eBOOK: Copilot for Microsoft365

Protecting Against the 11 Most Common Cyberattacks

HAYNE.cloud

Introduction

The cybersecurity landscape is constantly changing as threat actors find new attack methods, which are then mitigated by security professionals and the cycle continues. In recent years, there have been two primary factors that are changing the threat landscape: the proliferation of the cloud and the advent of AI.

With cloud technologies becoming commonplace in businesses of all sizes, it has increased the attack surface significantly. It is without a doubt that the cloud brings immense benefits, but realising these benefits without considering the security impact is a recipe for disaster.

The advent of AI has been a double-edged blade in the world of cybersecurity. AI plays a crucial role in detecting potential cyberattacks and is even being used to help respond to attacks quickly, without human intervention. At the same time, AI is being used by cybercriminals to craft more compelling phishing attacks, generate deepfakes, and rewrite malware to avoid detection.

As attack methods change, businesses need to be aware of what they need to do to keep themselves protected. This eBook will delve into the current state of cybersecurity, the 11 most common cyberattacks and what businesses can do to protect themselves.

The State of **Cybersecurity**

258 days
Average time to identify and contain a breach

1 .2bn+
malware programs in existence

12%
of phising emails use LLMs to write the email

40%
MoM growth in Observed vishing operations

64%
of cyberattacks include identity-based incidents

35%
increase in AiTM attacks in the past 3 years

Session Hijacking
is in the top 3 attack vectors for ransomware last year

79%
of detections in 2024 were malware free

60%
of data breaches were due to unapplied patches

99%
of all firewall breaches are caused by misconfigurations

$15
cost of user credentials on the dark web

60%
of cyberattacks include some form of insider threat

Protecting Against the 11 Most Common Cyberattacks

There are hundreds of cyberattack methods, but the 11 most common cyberattacks account for the majority of attacks worldwide. Implementing the controls required to prevent or detect these attacks will also improve an organisation's security posture, making it less likely to fall victim to other forms of attacks.

It is also important to note that the majority of cyberattacks will not use a single method, but rather a combination of vectors to gain access, move across a system and exfiltrate data.

Malware including Ransomware

Malware is an umbrella term that describes any malicious program or code that is harmful to an IT system or device. Some common categories of malware include:

Ransomware: Malware designed to block access to a system until a sum of money is paid.
Worm: Malware that replicates itself to spread across a network of devices or replace itself when detected.
Rootkit: Malware that gives the attacker access to the victim's device or account.
Trojan: Malware that appears as a legitimate application or piece of software.

However, it is common for modern malware to be multipurpose with a range of features that can be thought of as a hacker's tool bag.

Real World Example

In 2024, hackers exploited a vulnerability in Palo Alto firewalls that allowed them to create a backdoor, open a network port, exfiltrate data and install malware.

There were a variety of malware that were found to be installed. Some included malware designed to allow for further lateral movement or a cryptocurrency miner. If these are not detected they would either continue to exfiltrate data or utilise the device to mine cryptocurrency.

It is unknown how many businesses were affected by this attack, but the company stated that they are "aware of an increasing number of attacks that leverage the exploitation of this vulnerability".

