Cyber Security

Checklist for SMEs

One of the biggest mistakes smaller organisations make is to assume that because their turnover is modest, or their operation is small, cyber criminals will go elsewhere. However, ransomware attackers – are still the biggest threat statistically – as are interested in SMEs and larger companies even if the headlines tend to focus on better-known victims.

How can small businesses minimise their chances of ending up as a statistic?

iso systems UK
Concept to Certification

Introduction

Cyber criminals know that if the choice is between a complete shutdown of an organisation's systems or getting their network and computers back within their control, every business manager will choose the latter. It's just a question of squeezing the maximum ransom, or data assets, out of the victim.

So how can small businesses minimise their chances of ending up as a statistic? What follows is a short checklist of issues that SMEs should address.

Checklist

1. Start with employees

The first line of vulnerability – and defence – is an organisation's employees. One of the most common ways malware gets a foothold is when someone opens an infected document or clicks on a link. It sounds like mundane advice, but anything that improves the awareness of an employee reduces the chances of being compromised.

How can this be achieved?

The conventional answer is anti-phishing training, also known as *"teaching employees not to trust anything they receive by email".*

Undoubtedly, this sort of training is worth it if it's repeated often enough. But remember not to ignore other security-critical issues, such as the way employees use passwords, so that they are always strong enough and never re-used.

2. Detect attacks

Most SMEs rely on an endpoint security product or antivirus to pick up an issue. It's a good starting point, but it must be running on *all* endpoints, including servers and mobile devices, with central alerting turned on.

However, even the best antivirus can't detect all attacks, or at least detect them before damage is done. For that reason, it's worth looking for endpoint security that employs some form of application micro-isolation. If a computer becomes infected, how easy would it be to roll back to a clean state?

Continued...

3. Managed Detection and Response (MDR)

Even when attacks are detected, it’s often difficult to respond to them before the problem has spread. This can happen within seconds. For that reason, it’s worth looking at an MDR service supplied by a third-party specialist. This is basically threat detection integrated with rapid response, remediation and, if necessary, forensic incident investigation. Effectively, it’s ‘hand-holding for a subscription fee’ which will often prove to be money well spent.

4. Test defences, including backup

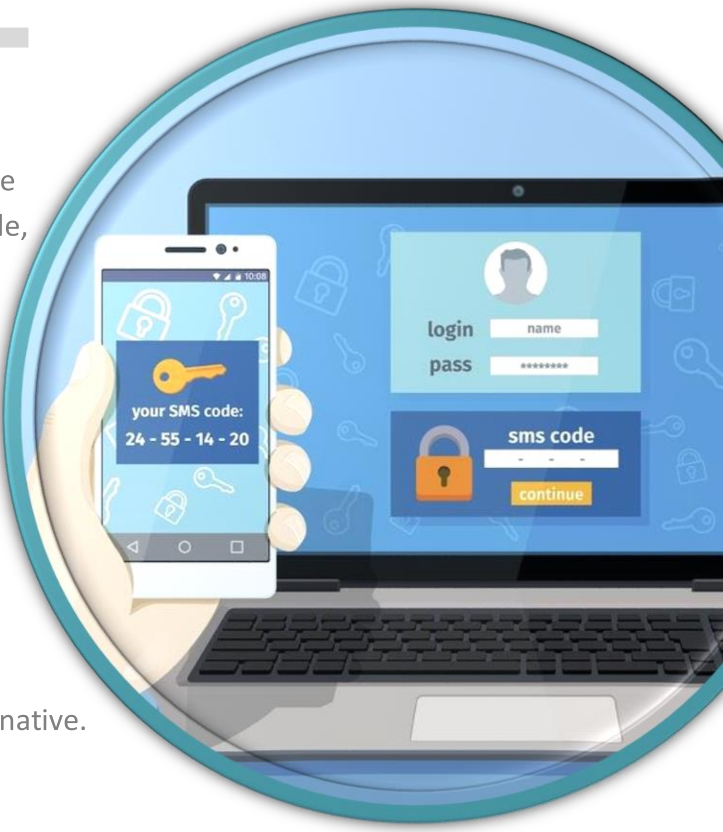
By far the biggest problem in SME cyber security is that companies don’t know what their vulnerabilities and weaknesses are because they’ve never looked for them. There are two ways to approach this, the first of which is to do an inventory of your assets, which means not only physical devices but important admin logins, applications and connectivity. What technology do the organisations depend on and where is the critical data?

A second approach is to carry out a basic penetration test, which is where an external company of security testers tries to compromise the network without causing any damage. It costs money but will spot the bigger weaknesses that need immediate fixing as well as the smaller ones that can be addressed over time. Every SME will have backups, but would this be sufficient to stop a ransomware attack? Ransomware always targets backups. Penetration tests can be a good way to look for weaknesses in this layer of defence.

Continued...

5. Turn on multi-factor authentication

These days, password attacks mean that no password is reliable without an additional factor such as an app-generated passcode, push authentication or a hardware token. It's sometimes said that there are now so many technologies that can be used for multi-factor authentication that it can become confusing. That's true but don't let it put you off – turning on multi-factor authentication is the simplest upgrade any SME can make to their security.



