UNDERSTANDING & DEFENDING:

The Top 4 Cyber Threats to UK SMEs

FOXTECH

Overview

Businesses in the UK are subject to a continuous bombardment of cyberattacks. Opportunistic criminals are continuously searching for organisations that do not have the Cyber Essentials in place, regardless of their size. This is why 1 in 3 UK businesses report some kind of attack or breach per year, and half of those find it impacted their business operations somehow.

From what we read in the news and see in the movies, we might imagine cybercriminals are hackers in hoodies with ninja skills or secretive nation-state cyber armies. This might lead us to think that our company is not under much threat if we don't have nation-state-level secrets or the control system for a nuclear bunker. However, this really isn't the case.

Who are the Hackers?

There is a complex interconnected web of organised cyber criminals trading in personal data and access to servers and botnets. One crime gang may be running massive phishing campaigns to hoover up login credentials and selling these for a few dollars each.

Other teams might buy these up to run targeted Business Email Compromise attacks – following your business processes to fool you into diverting a payment to an attacker's bank account. Yet others are scanning the internet for vulnerable servers, installing botnet malware and selling access for a couple of dollars per machine. Others rent these servers to run Denial of Service campaigns – where a week-long DDoS attack can be had for $500. You can see from this that you're under attack whether you think you have interesting data or not.

Your credentials, your servers and your customer's personal data all have value – the question is just how much. If you're an easy target, your data will be floating around on the black market, and your server may be breached – just for the $2 a botnet herder can get to add it to their network.

Attack Methodologies

The most common cyberattacks are:

- Phishing, **83%**
- Use of stolen credentials or impersonation **27%**
- Scanning and exploitation,
- Ransomware or malware **13%**

While the proportion of companies affected by each of these varies depending on who you ask, these are invariably the top four most common ways businesses' IT systems are breached.

Phishing

> "Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). "
>
> **UK National Cyber Security Centre.**

Phishing is seriously common. Many people will receive phishing emails every month, which can be extremely convincing, even to security professionals who deal with these every day. While most phishing emails go ignored, around 3.6% of users are still sucked in on a typical phishing campaign [3]. It is therefore no surprise that around 1 in 4 UK businesses suffer some kind of Phishing attack each year, and 1 in 3 GDPR notifications to the ICO are of this nature.

Defending Phishing

Email Filtering

Deploy robust email filtering to block suspicious emails, reducing the chances of phishing attacks reaching users.

Use Anti-Spoofing Measures

Implement DMARC, SPF, and DKIM to validate emails, helping in preventing spoofed messages from being delivered to users.

Security Awareness Training

Educate users through regular training on recognizing and reporting fraudulent messages, enhancing their ability to identify phishing attempts and reduce the chances of phishing being successful.

Access Filtering

Filter access to malicious websites to reduce the chances of users entering credentials on phishing sites.

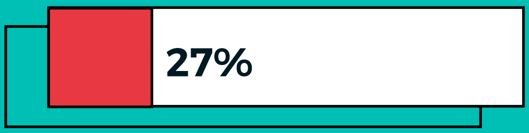
Security Monitoring

Implement continuous security monitoring to detect and alert on suspicious activities and anomalies swiftly, enabling immediate response to potential phishing attacks and mitigating risks.

Incident Response Plan

Have a structured response plan in place to act swiftly and efficiently when phishing incidents occur, minimizing potential damage.

Stolen Credentials



It can't have escaped your notice that many websites and online services need you to sign-up with an email address and password. Also – shocker – some of these get breached from time to time. When this happens, the user databases, complete with thousands of email addresses and possibly passwords, get sold on the dark web.

Now, a good website stores only a non-reversible "hash" of your password that makes it easy to check if you supplied the correct password when you log in, but rather hard to turn the hash back into the original password. In this case, it should be decades before the cybercrooks have cracked that password that has been shared with your gmail account, random online shop and social media accounts.

However, many sites do not do this correctly – in which case the crooks now have your email address and your favourite password; and will happily try that combination on any sites they can find.If you want a sobering experience – visit **https://haveibeenpwned.com/** and enter your email address.

You'll discover how many data breaches your email address has been found in. Now think back – did you use the same password in any of those sites as you use now? If yes, people will try those credentials in anything they can find – corporate email servers, your LinkedIn account – that VPN you set up but haven't used in ages.
You get the idea.

