Anatomy of a Breach

How hackers break in – and how you can fight back

Updated November 2017

Microsoft

Table of Contents

The Four Stages of a Breach

Security threats are relentless. A cyberattack can cause millions of dollars in damage – to both your company's bottom line and its reputation. Are you aware of the potential threats to your company? Do you have a plan in place to resist, mitigate and recover after a breach?

01 Getting the Initial Foothold

02 Expanding to the Network (Network Escalation of Privileges)

03 Gaining Elevated Control (Local Escalation of Privilege)

04 Staying for the Short- or Long-Term

Read on to explore what happens at each stage of a breach, and learn to how to formulate a defence strategy that will help you protect yourself and your company.

STAGE 01

Getting the Initial Foothold

Attackers gain a foothold in your organisation using a variety of tactics. From compromised workstations to unpatched internet-facing servers to badly configured third-party-managed devices, they will use anything available to breach defences and gain network access. Once inside, they can perform the necessary reconnaissance to identify and target your organisation's valuable information and resources.

Common Techniques

Exploit

Code that takes advantage of software vulnerabilities to access information on your server (or any other device) or install malware.

Password spraying

A more recent, novel tactic "sprays" several common passwords at tens of thousands of accounts at once to gain entry. Hackers cast a broad net at many organisations at once to better target where they wreak havoc.

Malware

Short for "malicious software," these programs can steal information, lock your PC until you pay a ransom or use it to send spam (e.g. viruses, worms and Trojans). This document focuses on what is often called "targeted malware," designed to infiltrate a specific industry or organisation.

Phishing

Tricks users into giving out personal, financial or company-specific information to gain unauthorised access to internal infrastructure. To entice users, attackers send emails with URL links that appear to be from trusted third-party vendors or internal employees.

Ransomware

This malware locks a user out of their computer or network without access to files, folders or drives. Attackers then demand a financial ransom to regain access; however, they don't always return access after payment.

Supply chain vulnerabilities

Involves tampering with or manipulating an external vendor's products, IT systems or processes during sourced components' development, manufacturing or delivery.

Watering hole

Attackers identify specific websites as spots that their intended targets frequently visit. Attackers place malicious links to malware on the sites in hopes of infecting them when they visit.

Zero day

Exploitation of a vulnerability that the software vendor hasn't disclosed or patched.

SOLUTION

An Ounce of Prevention

Organisations across all industries are not immune to threats, especially those posed by weak or compromised user credentials. As employees use more apps and devices and create different identities across corporate and social accounts, it's easier than ever for hackers to breach corporate systems. Why? More often than not, an employee will use the same password to save time and increase their productivity.

Stopping hackers at the front door is the ounce of prevention you need to protect your company. Your first line of defence is a strong identity and access strategy.

Protect Identities, Control Access

We recommend the following preventative measures:

Find out how much control you have over access.

Ask critical questions:

- Who is accessing the network?
- Where are they based?
- Is their device healthy or managed?
- What apps and data are they accessing?
- What's the business impact?

And turn to solutions that protect against identity breaches:

Microsoft Enterprise Mobility + Security:
Use Azure Active Directory to employ a robust identity and access strategy to ensure users are who they say they are before you let them into your network.

Conditional access lets you manage user identities with access policies that control, secure and restrict access to data. With multi-factor authentication, users must provide additional verification beyond just a username and password to confirm their identity.

Windows Hello
Try a password-free approach. Take away the hassle of remembering passwords and replace them with more secure sign-in methods using faces, fingerprints or PINs.

Windows Credential Guard
Protect user credentials in the midst of an attack using a virtualisation-based security solution that isolates sensitive identity data and protects it from theft attack techniques and tools.

Windows Defender SmartScreen
Help block phishing and exploit sites and occurrences of malicious app downloads using a phishing- and malware-filtering technology for Microsoft Edge and Internet Explorer 11 in Windows 10.