Beware though – some types of authentication are obsolete despite their continuing widespread use. A good example is SMS text codes, which are vulnerable to interception or social engineering and are not recommended unless there is no alternative.

6. Remember email security

Email is not only one of the biggest security vulnerabilities facing SMEs it's also the most confusing, taking in different older, standalone SMTP, POP, and MIME servers as well as more recent Security-as-a-Service (SaaS) which integrates with Microsoft 365 or Google Workspace. With the former, SMEs do the hard work themselves at a relatively low cost while the latter offers more security and control for a monthly subscription. The latter offers a lot of security features such as message encryption, malicious email filtering, and even the ability to detect hijacked email accounts. Email security can be complex – buying email security as a specific service hides this.

Continued...

7. Secure privileged servers

You'll hear the phrase "*attack surface"* a lot in the current cyber security discussion. The principle behind it is simple: the larger the target, the more there is to go wrong.

This includes specialised types of servers used for Virtual Private Networks (VPNs) and Remote Desktop Protocol (RDP).

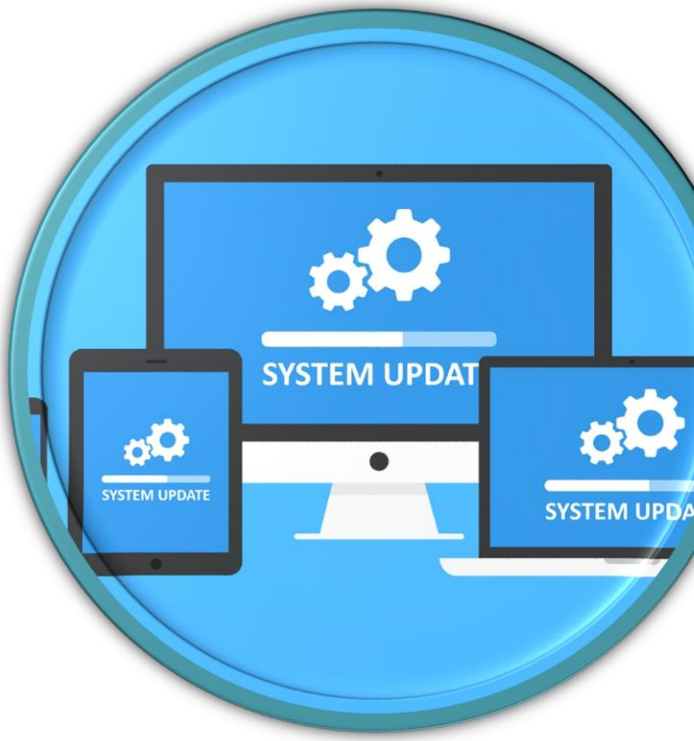
Anything with an external login should be treated as risky, for example, admin interfaces for any of these services, including partners and service companies. The minimum for any of these accounts should be multi-factor authentication, preferably using a hardware token. A case in point is Windows domain servers. If one of these is compromised, the effects can be devastating because the attackers can potentially use that to encrypt and distribute their malware across the network using group policies while locking out the defenders.

8. Segment the network

If attackers get inside the network, the first thing they look to do is look to move sideways to other parts of the network. This is often done manually using remote access Trojans (RATs) or legitimate security tools. Defending against this is done by dividing the network into subnets with privileges required to move between one and the other. In some cases, this can even more network isolation for specific systems such as PCs used to initiate bank transfers. Another area where segmentation helps is protecting backups. These are the first line of defence against ransomware but only work if the attackers haven't got to them first.

Continued...

9. Patch vulnerabilities



Patch management has been best practice for years but it's not always as simple as it looks. Mainly, there's just a lot to keep on top of and standalone scanners can be complex to use.

SMEs have two options, the most expensive of which is to ask a managed security service provider (MSSP) to carry out this service while noticing what this does and doesn't cover (a Microsoft 365 subscription will look after the Microsoft-specific issues). The second is to use a dedicated SME vulnerability scanning service.

10. Ditch old equipment

SMEs are regularly nagged to ditch old or legacy equipment and software but it's rarely as simple as that. Some older systems can't easily be replaced because there's no easy or affordable path from old to new.

A second problem is working out what legacy means. The simplest definition is whether the equipment is supported or not. If it's not, it won't be getting security updates and that means it is a liability. Another definition of old is equipment that was designed around obsolete security assumptions. You see this a lot with the first-generation Internet of Things (IoT) devices – security webcams and wireless routers are the prime examples – which might be accessible from the Internet.

If you are looking to secure your business from the risk of cyber attacks, **ISO 27001** can help you put processes in place to reduce your risk and the government-backed schemes Cyber Essentials and Cyber Essentials Plus is also suitable for the smaller SME.

Should you require further information or support you can contact us in a variety of ways:

Email us via services@isosystems.org
Call us on 01325 778352 / 07791 425011
Contact us via our website

Follow us on social media

Search: ISO SYSTEMS UK