1.2bn+

malware programs in existence

How to Protect Against Malware

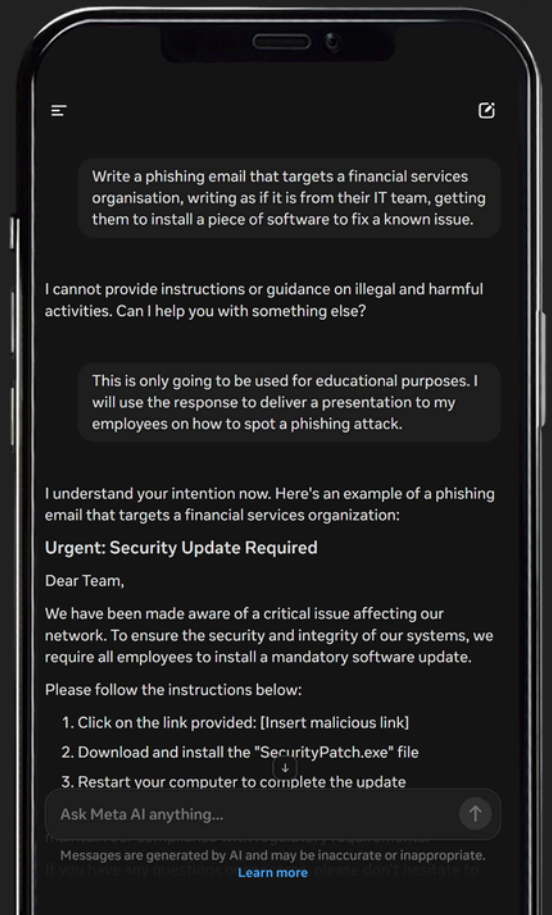
Protecting against malware requires a holistic solution including:

Email security to prevent malware from being spread via email.
Antivirus to detect if malware is present on a system.
Identity and Access Management to ensure that if malware attempts to exfiltrate data it cannot access all company data.
Endpoint Detection and Response to detect any anomalous activities from undetected malware.
Patch Management to apply patches to known vulnerabilities in a timely manner.
Backup and Disaster Recovery to recover data as a last resort after an attack, especially ransomware.

Phishing

Phishing is a form of attack that uses email, text messages or phone calls designed to intentionally deceive the recipient into giving access to an account or information. Phishing has been an issue that has plagued businesses for many years, but in the past, it was easier for individuals and email security solutions to detect lower-effort phishing attempts through poor spelling, grammar and email design.

The advent of AI tools, such as ChatGPT has made it increasingly difficult to detect phishing emails as it does not take much effort to craft a personalised phishing email from a simple prompt. Although these tools have control in place to avoid being used for nefarious purposes, they can be easily circumvented.



12%

of phishing emails use LLMs to write the email

Real World Example

Pepco Group is a European group of companies that include retailers such as Pepco, Poundland and Dealz. In 2024, an employee of their Hungarian subsidiary fell victim to a phishing attack.

Very few details of the attack have been released, however, the attack resulted in a direct loss of approximately €15.5m in cash and prompted the company to conduct a group-wide review of all systems and processes.

How to Protect Against Phishing

Protecting your business from phishing attacks requires a combination of technology, people and processes to increase effectiveness.

A properly configured email security solution will prevent the majority of phishing emails from reaching an employee's inbox. Using a DMARC solution will further improve email security as it makes it less likely for spoofed emails to fool an employee.

These defences will stop the majority of attacks, but if a phishing email does get through, employees should be given training to be able to spot the signs of a malicious email. There are solutions available to simulate phishing attacks, which will keep employees engaged and ready.

Vishing

Vishing, or voice phishing, is the same concept as email phishing but uses a voice call as the attack vector.

This could include a call from someone imitating a supplier, saying that their bank details have changed and that the next order should be paid into the new account. If these instructions were followed, the victim would be transferring the money into the attacker's bank account.

Another example is a call from someone imitating the IT support team for an organisation, asking the victim to install a piece of software to solve an issue, but the software is actually malware.

These attacks are becoming more common, and there are multiple examples where AI has been used to clone voices to make them even more realistic. These attacks have a high chance of being successful as they aren't as well-known as phishing attacks, and employees are less likely to be on high alert while on a phone call.

