fitzrovia

DEEP DIVE:

The Most Common Cybersecurity Attacks

The threats your business faces, are changing.

As businesses become increasingly reliant on digital and cloud technologies, the need for watertight cybersecurity strategy becomes ever more apparent.

Over the past year – over 80% of UK businesses fell victim to successful cyber-attacks. By exploiting the poorly adapted work practices and lack of employee awareness ushered in by COVID-19 - cybercriminal activity increased by almost 600%.

At the mercy of the pandemic, many organisations were forced into adopting unprecedented workplace policies, procedures and systems to meet the needs of government guidance and employee wellbeing. But with many now splitting time between the office and home working, businesses are again having to reimagine the way their business operates.

While this has been beneficial in encouraging strong cloud adoption, the move has further reiterated the increasing importance of adequate cybersecurity. For without strong cybersecurity, criminals can further exploit new vulnerabilities in businesses' cyber infrastructure.

With reports showing that as much as 74% of companies intend to permanently shift to hybrid working, it becomes essential to protect against the new and prevalent cybersecurity attacks.

It's predicted that over the coming years, businesses will move towards dedicated cybersecurity teams that solely focus on their organisations' security needs. But as cybercriminals continue to adapt to ever-changing digital landscapes, businesses have no choice but to remain ahead of the curve to understand and adapt their cybersecurity strategy. Otherwise, they risk the very real repercussions of an attack.

In this guide, we've compiled some of the most common attacks that could affect your business, as well as some remediation and prevention techniques

Table of Contents

Access Attacks

Unauthorised access attacks seek to acquire and maliciously use the unique credentials your team uses every day.

PHISHING

One of the most common of cyber-attacks, which many have likely encountered in the past, is a phishing attack. Phishing attacks are performed at scale and involve fraudulent emails being sent to unsuspecting users.

Phishing attacks often appear to come from trusted sources (banks, brands, or even colleagues etc.) but link to malicious sites or files that aim to either download malware or steal sensitive information. These attacks rely on creating urgency - requiring users to act to avoid negative consequences (such as fraudulent activity or undeliverable post for example). This social attack aims to manipulate vulnerable users - be it those who are timepoor, unaware or unsuspecting and uses these instances to obtain sensitive information that can either be sold or used as part of further cyber-attacks.

Phishing attacks are not limited to email. Hackers can utilise anything from phones to social media as a means to gain personal information.

The most effective tool to combat phishing attacks, is user training and awareness. Understanding how to spot legitimate sources and remain vigilant for anything seemingly suspicious is the best tool in combatting phishing attacks. Here are some common phishing attacks:

Email Phishing

Undoubtedly the most well-known attack, email phishing involves sending emails to potential victims impersonating a well known or trusted brand, which appears legitimate. By using certain tactics, it lures the user to a sense of heightened immediacy to click the link or download a malicious package.

Spoofing

Spoofing occurs when someone impersonates a trusted contact, pretending to be someone you trust in order to access sensitive personal information. Spoofing can come in many forms, such as Caller ID spoofing, Text message spoofing, IP spoofing, and Website spoofing among many others.

Spear Phishing/Whaling

While still using email, spear phishing is more sinister and targeted in nature. Cyber criminals gather information from publicly available sources (such as your company website or social media) and begin to target specific individuals within the company. Often using real names, job functions, or phone numbers.

Typically, these emails immitate senior staff and target staff who are likely to action the attack as an internal request. In some instances, attackers mimic CEOs and ask junior staff to purchase large quantities of gift cards, resulting in large financial loss that is irrepairable.

Phishing Attacks: What to look out for

- Remain vigilant of abnormal requests for personal information. If in doubt, call a support line obtained from their official website.
- Unexpected documents that require ‘access’ using a login and password may be an attempt to steal credentials.
- A tell-tale sign of fraudulent emails is poor grammar.
- Avoid clicking shortened, unfamiliar or incorrect links.
- Stay vigilant for emails with poor quality branding and logos. While similar, subtle differences can give it away.
- Keep an eye out for legitimate information about the organisation being spoofed.
- Ignore emails that don’t contain a substantial body of text.
- Browsers may alert you of visiting an ‘unsecure’ site which could mean the site could contain malicious code.

Did You know

19% of professionals use easily guessed passwords or share passwords across accounts

90% Phishing accounts for up to 90% of all breaches that organizations face

Clone Phishing

Usually deployed through email is clone phishing; this attack leverages services that someone has previously used. Cyber attackers know most of the business applications that require people to click links as part of their daily activities, and take advantage of this, sending targeted emails to those within an organisation that routinely use these services such as emails from services that can gain important information such as DocuSign which asks the user to input personal information that may be lucrative to an attacker.

‘Evil Twin’ Phishing Attack

This attack utilises a fake Wi-Fi hotspot, often making it look legitimate or similar to one that is used everyday, that could potentially intercept data during transfer. By using this fake hotspot, the attacker can engage in man-in-the-middle or eavesdropping attacks, allowing them to collect data like login credentials or sensitive information that has been shared during transactions/ interactions.

Watering Hole Phising

This occurs when attackers research into a company and look at what websites are routinely used by their employees. Then, they infect the IP addresses of these popular sites with malicious code or downloads. Often these websites tend to be websites that provide industry news or third-party vendors’ websites. When the user visits the website, they can unwittingly download the malicious code.

How we’re helping clients.

FitzFortify
Dark Web Monitoring (Gold)

Through our FitzFortify services we are able to identify if your organisation’s information has been breached and made available on the dark web. Our IT experts identify which accounts and credentials have leaked onto the dark web, providing information as to the source of leaks and the duration of exposure. Dark web monitoring is essential to prevent credential re-use, complete account takeover or email compromise.

