablets are encrypted by default but Windows and Apply clients and servers are not. Ensure that Windows clients/servers are protected with Microsoft BitLocker and Apple OSX devices protected with File Vault. These technologies are free but your managed service provider may charge a fee for monitoring and storage of recovery keys.

Perimeter Firewall

A firewall monitors traffic entering and leaving a device or network. Most modern devices such as Windows 10, OSX or routers have a basic firewall built-in. It is recommended that your business networks have a hardware firewall at their perimeter. If you have on-premise servers, this is essential. But having a hardware firewall is not enough, security services must be activated on the device. Different firewall vendors refer to security services with different names, but broadly speaking, active security services allow the firewall to be updated each day about new security threats. Despite what a managed provider tells you, a firewall without security services enabled is only acting as a router.

Web Filtering

Web filtering is a technology that discriminates against websites an end-user accesses. Web filtering is now a requirement of passing Cyber Essentials. There are two broad types of web filter. The first type of filter will block the suspect sites such as illegal, unethical and inappropriate. Most antivirus software will stop these types of site. The second is a filter that will block a legitimate website if it has been compromised. These filters are often called a Web DNS filter, and a monthly subscription is required. Most businesses do not adopt a DNS filter due to cost, but I suspect it will become as standard as running AV over the next few years.

The Basics.

End-User Security Training

The final defence in your security arsenal is a properly trained end user. Using online bite-sized videos, your team can be well-trained cost-effectively.

Backups

Technically, backups are not a security feature. However, they are a critical part of your IT estate and provide business owners peace of mind from all manner of threats, security, and otherwise. Ensure that your backup is checked daily, restores tested at least weekly, and data is stored in an offsite location. It is also important to understand the security in place to protect your data in the offsite location.

Check List.

- □ Patch Management
- □ Support OS
- □ Next Generation Antivirus
- □ Firmware
- □ Remote Access
- □ Network Publishing
- □ Password Policy
- □ Usernames
- □ User Purge
- □ SPF/Reverse DNS/DMARC/DKIM
- □ Email Forward
- □ Review File Access
- □ Wireless
- □ Removeable Data Storage And Auto Run
- □ Screen Locking
- □ Physical Security
- □ MFA (Multi Factor Authentication)
- □ Endpoint Encryption
- □ Perimeter Firewall
- □ Web Filtering
- □ End-User Security Training
- □ Backups

The Advanced.

Cyber Essentials

Cyber Essentials is a government-backed scheme that recognises a business for meeting best practices security standards. It is more common place now for prospects to ask if a business has Cyber Essentials, and some companies won't trade with you if you don't have this.

Offboarding Policy

An offboarding policy is essentially a checklist of items that need to be actioned when an employee leaves the business. From a security perspective, this will include disabling the user from a server or cloud access. But there are typically many other access rights that need disabling. Ensure that you have a comprehensive offboarding policy that revokes user access to all systems.

GDPR Policy

The fines for not being GDPR compliant can be significant. Broadly speaking GDPR advises that you must take "reasonable measures" to secure personal (PII) data. How you achieve this is outside the scope of this document, but we recommend seeking advice from a GDPR specialist. This advice will often result in having a data map, GDPR policy and GDPR training for your employees.

Dark Web Scanning

Many of the breaches we have seen over the last five years have been caused by a threat actor using someone's username and password to gain access to a system. Usernames, passwords and personal data are continuously bought and sold on the dark web. It is now possible to scan the dark web for information about your companies domain name. The scary thing is, We are yet to run a scan for a business, where it picks up zero results. Ensure that you monitor the dark web for breaches or run annual dark web scans.

The Advanced.

Attack Simulations

We run attack simulations to see how end-users respond to certain types of security threats. These results are recorded and used as a training tool. We never advise this to be used to single out individuals, but only to gauge a businesses level of preparation for a real security threat. A typical attack simulation would be to send users an email, phishing for their password. The attack simulation can record who opened the email, who clicked the link and who provided credentials. We recommended running attack simulations twice annually.

Cyber Insurance

Over the next three years, cyber insurance will become as common for businesses as company car insurance! Depending on the type of insurance, this protection offers financial compensation for damage caused by the breach and for any ICO fines. In most cases, you also get access to a cyber response team if a breach takes place. You can opt-in for free cyber insurance when you pass your cyber essentials certification.

BYOD

BYOD or "Bring your own device" presents a big security threat. It is commonplace for remote works to use personal devices that store company data. It's difficult for a business to ensure that these personal devices conform to the security standards that they need. The most secure solution is to prevent access to systems from personal devices, or have a strict policy that governs the types of devices that can connect.

Check List.

- □ Cyber Essentials
- □ Offboarding Policy
- □ GDPR Policy
- □ Dark Web Scanning
- □ Attack Simulations
- □ Cyber Insurance
- □ BYOD

Microsoft 365 Security.

M365 provides hundreds of security features that other cloud solutions and on-premise servers do not. Some of these features have already been listed earlier in this document.
In this section, we want to focus on some of the lesser-known features that can help keep your business secure.

*Some of these features require an additional license.

DLP

DLP or Data Loss Prevention monitors data leaving your M365 tenancy via any means and checks if the data is sensitive, confidential or personal. Users can be warned that they are breaking company rules, and that the communication needs to be authorised by a manager. The feature is in its infancy, but greatly aids in GDPR compliance.

IRM

IRM or Information Rights Management provides an extremely high level of security but should be used sparingly. Once enabled on a SharePoint site, IRM will encrypt all supported file types. This means that if a user copies one of these files to a personal device and then leaves the company, they will no longer be able to open the file.

Intune/Conditional Access/MDM

One of the advantages of a cloud solution, such as M365 is that it can be accessed from any location and on any device. While improving operations, this out of the box setup presents a security challenge. By combining Intune, conditional access and MDM policies, we can specify which devices, locations and users can access M365, and the type of access that they have. For example, users can access from their personal device but are prevented from downloading and syncing data.

Microsoft 365 Security.

Email Encryption

M365 offers native email encryption that the user can very easily apply. Once applied, a message can have forwards and edits restricted, or prevent the message from being sent outside the organisation.

ATP

ATP or Advanced Threat Protection refers to a broad set of technologies across the M365 platform. Think of it like antivirus for your cloud. Just enabling ATP is not enough; to leverage its full set of features, your managed service provider will need to configure the ATP services correctly and have users trained on them.

Check List.

- □ DLP
- □ IRM
- □ Intune / Conditional Access / MDM
- □ Email Encryption
- □ ATP

redsquid.

— MAKING A DIFFERENCE —