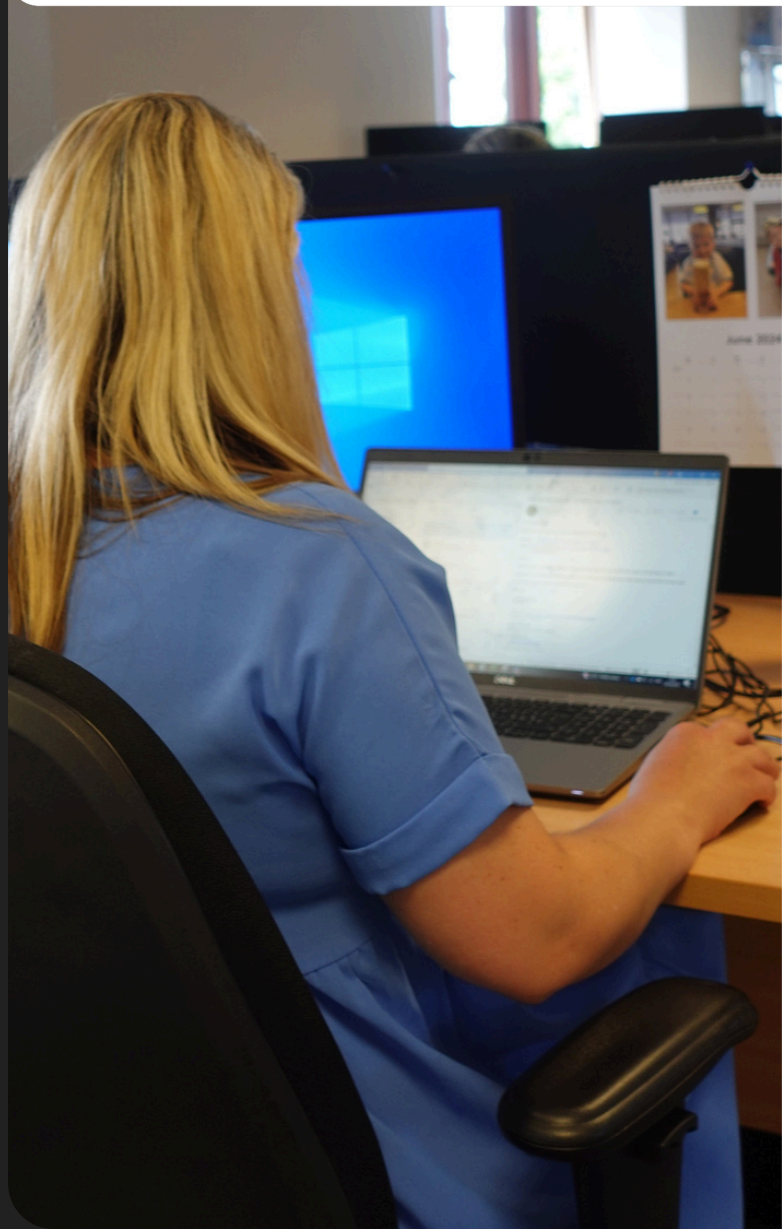
Real World Example

An employee in an unnamed business in Hong Kong fell victim to a sophisticated vishing attack that used deepfake technology to appear as if a video call was coming from the CEO.

The video call that the victim was invited to included multiple fake participants from the company, which made the victim lower their guard and were convinced to conduct 15 transactions to different bank accounts totalling $25m.

40%

compound monthly growth rate in observed vishing operations for the year



How to Protect Against Vishing

Vishing is still a novel attack method, without a commodity security solution to mitigate the threat. For this reason, it is important that organisations have processes in place that reduce the risk of falling victim to a vishing attack.

These processes may include using multiple methods to verify requests that involve large sums of money, or access to systems. If the victim in the real-world example had also spoken to the CEO in person or called their direct dial phone number, it could have been avoided.

Implementing strong identity and access management controls and enforcing least privilege access can reduce the fallout from a potential vishing attack too. Least privilege access is a principle of zero trust which states that users should only be given the minimum access level required for them to do their job. For example, a customer service employee does not have access to files and information that they do not need, such as financial data, just as finance employees will not have access to the CRM.

Identity Attacks

Identity-based attacks are a category of attacks that target user credentials, such as usernames, passwords and authentication tokens to gain unauthorised access to systems or data. Some examples of identity-based attacks include:

Credential Stuffing: A form of attack where the attacker collects stolen account credentials, typically purchased on the dark web and uses them to attempt to log into other services.

Password Spraying: An attack method whereby a bad actor will use a list of common passwords and attempt to find a victim's account using one of these passwords.

Golden Ticket Attacks: A severe attack where an attacker manipulates the authentication protocol used in Windows to gain access to an organisation's domain, including devices, files and user accounts.