INDUSTRY PROFILE

Finance

Cyberattacks have increased in the financial services industry in recent years. Although many organisations are taking precautions, the ever-evolving digital landscape continues to create employee challenges.

If not properly set up, test environments without protections that validate endpoint request access can lead to breaches. That's precisely what happened to one financial firm during tax season. Employees noticed unusual activity when a new file appeared on affected desktops, containing a webpage with ransom payment instructions to pay for the attacker to supply decryption keys needed to recover files. In all, hundreds of servers and workstations on the corporate network revealed targeted ransomware-encrypted documents.

A test server left exposed to the internet revealed the culprit. Hackers obtained both a public-facing IP address and access to the internal private IP address space. Upon further investigation, no Network Security Groups or firewall appliances were in place to protect any systems within the environment. And the test server operated with single-factor authentication, leading to further detrimental exposure.

Automated malware commonly searches for open systems on the internet to gain access to, and in this case, the malware that attacked applied a brute force algorithm to attempt to log in to the network. In less than a day, the virus successfully accessed a username and password for the test server. The culpable account's username and password were identical – this is typically one of the first things a brute force attack will attempt. The compromised server account belonged to a domain administrator, giving the attacker unfettered access within the network. The account was used to stage and deploy the ransomware that affected systems within the network, and the attacker also accessed a domain controller. As a result, the firm had to consider all account usernames and passwords compromised.

STAGE 02

Gaining Elevated Control

Whether infiltrating your company or one of your suppliers, local escalation of privilege is their next step. Attackers typically look for ways to consolidate control of the local system. Failing that, they look for another system that offers a higher chance of success in gaining administrative privileges, or greater access to valuable data.

Wherever they end up, the attacker's goal is to identify the accounts belonging to users that are responsible for managing the system, and to impersonate these users to gain access to system resources. Then, using both built-in tools and downloaded malware, the attacker attempts to identify other systems of interest and network resources in order to capture usernames and passwords – since only accounts with a high level of access can accomplish these actions.

Don't ignore your company's supply chain as a potential entry point or place to gain elevated control. In fact, there are weaknesses in many parts of the chain that an attacker can exploit, resulting in business disruption.

Common Techniques

Keyloggers

A type of malware that records which keys a user presses. Also known as keystroke logging, this software enables attackers to collect usernames and passwords to log in to the target organisation's network.

Network scanning

A reconnaissance technique that catalogues the systems that are currently accessible, such as the host machines, services and resources that are active on a network. Attackers then create a target list of interesting systems that they will attempt to access with their newly acquired administrative credentials.

Pass the Hash (PtH)

An attacker's technique to use a victim's password's underlying hash (code) to masquerade as that user. The attacker doesn't need to know the actual user credentials to authenticate to a remote server/service.

SOLUTION

A Winning Network Solution

As threats increase in sophistication, many organisations are unable to detect malicious activity and swiftly respond. The reality is, once attackers are in your network or supply chain, they can steal information, breach your corporate privacy policy, destroy your customers' trust and cause major business disruption.

You can stay ahead with a solution that:

- Detects threats and attacks that have made it past other defences
- Provides key information about where and why the attack happened
- Gathers detailed footprints of attacker actions across the organisation
- Supplies information about the attack and recommends a response

Comprehensive risk management is a key part of a stronger security strategy. This means understanding the assets you have, the potential risks to those assets, the cost to the company if those assets are leaked and the controls you have in place to help protect them. You need to understand the vulnerabilities across your company's identity, apps, data, devices and infrastructure in order to protect against threats and quickly recover. These approaches should be seen as part of the security lifecycle that evaluates risk on an ongoing basis and feeds lessons learned back into the system.

Build a Secure Framework

We recommend investing in these security measures:

Windows Defender Advanced Threat Protection

Collect and analyse behaviours observed on the device – whether in attachments or links included in incoming emails – to detect targeted advanced attacks. Questionable material is not allowed to reach your users, reducing threats to your network. With this rich cloud-based console, you get full visibility into your endpoint security.