Data Processing Attacks

Unauthorised data processing attacks involve the witholding, use or selling of your business data in either direct attacks or on the dark web.

Man-in-the-Middle Attack (MitM)

This attack occurs when a perpetrator intercepts a two-party transaction and intercepts it by breaching the communication protocols between each party. Once the attacker accesses this transaction, they can both steal and manipulate the data by interrupting the traffic.

Due to the unique session ID between your machine and the remote web server, an attacker works to hijack the session by getting hold of the session ID and posing as your computer. Allowing them to gain access through a protocol request and giving access to your data. Phishing or malware attacks can often lead to a MitM attack due to having access to your computer or credentials already.

How we're helping clients.

FITZ MSS

Azure

FitzMSS provides enterprise grade security built with the user in mind. FitzMSS counteracts an array of security issues. In the instance of an attack, security experts can remotely lockdown corporate devices to prevent the dissemination of sensitive data.

Did You know

A Ponemon Institute study showed that 62% of employees reported access to company data that they didn't need to have.

According to Netcraft, Man-in-the-Middle attacks were thought to pose a threat to 95% of HTTPS servers.

Between 2018 and 2020, there was a 47% increase in the frequency of incidents involving Insider Threats. Including accidental data loss and malicious data exfiltration.

Insider Threat

Insider threat is defined by the risk to an organisation that is caused by employees, former employees, business contractors or associates of the business. Insider threat can effect small businesses through a variety of different ways.

While some issues may arise from ignorance or carelessness, at times there are more sinister motives with malicious intent.

Either way, the outcome remains the same. Rather than the threat of attack coming from an external source, the attackers on an insider threat already have access to private company information and can use this for nefarious intentions.

How we're helping clients.

Cybersecurity
User Awarness Training

Fitzrovia IT provides cybersecurity training to businesses and their employees - a means to pre-empt and prevent cyberattacks. Our experts provide comprehensive training in cybersecurity best practice. Teaching people how to recognise, report and prevent cyber-attacks.

As part of training we can simulate phishing emails to gauge the response from employees, and subsequently compile a report containing company specific recommendations.

Malicious Disruption Attacks

Designed to impact your business, malicious disruption attacks are built to damage the processes that keep your operations running smoothly.

Malware

Malware refers to the various forms that can be harmful to your computer system that is often deployed when a user clicks on a link or attachment which is used to plant malicious software within the system.

Once the malware has been deployed within a user's computer system, it can cause a myriad of problems such as denying the user access to essential parts of the computer, obtaining personal information by collecting data from the hard drive, or even completely crashing the system, rendering the computer unusable.

There are various forms of malware currently in circulation, below are some common types that you may encounter:

Virus

A virus is a specific type of malware that self-replicates by inserting its code into other programmes.

Viruses spread through various means such as emails, infected websites or even USBs. These are then activated once the victim opens the file. Once activated, a virus may delete or encrypt files, modify applications, or disable system functions.

Worm

A computer worm spreads copies of itself from computer to computer and can replicate itself without any human interaction.

Computer worms can be so devastating due to their ability to spread without user interaction. Viruses require an end-user to remove it, before it can try to infect other innocent files and users.

Trojan

These attacks disguise themselves as legitimate programmes, but they contain malicious code.

A common type of this attack will be a familiar one, the fake 'antivirus program', which alerts the user that their machine is 'infected', then instructs you to run a program to clean your machine. Once the victim has taken the bait and installed the programme, the Trojan then accesses your files.

Ransomware

Acting as a block when deployed, this will prohibit you access to your device until you pay a 'ransom' fee to its creator, often being very expensive and difficult to remove.

Once the programme is activated, most attackers immediately look for and encrypt users files within a few minutes, locking the user out quickly.

Spyware

Spyware is utilised by cyber criminals to log the keystrokes of victims, essentially shadowing the user to see their logins/passwords to gain access to their accounts/property.

This surveillance can lead to the cyber criminals accessing various bits of important data such as login credentials, card and PIN numbers, email addresses etc. They can then sell on this information to other criminals for use.

Did You know

£616,927.05

the average cost for ransomware remediation in the UK

65%

the average amount of data restored once payment has been received

Denial-of-Service(DoS)/Distributed Denial-of-Service (DDoS)

DoS attacks are flooding of a system, server, and/or network with traffic which then overloads it, making it unusable to others. This prevents those who wish to use your site access to it. These attacks can usually be attributed to the goal of causing a disruption as well as impeding the response time for service requests, which can harm business.

Additionally, there are what is known as Distributed Denial-of-Service (DDoS) attacks. This type of attack is very dangerous as it is performed by various machines at the same time, leading to a complete system failure and the site going offline. This enables another attack on the network, which can lead to further damage.

How we're helping clients.

FitzFortify
Dark Web Monitoring (Gold)

Penetration testing services from Fitzrovia IT identify, test, and highlight vulnerabilities in an organisation's network security. Using both automated and manual technologies, we conduct internal/external infrastructure, Wi-Fi, API and Web Application tests to identify vulnerabilities and provide a comprehensive security report.

FitzMSS
SentinelOne

Within FitzMSS we utilise SentinelOne, an advanced Endpoint Detection and Response (EDR) platform that utilises AI and Behaviour Analysis to protect against malware, ransomware and cyber security threats. If malware is detected within a corporate device, we're able to immediately isolate the threat by removing the device from the corporate network. Once the device is off the network we can conduct in depth analysis to identify the source of the malware, and detect if any further devices have been affected.

fitzrovia

www.fitzroviait.com
020 3727 6020