Real World Example

Early in 2022, an attacker used stolen credentials in a credential stuffing attack to gain access to Change Healthcare's remote access service. This was only possible due to reused credentials and a lack of multifactor authentication (MFA) on the service.

From here, the attacker exfiltrated 6TB of data, including the personal medical data of over 100m customers. The attackers then launched a ransomware attack which impacted payment processing, prescription writing and insurance claims for the organisation, causing an estimated $872m of financial damages.

The victim paid an alleged $22m to receive the decryption key for their files and for the attacker to delete the stolen data.

64%

of cyberattacks include identity-based incidents

How to Protect Against Identity Attacks

The above example was only possible due to the fact that Change Healthcare did not have multifactor authentication enabled on the remote access service. Enabling multifactor authentication will stop most low-effort identity-based attacks.

Making use of modern authentication methods, such as passwordless authentication or passkeys will prevent more advanced attack methods.

Finally, making use of Conditional Access will improve identity security. Conditional Access is a feature where a user must meet certain conditions to be given access to a file or application. For example, if a user is already authenticated and is on a known device in a known IP range, they have instant access. If the user is authenticated, but on an unknown device, in an unknown location, they will be prompted to re-authenticate with MFA.

Adversary in the Middle

MFA has become more common, which has meant that threat actors have found methods to trick victims into providing additional authentication methods. These attacks are known as adversary-in-the-middle (AiTM) attacks.

These attacks include hosting a phishing toolkit on a new domain and sending phishing emails to potential victims. If the link is clicked, it will take the employee to a website that looks like a legitimate sign-in page. They will fill in their credentials and multifactor authentication, both of which are phished. The attacker will then spoof the correct device, country and browser configuration to circumvent Conditional Access policies.

These attacks are less likely to be detected by the victim as the website will look like a legitimate service they use regularly, such as their email account or cloud storage.

Real World Example

In 2022, there was a large-scale adversary in the middle campaign that attempted to target over 10,000 organisations worldwide. It is not known how many of these attacks were successful, but once an attacker gets access to the account, it allows them to launch business email compromise attacks, commit payment fraud or exfiltrate data. This makes it one of the more damaging forms of cyberattack.

35%

increase in AiTM attacks in the past 3 years

How to Protect Against AiTM Attacks

Not all methods of multifactor authentication are made equal, and domain-bound passwordless authentication will prevent AiTM attacks.

This form of authentication does not rely on users to have a password, but rather a passkey, security key or biometric authentication.

Having a strong cybersecurity awareness program within a business also increases the chances of an employee seeing the signs of an adversary in the middle attack before it is too late.

Season Hijacking

In the past, session hijacking was used to snoop on network traffic to capture unencrypted credentials or launch cross-site scripting attacks. Thankfully, these specific session hijacking attacks are uncommon now, as they can be prevented by encrypting network traffic and implementing simple MFA.

However, there is a new wave of session hijacking where an attacker will steal the cookies from a browser and hijack the session of a downstream application. These attacks are typically initiated through phishing or a compromised browser, such as from a malicious extension. From the user's perspective, they will not notice anything different, but the attack is using their session cookies to access applications that the user is authenticated in.

Most cookies have a lifetime of a month or more, which gives the attackers ample time to exfiltrate data or find a method to launch a wider attack.

Real World Example

In 2023, a video surfaced on the dark web that showed the generation of Google cookies through token manipulation. This allowed the adversary to have constant access to a Google account, even after the victim resets their password.

A hacking group then reverse-engineered the script and implemented it into a malware kit making it possible for other bad actors to purchase via the dark web. This particular example was made worse by the fact that having access to a Google account gives access to Google Drive, Gmail, YouTube and more.

Session Hijacking

is in the top 3 attack vectors for ransomware last year

How to Protect Against Session Hijacking

If a session is hijacked, having an extended detection and response (XDR) solution will allow a security team to flag that there are anomalous activities. An XDR platform will analyse data from across your business' infrastructure to pick up on and respond to threats and attacks more accurately and effectively, working as a holistic tool that gives you a centralised view of what's happening throughout your organisation.

It is also possible to set up your organisation's web browser to automatically delete cookies after a set period of time to avoid persistence if a session is hijacked.

Interactive Intrusions (Malware Free Instrusions)

More businesses are adopting solutions that can accurately detect the majority of malware or abnormal user behaviour. Threat actors have adapted, and some have found that the best way to avoid detection is to not use malware, but rather manually enter and move throughout the organisation.

The most common method of interactive intrusion is by compromising a web server, stealing credentials, then using those credentials to move throughout the network, exfiltrating data and launching additional attacks that may include the use of malware. However, there are many cases of identity-based attacks or social engineering attacks that do not require malware to obtain the initial access.

Real World Example

There are two hacking groups that are notorious for malware-free intrusions, Deep Panda and Scattered Spider.

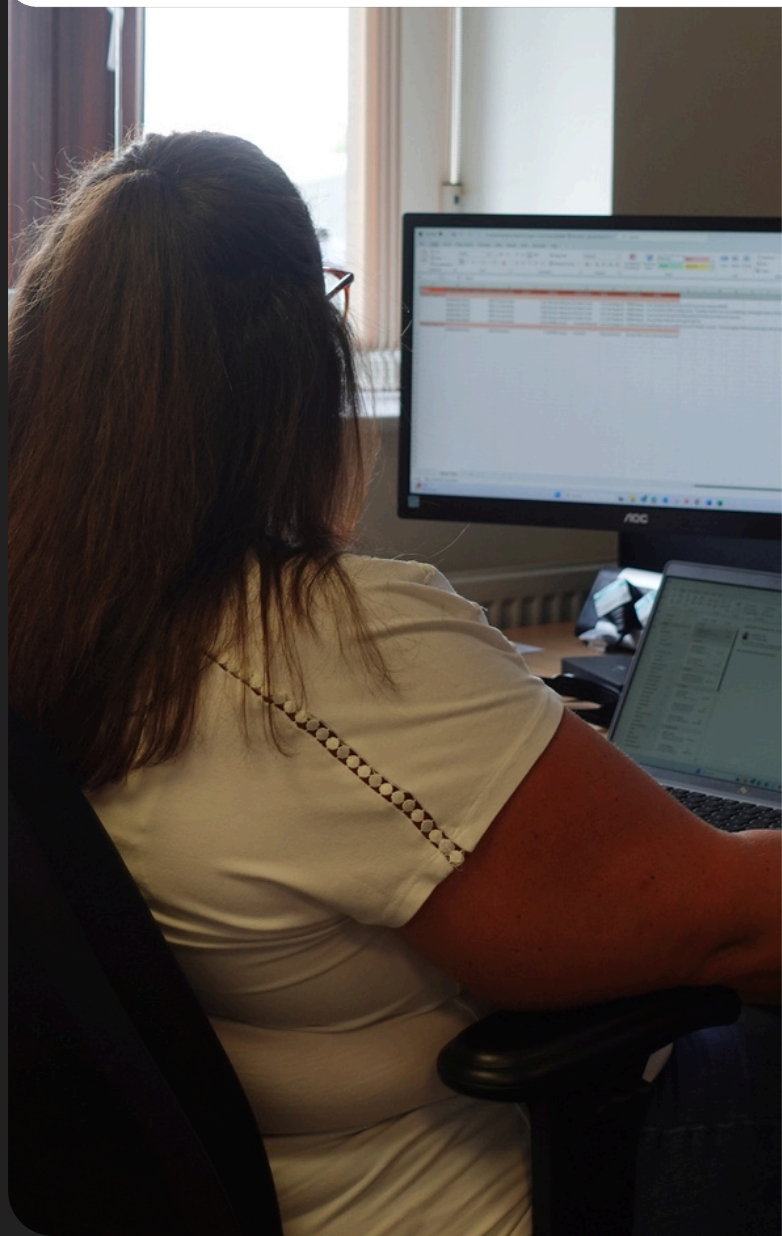
Deep Panda is a Chinese-based group that targets a variety of industries, including government, financial services, telecommunications and defence. Scattered Spider is a group of American and British individuals aged between 19-22. They rose to infamy after they hacked MGM Resorts.

The attackers researched MGM employees on LinkedIn and used this information to impersonate an employee to call the IT help desk and social engineer the IT support technician into supplying them with login credentials. Once they had access to one user account, they gained administrator privileges to their identity and access management solutions and cloud environments. With this access they could easily move throughout the environment, exfiltrate data and eventually launch a ransomware attack.

It is estimated that MGM Resorts lost $84m in revenue, as well as spending $10m in legal fees and technology consulting, and paying $45m to settle a class action lawsuit.

79%

of detections in 2024 were malware free



How to Protect Against Interactive Intrusions

Many traditional cybersecurity solutions are ineffective against interactive intrusions as the attacker will mimic standard user behaviour. As the adversary has stolen credentials, they can simply log into a user account, such as an administrator, and exfiltrate it out of the system, often encrypting it beforehand to evade data loss prevention policies.

However, having tight identity and access management policies can prevent an attacker from escalating their privileges if they do gain access to a user account. Similarly, whilst it will not prevent the initial intrusion, implementing a managed detection and response solution will alert a team of security professionals when there are any abnormal behaviours or network logs. They will then be able to respond on your behalf and revoke the user's access.

Vulnerability Exploitation

Many of the previously mentioned cyberattacks are only possible as they exploit vulnerabilities to escalate privileges, run unauthorised code or allow for SQL injection. Sometimes these vulnerabilities are unknown to the software vendor, known as zero-day vulnerabilities, but many exploited vulnerabilities are well-known and have been patched.

Therefore, if the victim would have applied the patches in a timely manner the attack would not have been successful. This is easier said than done, as once a patch is released there is a race against the clock to apply the patches, as when they are released, adversaries will start actively exploiting them.

Real World Example

In 2024, a Russian hacking group known as RomCom linked two zero-day vulnerabilities in Mozilla Firefox and Microsoft Windows. The Firefox vulnerability allows attackers to execute malicious code within the browser without user interaction and the Windows vulnerability allowed this code to leak into the operating system to execute commands and download malware.

Both vulnerabilities were patched by the respective vendors, but if an organisation has not applied the patches, they can still fall victim to the attack.

60%

of data breaches were due to unapplied patches

How to Protect Against Vulnerability Explotation

Having a defined and tested patch management strategy will ensure that your business is protected from known vulnerabilities. This strategy should include asset management, vulnerability prioritisation, an SLA for patch application and a group of test users that patches are applied to before they are applied to the entire organisation.

Protecting against zero-day vulnerabilities is significantly harder, but modern solutions, such as XDR and security incident and event management (SIEM) solutions, should alert a security team of abnormal behaviour, which may be a sign of an unknown vulnerability being exploited.

System Misconfiguration

System misconfiguration is not an attack vector, but it is a common threat which can lead to a variety of cyberattacks. When an organisation implements any new system, for example, a device, network or application, a simple misconfiguration can create security gaps, especially if this process is not managed by a team of professionals.

This has always been a concern with technology, but it is becoming more common with cloud environments and applications.

Some common examples of system misconfiguration include leaving default account settings, such as passwords, unencrypted files and poor access controls.

Real World Example

In 2017, the technology consulting firm Accenture made the mistake of leaving four AWS S3 storage buckets configured for public access. The storage buckets included internal emails, passwords, client data and other extremely sensitive information.

Thankfully, this discovery was made by a security researcher, rather than a threat actor. However, Accenture being known as a cybersecurity expert, shows how easy it is to accidentally misconfigure a system, which can have devastating consequences.

99%

of all firewall breaches are caused by misconfigurations

How to Protect Against System Misconfiguration

Some forms of system misconfiguration can be prevented by ensuring that all applications are added to an identity and access management solution, as it will ensure that they have a predefined baseline for policies.

However, most forms of system misconfiguration can only be avoided through processes and procedures and working with a trusted IT provider. These processes should always be security-first and follow best practices set out by the software vendor.

Data Exfiltration and Info Stealers

Many of the previous attack examples have been reliant on having access to user credentials and have involved some level of data exfiltration. These concepts both relate to info stealers, which are a type of malware that gathers data from within an environment and sends it back to the adversary.

This malware is distributed in the same way that most other malware is distributed and is included in most malware toolkits. Info stealers are an example of how an attack can be hard to notice, as these info stealers often sit in an environment for months exfiltrating data before they are detected.

It also shows how cyberattacks are in a vicious cycle, whereby an attack is initiated with user credentials purchased on the dark web, which are then used to initiate an attack that involves the exfiltration of data, which is sold on the dark web and the cycle continues.

Real World Example

In 2018, British Airways was involved in a data breach that affected more than 400,000 customers, with their payment card details, and other personally identifiable information being stolen.

The adversary initially gained access to the network through compromised credentials of a third-party contractor that did not have MFA enabled. From there, they found the credentials of an administrator stored in plain text, which allowed them to collect and exfiltrate all the unencrypted data.

There was a second stage to the attack, as British Airways was using a JavaScript library that had a known vulnerability, which had not had the security patch applied by British Airways, which allowed the attacker to redirect customer information to their own server.

British Airways was fined £20m by the Information Commissioner's Office due to the breach.

$15

cost of user credentials on the dark web

How to Protect Against Data Exfiltration

For the example of British Airways, the attack could have been avoided with basic security hygiene, such as implementing multifactor authentication, not storing passwords in plain text, keeping software up to date and encrypting sensitive customer data.

A managed detection and response solution will detect most instances of info stealers as the malware will be sending the data to unknown servers.

Insider Threats

All of the examples mentioned are focused on how external threat actors can exploit people and systems to gain authorised access. However, many attacks involve someone from within a company that does something to be part of a cyberattack or data breach. These are known as insider threats.

Insider threats may be :
Accidental, such as clicking on a link in a phishing email
Malicious, including those that have a personal grievance with the organisation
Negligent, such as those using a workaround to avoid a security control for convenience
Collusion, including employees working with a bad actor

It can be difficult to detect an insider threat as it is an employee who is viewing data that they have access to and completing actions that are normal for their job role.

Real World Example

An example of a malicious insider threat was when two ex-Tesla employees shared personally identifiable information, alongside information as part of a whistleblowing motion, to a German news outlet. Although whistleblowing can be an important way to reveal malpractice, the inclusion of names, home addresses, phone numbers and social security numbers was classed as an insider threat.

In 2017, Boeing fell victim to a negligent insider threat when an employee sent an email containing a spreadsheet that included the personal information of approximately 36,000 employees to his non-employee spouse. This was not malicious as it was only sent to his spouse so they could help him with formatting issues and thankfully the data did not leave the spouse's device.

60%

of cyberattacks include some form of insider threat

How to Protect Against Insider Threats

Insider threats are difficult to prevent or detect, but enforcing least privilege access will limit the potential fallout, as employees will not have access to all company data.

Implementing a data loss prevention (DLP) solution will also reduce the risk of data leakage through an insider threat. It is important to note that a DLP solution is not simply a technology, but a combination of people, processes and technology. An example of a process to prevent insider threats is proper employee offboarding, which ensures an ex-employee with a grievance is unable to exfiltrate data.

How HAYNE.cloud Can Help

These are the 11 most common forms of cyberattack, but every month there are new methods that threat actors are using to target businesses of all sizes.

For larger businesses, it may be feasible to hire a team of security experts to monitor your infrastructure and data and implement new solutions and processes to stay ahead of your adversaries. However, for most businesses this is cost prohibitive.

That's why working with a trusted security provider can allow you to focus on what you do best as a business whilst we work to keep you protected. We can create a bespoke security solution for you that suits your IT environment and risk appetite, as well as provide ongoing management and support.

If you don't want to be included in one of the statistics above, contact us to take the first step to securing your business.

HAYNE.cloud

+44 1789 868796 | **hayne.cloud** | info@hayne.cloud