Azure Advanced Threat Protection

Detect and investigate advanced attacks and insider threats across your organisation and network. Azure Advanced Threat Protection can support the most demanding security analytics workloads for the modern enterprise.

Office 365 Advanced Threat Protection

Protect employee email inboxes in real time against unknown and sophisticated attacks through unsafe attachments and malicious links. All suspicious content goes through a real-time behavioural malware analysis that uses machine learning to detect suspicious activity. And if it detects an unsafe URL, it automatically blocks the site so users cannot access it.

Recipe for success

When choosing a vendor or service provider, ensure their policies and practices are worthy of your trust. First determine the types of service you should outsource, the appropriate level of access and whether you can use the cloud (instead of a third party). If you determine that the best option is to go with an outside vendor or cloud service provider, diligently review, vet and scrutinise the potential provider. Find out if they carry insurance in the event disaster strikes.

Ask your potential vendor these questions:

- Do you follow Enhanced Security Administrative Environment (ESAE) best practices?
- Do you enforce restrictions on where Domain Administrator (DA) and Enterprise Administrator (EA) accounts can log in?
- Do you use privileged Identity Management for Active Directory Azure?

INDUSTRY PROFILE

Manufacturing

Securing networks and software against cyberattacks and data breaches is essential. But the supply chain is also vulnerable to security risks.

One manufacturer discovered an intrusion into a system the company used to make service-related announcements. Upon investigation, they found that their customers' email addresses and company names had been compromised.

But it gets worse. Since the data loss, several phishing campaigns have mimicked the company's legitimate communications format. Attackers are leveraging the knowledge that captured email accounts have used the service in the past and will be more likely to click links without proper inspection.

To gain an initial foothold, hackers send phishing emails to a small set of executives and their administrative assistants. The email contains a URL to a malicious Word document. Targets who follow the hyperlink, enabling macros, are considered malicious downloaders.

A malicious downloader allows the attacker to install anything on the infected computer. In this particular case, the downloader installed two applications: one that harvested user financial information and another that stole credentials (acting as a keystroke logger). Everything from corporate credentials to social media login information to remote access authorisations were targeted.

Then, the hackers took it a step further. They used a second malicious Word document to leave a backdoor on nearly a thousand systems, including many high-value servers and domain controllers. The attackers used the captured credentials to live off the land.

STAGE 03

Expanding to the Network

At this point, the attacker has gained widespread access to your network by spreading out from an individual workstation or server into as many systems as possible. The attacker may then install a permanent backdoor or alternate mechanism for long-term access to the systems.

The attacker will use tools, such as a type of malware called "implants", as well as automated viral algorithms. Some methods can appear more legitimate, such as creating fake accounts and gaining remote access. This lets the attacker get back into the network and live off the land (hiding in plain sight in the environment while accessing various resources). Typically when using implants, attackers have a central command-and-control infrastructure for all the resources they control. They use this to ensure that their foothold throughout the network is up and running correctly. If they see any of their controlled access systematically go offline, they know someone is onto them and can try to re-establish their access and evade detection.

Common Techniques

Botnet
A network of private computers infected with malicious software controlled by a malicious hacker or group who can use it for large-scale attacks.

Command and control (C&C)
Servers and infrastructure are used to control many computers via centralised commands, such as a botnet. The black hat hacker running a botnet C&C is called a botnet controller or botmaster.

Implant
A small, hidden program that an attacker installs on your PC without your knowledge.

Living off the land
A phrase that refers to when attackers rely on native resources (as opposed to malware) to maintain a low profile and wreak havoc on a system.

SOLUTION

Comprehensive Defence Posture

As employees use more devices to get their work done, companies are increasingly more likely to store sensitive data in the cloud, on their devices and in on-premise file shares. Sometimes, workers may accidentally or inadvertently share sensitive information with others. For this reason, a comprehensive approach to protecting your sensitive data is critical.

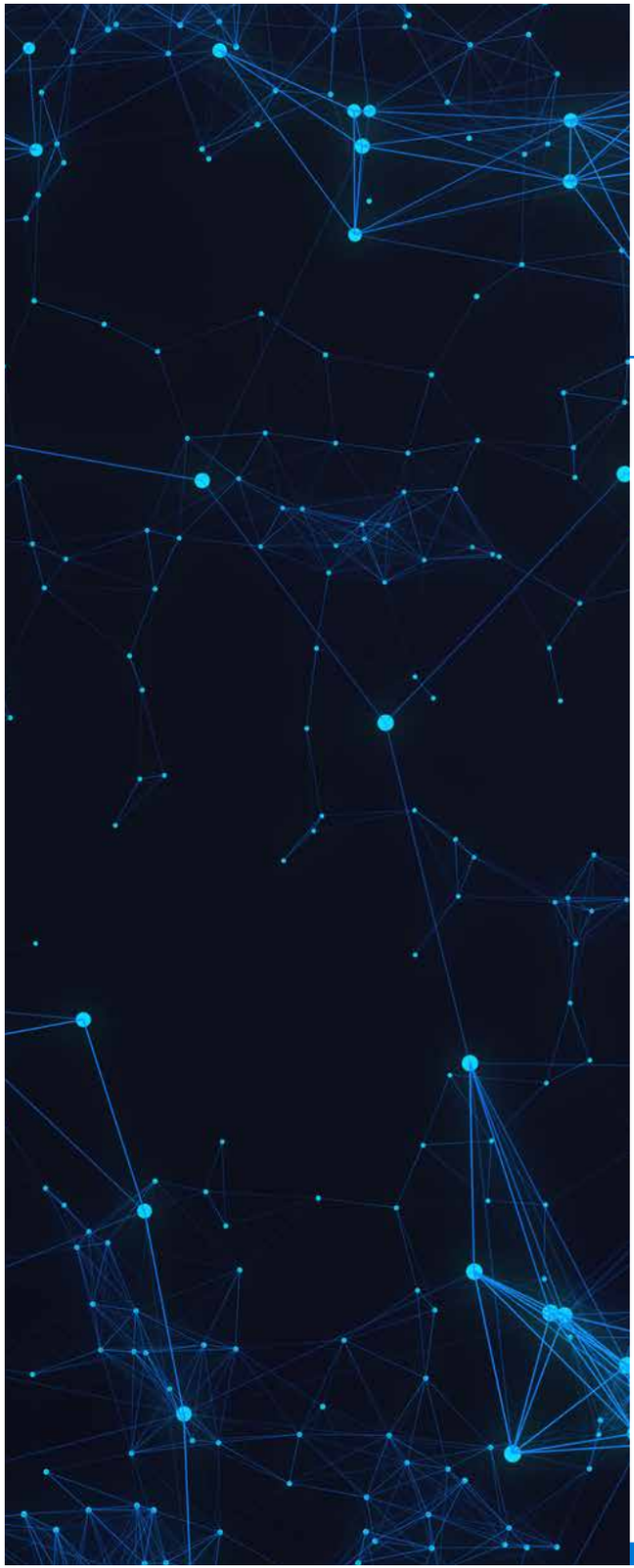
Here are four steps to take when considering a stronger defence posture:

1 **Know where your data lives**
As data travels outside of your company's environment, you need to know where it's being created and shared – whether it's spread out on-premise, geographically, across devices or in the cloud.

2 **Determine your data's level of sensitivity**
Whether it happens automatically or manually, applying sensitivity labels and custom controls to data makes it easier for you to reinforce policies and restrict unauthorised user access.

3 **Apply protective actions**
Once your data's been classified into categories, applying policy rules adds a higher level of protection. You can encrypt files, restrict access, block content sharing, provide end-user notifications and control data usage across the cloud.

4 **Regularly monitor data**
Gain visibility into how employees are using and sharing sensitive information so that you can drill into event details, identify high-risk events and revoke access to documents, data or apps as necessary.



Protect Sensitive Data

We recommend the following defence mechanisms.

Azure Information Protection

Control and secure email, documents and sensitive information wherever it's stored or shared, whether across cloud services or in on-premises environments. With Azure Information Protection, you can classify data based on sensitivity, encrypt data and define usage rights and apply protection without interrupting the working day.

Office 365 Data Loss Protection (DLP)

Keep sensitive information in Office 365 from landing in the wrong hands or being accidentally shared with others. With DLP, you can identify, monitor and automatically prevent sensitive information from being accidentally shared across many locations, help users learn how to stay compliant without interrupting their workflow, and view reports to ensure your organisation maintains compliance.

Office 365 Advanced Data Governance

With proactive policy recommendations and automatic data classifications, you can take actions – such as retention and deletion – on data throughout its lifecycle. With Advanced Data Governance, you can apply compliance controls to on-premises data by intelligently filtering and migrating data to Office 365.

Microsoft Cloud App Security

Get deeper visibility, granular data controls and enhanced threat protection with enterprise-grade security for your cloud apps. Microsoft Cloud App Security enables you to discover and assess risks, protect your information, control access in real time and detect and protect against threats.

INDUSTRY PROFILE

Shipping

Companies in the shipping and transportation industry should keep a risk-based approach to cybersecurity top-of-mind. For some, it might start with addressing legacy applications and dated systems.

One shipping organisation's data was compromised via an internet-accessible legacy web application running on a dated Linux operating system.

Hackers took advantage of the fact that the shipping organisation didn't have centralised monitoring software installed or enabled on their system. Once they gained an initial foothold, they discovered a jump system that wasn't part of the domain: an isolated Windows system in the DMZ. Here, they loaded variants of NBT scanning software and scanned for other NetBIOS-enabled targets, which eventually provided a pathway to the internal network. They also uploaded additional tools for backdoor persistence.

Once the first domain on the internal network was compromised, attackers harvested domain admin-level credentials and used them to connect to other systems, including a domain controller in two different domains. For one of the domains, anti-virus software blocked attempts to steal all user credentials. But the second domain was not so protected and credentials were stolen, and the attacker covered most of their tracks by modifying the system audit logs.

STAGE 04

Staying for the Short- or Long-Term

Bragging rights, revenge, amusement, money, political espionage or a passionate commitment to the freedom of information – a hacker's motivation can influence whether they stay for the short- or long-term.

In an advanced persistent threat attack (APT), attackers want to stay on the network long-term, deploying stealthy and continuous processes, such as monitoring and extracting data while remaining undetected for the longest possible time. They'll create accounts for themselves to ensure that they stay on the network and change passwords to evade detection. For the short haul, attackers may take a smash-and-grab approach, breaching a system and taking whatever they can quickly get, with little interest in staying put.

As in stage three, hackers will use implants or bots to create and preserve several ways to get back into the network and hide in the environment. They use a command and control server to ensure their foothold, explore resources and access channels throughout the network as they please. If they suspect they've been detected, they have the means and resources – like a backdoor – to slip away until the heat dies down and reconstruct their access later.

Common Techniques

Advanced persistent threat (APT)
A targeted attack against a specific entity that tries to avoid detection and steal information over a period of time.

Assume breach mindset
A strategic mindset that business leaders and CISOs adopt, requiring a shift in focus from purely preventive security measures to ongoing detection, response and recovery from threat occurrences.

Backdoor
An entry point into a system or network that enables continued access.

Smash-and-grab
A carefully orchestrated hacking approach where an attacker exploits a system, steals data, then leaves.

SOLUTION

Building Better Security

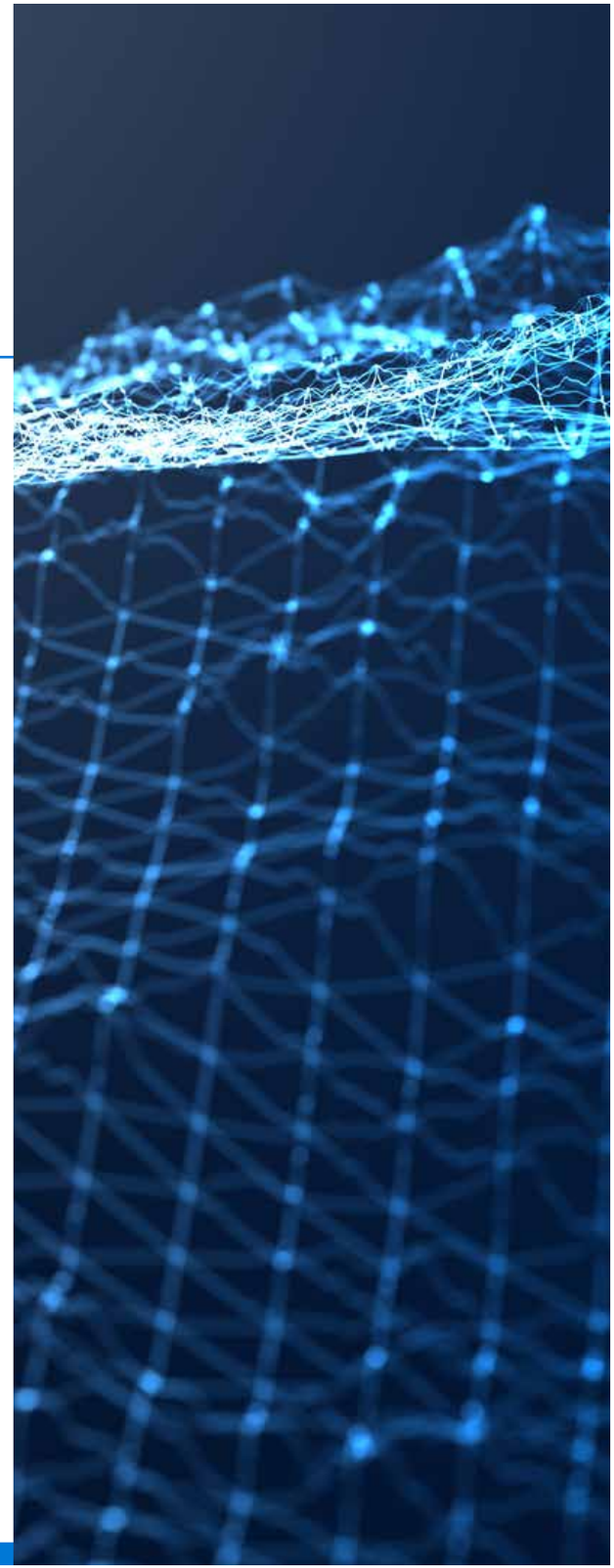
Managing security has never been more complex. Considering multiple point solutions to manage resources across so many environments may seem like a better option, but this often results in less visibility into your entire network's security posture and an inability to correlate incidents to see the bigger picture.

More often than not, maintaining scattered solutions can lead to the most dangerous of these challenges: ineffective responses to threats that grow both in number and sophistication, targeting your organisation and your customers. It's a level of risk you need to be prepared for – and can be.

Whether your assets are deployed in the cloud, on-premises or across a hybrid environment, you need to manage and secure your organisation's security across four core components:

1. Identity
2. Devices or endpoints
3. Apps and data
4. Infrastructure

You need visibility, control and guidance to understand your company's risks, define consistent security policies and elevate your security strategy through actionable intelligence and recommendations.



We recommend using the following tools to mitigate a short- or long-term attack:

Azure Security Centre

Extend protection across clouds and on-premises datacentres, while empowering IT, ops and security teams to easily understand your company's security posture and prevent, detect and respond to threats. With Azure Security Centre, you can monitor and assess Azure workloads' and resources' security state, identify vulnerabilities with continuous assessment, and investigate with advanced log analytics.

Azure Backup

Protect your company's data wherever it resides: in your enterprise datacentre, remote and branch offices, or in the public cloud. Get cost-efficiency and minimal maintenance, consistent tools for offsite backups and operational recovery, and unified application availability and data protection.

Windows Defender Security Centre

Enable your devices' threat management by combining common Windows security features in one easy-to-use app. The Windows Defender Security Centre is a single place to see the status of each of your Windows security features, customise notifications and get help when a threat is detected.

Office 365 Security & Compliance Centre

Manage compliance for all of your organisation's data across Office 365. Grant permissions to people who perform compliance tasks like device management, data loss prevention, eDiscovery, retention and more.

Purchase protection

The best way to prevent hackers from attacking through a remote access connection is to simply ban remote access, but this isn't realistic for many enterprises, including those in retail or online services.

Here are some safer ways to allow vendors to access your network:

Publish via Azure

Move certain in-house workloads, such as web interface access and backend databases, to a trusted cloud platform as a service (PaaS). The cloud workload can be kept at a minimal level of access to only required data on the in-house network. This method limits the number of users that have direct access to a customer's network and it reduces the privileges that a user within the network needs to have by limiting access to only required PaaS resources.

Multi-factor authorisation (MFA)

Users are required to provide additional verification beyond just a username and password, such as using a phone call or text message to confirm their identity.

Migrate from a remote desktop connection (RDP) server to virtual machines (VMs) in Azure:

Using VMs lets you maintain unique passwords for network segments and control access to information.

INDUSTRY PROFILE

Service Automation

Service automation companies are increasingly becoming a hacker's target, particularly to cause reputational damage or to use as a stepping stone to gain access to other organisations.

When a professional service automation organisation suspected a potential compromise, an investigation revealed three distinct sets of attack activity on the corporate network using several tools customised for the organisation. The attacker leveraged their access along with evidence of potential exfiltration.

Hackers compromised a domain account with local admin privileges for 1,000 machines with the ability to gain access to an additional 50,000 machines. The attackers logged on, installed a remote access tool, and stole credentials – remaining undetected for three months.

Several user systems and domain controllers were controlled by the attacker using a legitimate account via an external VPN connection. Even though this organisation didn't consider itself a target, its lack of focus on secure design and detection allowed attackers to persist through the use of keyloggers to maintain current account access. With these credentials, attackers used legitimate remote tools to access both the network infrastructure and critical data stores. The lack of detection was proven by the significant amount of commodity malware, ransomware and uncontrolled access. All of this allowed the attacker to easily blend into the environment.

CONCLUSION

Protect, Detect, Respond

Ready to improve your enterprise security posture? We recommend taking a holistic approach. Understand how targeted attacks typically succeed. Recognise that it's not a matter of if – but when – you'll be attacked. Both long-term compromises and short-term attacks to enterprise systems happen regularly, so actively look for them and take steps to mitigate your risk. Know how to quickly and effectively respond to a targeted attack with an incident response strategy.

Keep these four things in mind:

Preparation pays off

Planning for a major incident can reduce company damage, cost and management difficulty.

Operationalise your incident management processes

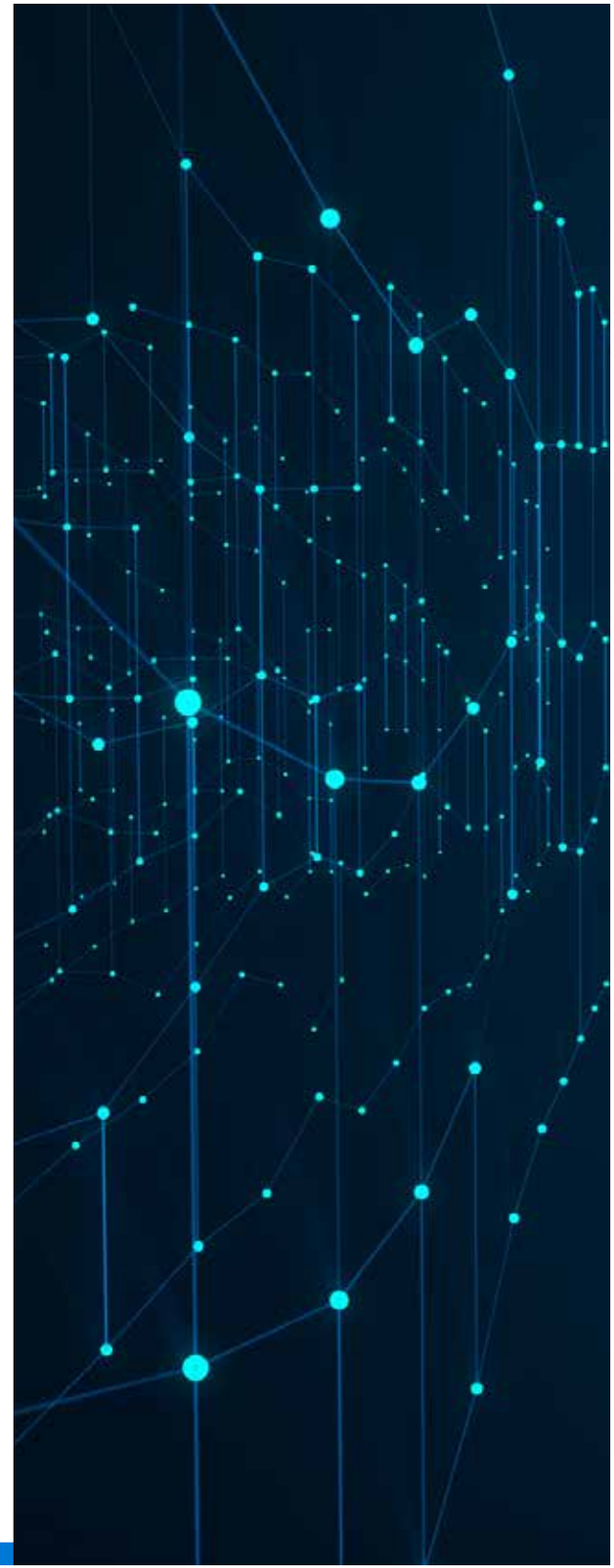
Include major cybersecurity incidents in your standard business risk management processes.

Coordination is critical

Effective cybersecurity incident management requires collaboration and coordination amongst technical, operations, communications, legal and governance functions.

Stay calm, and do no harm during an incident

Overreacting can be as damaging as underreacting.



We've broken down the strategy into three steps:

01

Protect

Take a risk-management, least-privilege approach. Ask these questions:

- Does this person really need access to that resource?
- Do we know where our data is?
- Do we know who has access to it?
- Are we compliant where necessary?
- Is our software up to date?

02

Detect

Be suspicious and assume you will be breached. Ask these questions:

- How will we know when a breach happens?
- Do we have the right tools in place to detect a breach?
- Do we have the right tools in place to analyse a breach?

03

Respond

Verify that you have a response process set up with appropriate triggers. Ask these questions:

- How will we respond to a breach?
- How will we manage damage to assets and our reputation?
- Do we have a customer communications plan in place?
- How will we learn from this?

Microsoft is committed to supporting organisations that are looking to prevent, detect and respond quickly to cybersecurity threats.

To learn more about Microsoft security solutions and services, visit www.microsoft.com/secure

For comprehensive guidance on how to reduce your organisation's business and security risk during an incident, visit https://aka.ms/IRRG

Microsoft