Defending Credential Theft

Use a Password Manager

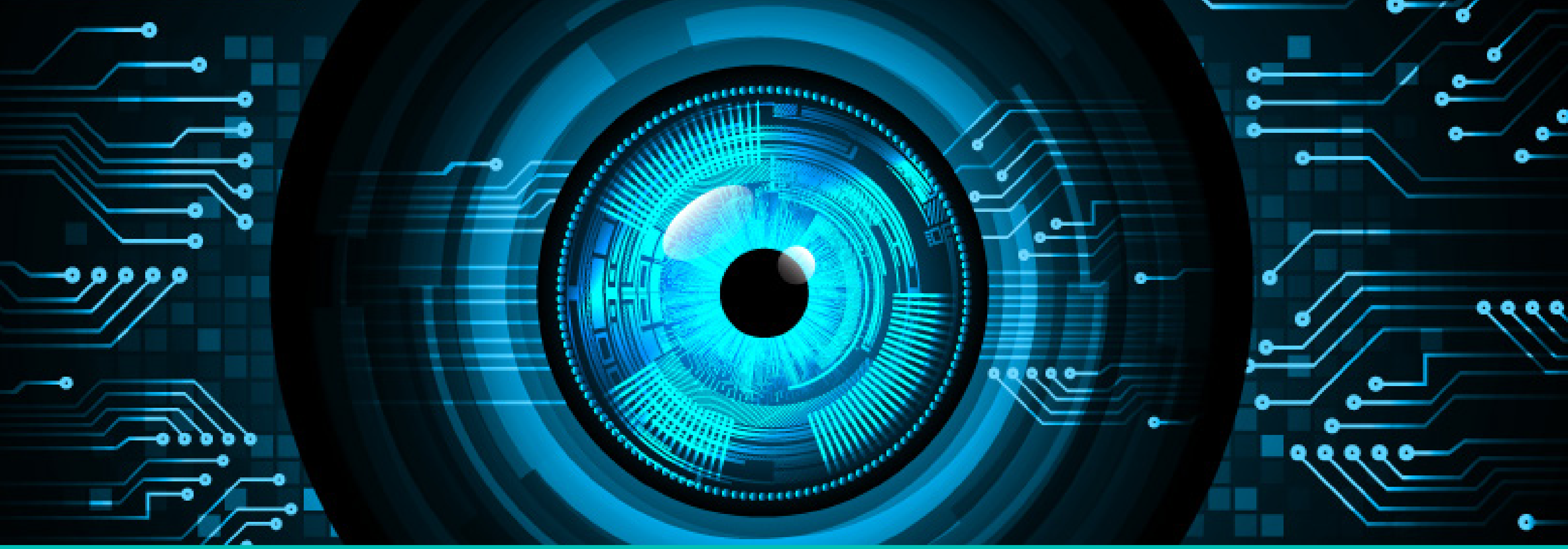
Password managers securely store and generate unique, complex passwords. This reduces risk of credential theft and reduces the impact should it occur.

Enable 2-Factor Authentication

Requiring two forms of identification adds an extra layer of security, protecting against unauthorised access even if passwords are compromised.

Monitor Your Systems

Regular system monitoring and alerts for suspicious activity allow quick identification and defence of potential security threats.



Scanning and Exploitation

13%

The internet is like the wild west – except on the internet, the Cowboys can knock on the door of everyone in the world in about 45 minutes.[5] This means that anything that is accessible from the general internet will receive a fairly continuous stream of attacks and probes for vulnerabilities.

While you might think that keeping up with these threats is a hopeless task – the good news for defenders is that the internet has a lot of easy pickings.

According to IBM [6] threat intelligence report, 8 of the top 10 most exploited vulnerabilities in 2020 had been fixed by the software vendor over a year ago.   This says that if you are prompt at installing updates, you can bat away most attacks.

Defending Exploits

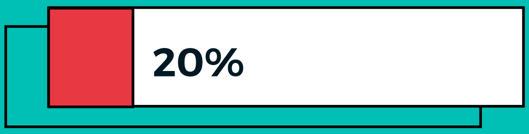
Minimise Internet Attack Surface

Use firewalls to ensure that systems not requiring access from the internet remain inaccessible. This significantly reduces the risk of these being exploited. Verify firewalls are working as intended with regular penetration tests and use open-source intelligence sources to discover “shadow IT” and manage the cyberrisk that creates.

Patch promptly

An effective vulnerability management programme should assure that updates are being promptly installed, especially to internet-accessible systems. Apply patches ensures that well-known vulnerabilities are addressed, reducing the likelihood of exploitation.

Ransomware



Ransomware features in about 1 in 5 cyber incidents. [2,6] In this attack type, the lucky recipient powers on their laptop to be greeted with a message stating that all of the data on their system has been encrypted. And, you can get the decryption key for an annoyingly plausible $80,000. And, for the less lucky, all their work colleagues also get the same message.

This can be more than an annoyance. Even if you have good backups – cleaning up after ransomware is time-consuming and requires careful attention to detail to avoid re-infection. An average company's IT will be down for 23 days during the clean-up.

If losing access to your data wasn't enough, these days, ransomware gangs favour the double punch in the face of encrypting your data and threatening to publish it to the world if you don't pay up.

Defending Ransomware

Protect Admin Interfaces

Ensure that administrative interfaces, like Windows Remote Desktop, are not accessible from the internet unless absolutely necessary to avoid unauthorized access.

Take and Test Backups

Regularly back up essential data to quickly restore systems and avoid data loss in the event of a ransomware attack. Make sure these are tested, so that you know they will work in the event that they are needed.

Use Anti-Virus

Implementing anti-virus on email and workstations is crucial for detecting and removing malicious software, preventing ransomware from infiltrating and compromising the system.

Conclusion

Anyone in IT knows that things often do not go to plan. Therefore, Independent Monitoring, Verification, and Assurance are vital components of any cybersecurity strategy.

Together, these give you the confidence that the controls you think you have are working, and help you respond quickly when mishaps occur.

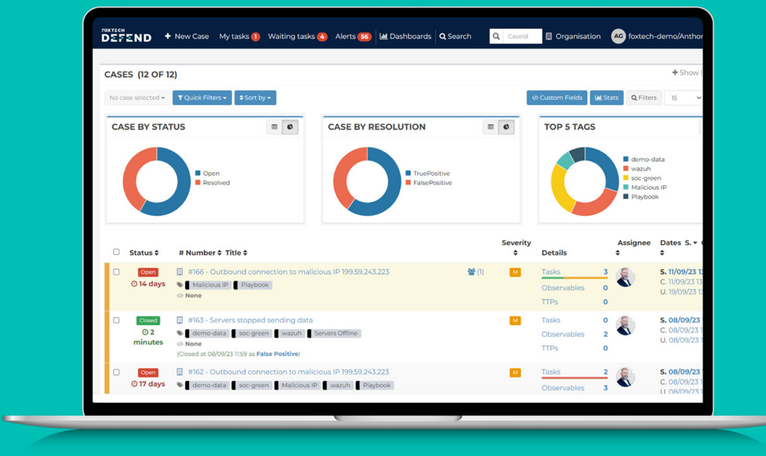
FoxTech Defend is not a tool
It is a Solution

FOXTECH DEFEND

In a rapidly evolving cybersecurity landscape, choosing the right partner to defend your digital assets is crucial. **FoxTech Defend** stands out, marrying cutting-edge **SIEM** and **XDR** technologies with our team of dedicated **UK based cybersecurity experts** working tirelessly to secure your digital assets.

More than just a log and alert tool, we actively shield your business from threats and continually customise Defend so it is tailor-made for your business, ensuring optimal protection.

Our team does more than just defend you; they're also directly accessible to support you, ready to assist with any remediation issues you might face.



CASES (12 OF 12)

☐	Status	# Number Title		Severity	Details	Assignee	Dates S.
☐	Open 14 days	#166 - Outbound connection to malicious IP 199.59.243.223 Malicious IP Playbook None	(1)	M	Tasks 3 Observables 0 TTPs 0		S. 11/09/23 1 C. 11/09/23 13 U. 19/09/23 13
☐	Closed 2 minutes	#163 - Servers stopped sending data demo-data soc-green wazuh Servers Offline None (Closed at 08/09/23 11:59 as **False Positive**)		M	Tasks 0 Observables 2 TTPs 0		S. 08/09/23 C. 08/09/23 U. 08/09/23
☐	Open 17 days	#162 - Outbound connection to malicious IP 199.59.243.223 demo-data soc-green Malicious IP wazuh Playbook		M	Tasks 2 Observables 3		S. 08/09/23 C. 08/09/23 U. 08/09/23

Automated Vulnerability Management

"Reduce your cybersecurity risk by proactively managing vulnerabilities"

FOXTECH ASSURE

Fixed Price
Penetration Testing

FOXTECH VERIFY

References

1 DCMS Cyber Security Breaches survey 2021

2 ICO Statistics

3 Verizon 2020 DBIR

4 Privacy Affairs Dark web pricing
https://www.privacyaffairs.com/dark-web-price-index-2021/

5 With a Gb internet connection, you can do a simple scan of every IP address on the entire internet in about 45 minutes!

6 IBM X-Force 2021 Threat Intelligence Index

7 Coveware ransomware report
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound