Anatomy of a Breach

How hackers break in – and how you can fight back

A cyberattack can cost your company millions. Do you have the right plan in place to resist, mitigate, and recover from a breach?

Microsoft

TABLE OF CONTENTS

Introduction

The Four Stages of a Breach

The Four Stages of a Breach

Security threats are relentless. Before you know it, a cyberattack can cause millions of dollars in damage, both to your company's bottom line and to its reputation. Are you aware of the potential threats to your company? And do you have a plan in place to resist, mitigate, and recover from the four stages of a breach?

Read on to learn more about each stage and examine some real-world examples of the types of damage that attackers do during each one. You'll also learn how to formulate an "assume breach" defense strategy to help protect yourself and your company.

Stage One:
Getting an Initial Foothold

Stage Two:
Gaining Elevated Control
(Local Escalation of Privilege)

Stage Three:
Expanding to the network
(Active Directory Escalation of Privileges)

Stage Four:
Settling in for Long-Term Persistence

Stage One: Getting the Initial Foothold

The tiniest opening can allow an attacker to gain a foothold in your organization. Whether through a compromised workstation, an unpatched Internet-facing server, or a badly configured third-party managed device, an attacker can and will use anything available to breach a company's defenses and gain access into its network. Once inside the system, a hacker can perform the necessary reconnaissance to identify and target your organization's valuable information or resources.

Common Terms:

Phishing: A way to trick users into giving out personal, financial, or enterprise-specific information that could be used to gain unauthorized access to internal infra-structure. Attackers may use phony websites or email messages that look like they are from a trusted contact (for example, from third- party vendors or other internal employees) to entice users to click malicious web links, documents, and other infection points.

Watering hole: A specific website that attackers have identified as being frequently visited by their intended target. The attacker places malicious links to malware on the site in the hope that the target will be infected when they go there.

Malware: Short for malicious software, these programs perform unwanted actions on your PC such as stealing information, locking your PC until you pay a ransom, or using your PC to send spam. Viruses, worms, and Trojans are all types of malware. (This document focuses on what is often called targeted malware, the kind that is designed to infiltrate a specific industry or organization.)

Exploit: A piece of code that uses software vulnerabilities to access information on your PC or install malware.

Zero day: A software exploit that hasn't been disclosed or patched by the software vendor.

Industry profile: Healthcare

The healthcare industry has witnessed significant consolidation within the past few decades as hospitals merge. Although consolidation has been successful from a healthcare perspective, the process of merging often creates technology challenges for staff. Newly combined hospitals may choose to reduce their overall information technology investment by centralizing IT services into a single department.

The process of merging networks, infrastructure, and software can lead to a breach if not handled correctly. Attackers typically begin by breaching the network that has the weakest security. Once they are in, they can use internal security weaknesses to get access to the more secure network. In one real world case, an attacker got into one network and then used social networking via email to crack another hospital's network. The hospital realized something was wrong when an upgrade caused stability issues in its servers, and investigators discovered a long-standing piece of malware that enabled the compromise of the network.

Many factors contributed to the overall breach. The hospital didn't segregate its network from other organizations, allowing attackers to enter through the less-protected network. Common credentials were used throughout the network, making it easier for attackers to access different areas once they were in. Plus, legacy applications developed in-house were operating with privileges that were too open. It took several years to redesign and rebuild the network, plus a cultural shift to reclaim it.

Once a foothold is established, an attacker's job becomes easier. Entering a network through one of these methods allows an attacker to uncover more powerful credentials, opening up new, potentially more sensitive areas of the network.

An Ounce of Prevention...

Stronger security measures, including staff training and implementing the right technology solution, can help hospital networks stay healthy.

We recommend the following preventive measures:

Implement a solid foundation of industry security standards: Segregate networks, enforce strong password requirements, follow "least privilege" practices, and require individual passwords for each network or access area. This is particularly critical for legacy devices that are susceptible to attack, but cannot be patched.

Upgrade networks: Keep network infrastructure up to date to ensure you have the latest security

Use solutions with assurance built in: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to all U.S. healthcare companies and establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. Microsoft's Cloud Services are compatible with HIPAA, and the Advanced Threat Protection feature in Windows 10 and Office 365 automatically screens all attachments and links included in incoming email for potential threats. Questionable material is not allowed to reach the end users, reducing social engineering threats to your network.

Stage Two: Gaining Elevated Control

Once an attacker has infiltrated an organization, the next step is local escalation of privilege. Attackers typically look for a way to consolidate their control of the local system, or they look for another system that offers a higher chance of success in gaining administrative privileges or greater access to valuable data. The attacker's goal is to identify the user accounts that are responsible for managing the system to impersonate the ability of those accounts to manage, update, and access system resources. Then, using both built-in and downloaded tools, the attacker attempts to identify other systems of interest and network resources, and to capture usernames and passwords. Typically, these actions cannot be accomplished as a normal user.

Common Terms:

Keyloggers: Malware that records which keys a user presses. Also known as keystroke logging. Recording keystrokes enables attackers to collect the usernames and passwords to log into the target organization's network.

Pass the hash (PtH): A technique where an attacker uses the underlying hash (code) of a victim's password to masquerade as that user. The attacker doesn't need to know the actual user credentials to authenticate to a remote server/service.

Network scanning: Attackers use this reconnaissance technique to catalogue the systems that are currently accessible to them, such as the host machines, services, and resources that are active on a network. The attackers then create a target list of interesting systems that they will attempt to access with their newly acquired administrative credentials.

Industry Profile: Entertainment Media

Take one high-profile industry, add in some controversial content, and you have a target for hacktivists. Attacks on media and entertainment organizations are often driven by a desire to make a statement as much as a wish to steal information. Past hacktivist attacks have caused chaos by releasing sensitive company information or taking over an organization's websites.

In one such case, a company suffered a breach that not only stopped it from functioning, but leaked sensitive data about employees, customers, and intellectual property. While it isn't fully known how this breach originally occurred, similar cases have arisen from well-known attack vectors such as social engineering, unpatched vulnerabilities, and simple misconfigurations.

For a media company, the damage can be far reaching. The breadth and probable impact of this breach—both financially and geopolitically—was unprecedented. In addition to the tangible costs of finding and shutting down the actual attack, the larger cost is to the company's reputation: It must now spend time and money repairing relationships that could be better spent developing new projects.

A Winning Network Solution

Developing a stronger security strategy can help prevent a devastating attack, and a key part of that is comprehensive risk management. 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 those assets. It's also critical to be able to detect when an issue occurs, contain it, and respond to consequences effectively. These approaches should be seen as part of the lifecycle on security within an organization where risk is evaluated on an ongoing basis and lessons learned feed back in to the system.

We recommend betting on these security measures:

Protect, detect, respond: This approach helps build a framework around securing systems and is one of the approaches Microsoft and other companies use to understand risk, deal with an eventual breach, remediate, and learn from it.

Implement "least privilege" access: Define your network's access controls based on roles rather than individual work styles, and then restrict access to the minimum required to complete assigned duties and functions. If an individual doesn't need access to a network or a resource for their job, don't grant it. This is a common way to help contain breaches.

Security Development Lifecycle: This software development process helps developers build more secure software and address security compliance requirements while reducing development costs.

And putting these tools to work:

Local Administrator Password Solutions (LAPS): This solution can be used to set a different, random password on every computer within a domain. Then, domain controllers can use it to determine which users (e.g., helpdesk administrators) are authorized to read passwords.

Windows 10 Credential Guard: This virtualization-based security, introduced in Windows 10 Enterprise, isolates secrets so that only privileged system software can access them.

Microsoft Advanced Threat Analytics (ATA): Helps you identify PtH breaches and threats using behavioral analysis.secure software and address security compliance requirements while reducing development costs.

Industry profile: Food Manufacturing

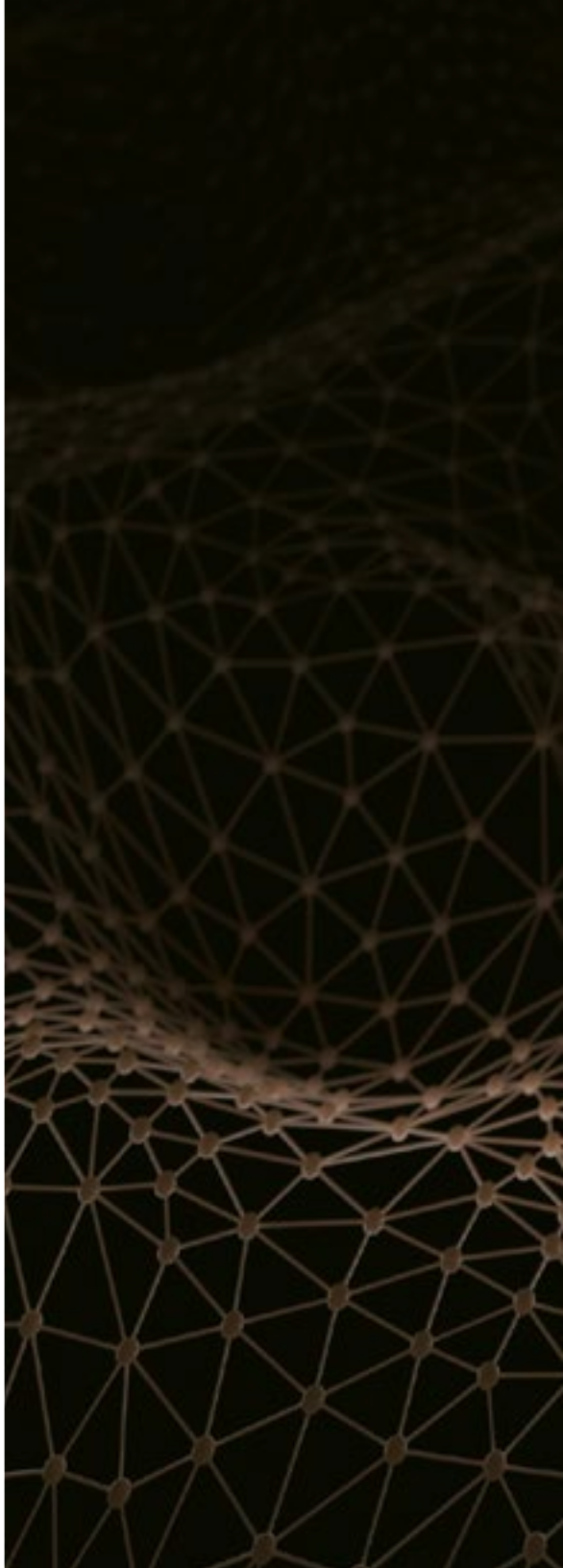
A large beverage company knew it needed to do more to improve network security while reducing IT costs, but didn't know where to start. It decided to outsource its IT and focus on what they it did best: making refreshing drinks. Outsourcing the work to an IT company should have made the company's data more secure. Instead, the beverage manufacturer got burned. The vendor company failed to follow due diligence processes when protecting the customer's critical accounts. It also failed to maintain high integrity with the customer's high-value accounts, which accessed high-value servers.

In this case, because the IT vendor did not segregate the beverage company's accounts from the vendor's normal activity, these accounts were exposed to normal attacks such as social engineering through vendor employee email and the happenstance of web surfing. Once the attacker obtained the beverage company's accounts, the attacker was able to administer the beverage company remotely just like the IT vendor. To make matters worse, the beverage company had to respond through the IT vendor as the customer's backbone systems were no longer held locally. This made the investigation coordination and remediation effort difficult until these critical accounts were brought under control by the remediation team.

Some critical workloads could be outsourced while the beverage company kept the "keys" to its data and backbone systems within the organization. Costs could be reduced without outsourcing by moving some business systems to the cloud (for example, by replacing an onsite email deployment with a hosted and managed solution, such as Office 365) while focusing in-house workstreams on core manufacturing. A hosted solution helps reduce employee workload, creates predictable monthly costs, maintains the business's control, and leverages the expertise of the service provider.

If the environment includes many systems with excess capacity, the company should consider shifting them to a trusted cloud service. The cloud provides the ability to have full platform, infrastructure, and services without having to set up and maintain all the systems and datacenters. The company does not have to manage patching and administering operating systems and hardware.

It is always important to ask questions, be it of an outsourcing vendor or a cloud service provider, about its practices and policies on data security, privacy and control, compliance, and transparency. If the beverage company had identified the risks in the outsourcing company's security practices, it could have made a more informed decision about where to place its trust.



Recipe for success

Outsourcing IT functions can be an attractive solution in terms of reducing overhead. However, it's imperative to investigate whether IT outsourcing will provide the best defense of your company's data and intellectual property—and then you must choose a vendor or service provider whose own policies and practices are worthy of your trust. As the beverage company discovered, the benefits of outsourcing must be balanced against the risk of placing your data security needs in the hands of an outside business.

We recommend asking the following questions before searching for a vendor :

- **What types of services should we outsource?**
- **What level of access should we outsource?**
- **How can we use the cloud to reduce IT costs (instead of outsourcing to a third party)?**

After you review your situation, you may determine that going with an outside vendor or cloud service provider is the best option. Make sure to review, vet, and scrutinize the potential provider diligently. Ask it questions, and find out if it carries 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 regarding where Domain Administrator (DA) and Enterprise Administrator (EA) accounts can logon?**
- **Do you use privileged Identity Management for Active Directory Azure?**

Stage Three: Expanding to the network

In stage three, the attacker gains 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; some of these might be malware (called implants). Some methods can appear more legitimate, such as creating fake accounts and gaining remote access so that the attacker has several ways not only to get back into the network but to hide in the environment and access various resources. Typically when using implants or bots, attackers have a central "command and control" console for all the resources they control. They use the "C&C" to ensure that their foothold throughout the network is up and running correctly. If they see any of the access they control go offline systematically, they know that someone is on to them and can try to reconstitute their access and evade detection.

Common Terms:

Bots: Small, hidden programs that are installed on your PC by an attacker without you knowing.

Botnet: Malicious system in which multiple copies of a bot are installed on many PCs and controlled by a malicious hacker, who can use it for large attacks.

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

Industry profile: Government Institution

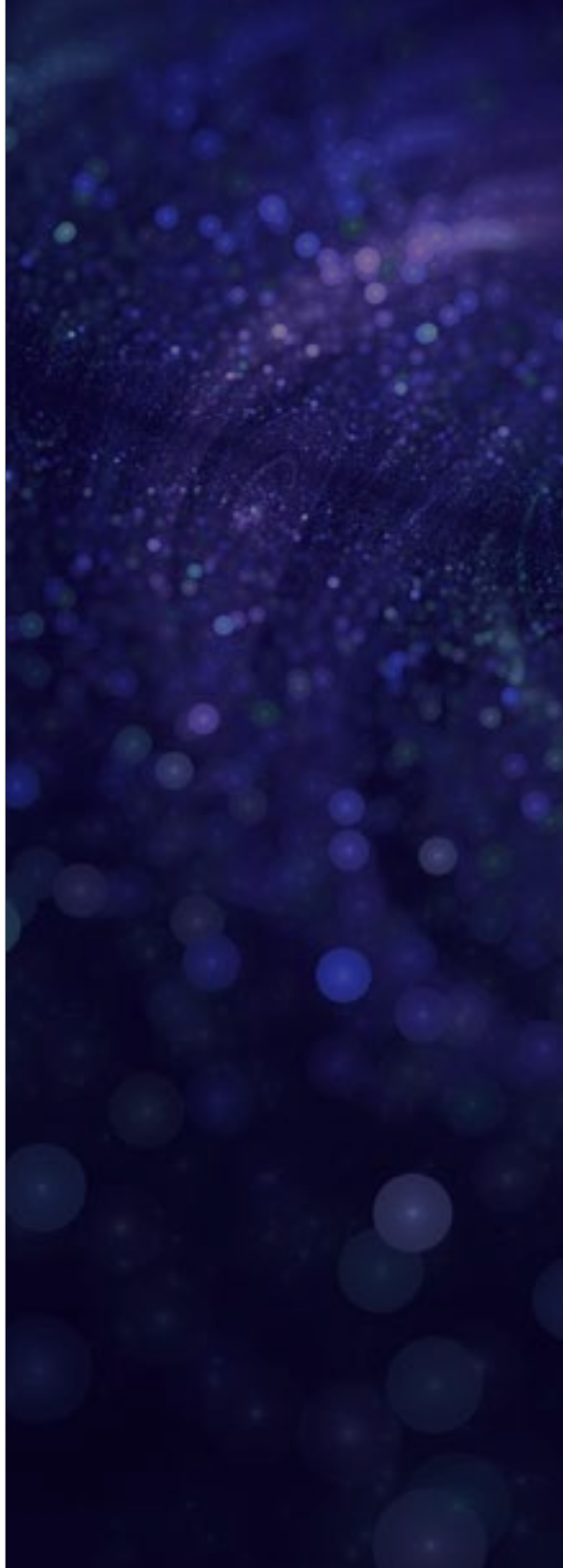
This government institution did almost everything right. Software was patched in a timely manner, a relatively low number of end users had administrative rights, and routine security checks (reviews) were being performed. Bonus points for maintaining dedicated administrative workstations for Domain Administrator (DA) and Enterprise Administrator (EA) use. (DAs and EAs regulate all other accounts in an organization. Very few people in an enterprise should have this level of access, and assignment of DA and EA credentials should be closely monitored.)

The organization's fatal flaw: using the same local administrative password across the enterprise for HR, accounting, and critical IT management computers. How do smart people with a government's resources at their disposal make this error?

Using shared local administrative passwords is a standard practice in many organizations that don't realize the risk. Sometimes the initial setup of systems doesn't work as expected with limited accounts. To resolve the issue, administrators will give those accounts more rights until the application functions. If the issues aren't resolved, the administrator may leave the extra rights in place as a workaround. In other situations, local accounts may be used in an emergency, and then left on the system for future use. In either case, the system is now open to attack. These IT behaviors reveal a security mindset that thinks only locally and cannot provide proper protection in the threat landscape of today's always- on, always- connected Internet.

In the case of this government office, an attacker was able to get into the network when a user accessed either an infected document or clicked a link to a website that hosted malicious code. (The exact point of infection is not known.) Because the organization used the same local administrative password across departments, the attacker was able to explore the network and harvest DA and EA credentials. These credentials were the "keys to the kingdom": the attacker was able to implant code in datacenters, servers, and on Microsoft Exchange, resulting in a complete network compromise that cost millions of dollars.

The literal costs of the hack included rebuilding systems, reissuing passwords, and public investigations on data theft and "what went wrong." You can't put a dollar figure on the loss of trust experienced by the victims of the hack.



Comprehensive Defense Posture

The government institution did a lot of things right, but it takes a comprehensive approach to successfully block an attack.

We recommend the following defense mechanisms:

Microsoft Enhanced Mitigation Experience Toolkit (EMET): This utility helps prevent software vulnerabilities from being successfully exploited.

Microsoft Office 365: This suite of products is designed to help meet your organization's security needs, including data usage with legal, regulatory, and technical standards.

Enhanced Security Administrative Environment (ESAE): Leverages advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.

Privileged Identity Management for Active Directory: Allows you to manage, control, and monitor your privileged identities and their access to resources in Azure Active Directory plus other Microsoft online services (e.g., Office 365 and Microsoft Intune).

Microsoft Advanced Threat Analytics (ATA): Uses behavioral analysis to monitor anomalous use of accounts and credentials.

Operations Management Suite (OMS): Cloud-based IT management solution that helps you with monitoring, alerting, and tracking an attacker.

Stage Four: Settling in for Long-Term Persistence

In stage four, the attacker settles in for the long haul, deploying stealthy and continuous processes, such as using malware to exploit vulnerabilities and monitoring and extracting data while attempting to remain undetected for the longest possible time. Attackers will create accounts for themselves to ensure that they stay on the network, and they'll change passwords to evade detection.

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 C&C to ensure their foothold and explore resources and access channels throughout the network as they like. If they suspect they've been detected, they have the means and resources to slip away and reconstruct their access.

Common Terms:

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: This is a strategic mindset. For business leaders and CISOs, it means shifting your focus from purely preventive security measures to detection, response, and recovery from security issues.

Industry profile: High-Tech Manufacturing

Hackers can be very, very patient. After infiltrating a network, they can go undetected for hundreds of days. During this time, they will rebuild systems, overwrite logs, and update their hacking tools. A high-tech manufacturing company had an uninvited guest on its network for at least one-and-a-half years before detecting the hack. During that time, the attacker successfully implanted advanced targeted malware into a customer's Home Drive Server, which housed virtually all of the customer's intellectual property (IP).

The customer's PowerPoint presentations, documentation, project schedules, and manufacturing process details were all now available for the attacker to harvest on a regular basis. A massive amount of research and development information was stolen from various parts of the customer's network before the breach was discovered.

Building Better Security

No one knows how the attackers got into the manufacturer's customer's network. Based on the nature of the attack, we know that the attackers found a way to authorize themselves to implant the malware.

We recommend using the following tools to prevent this type of breach:

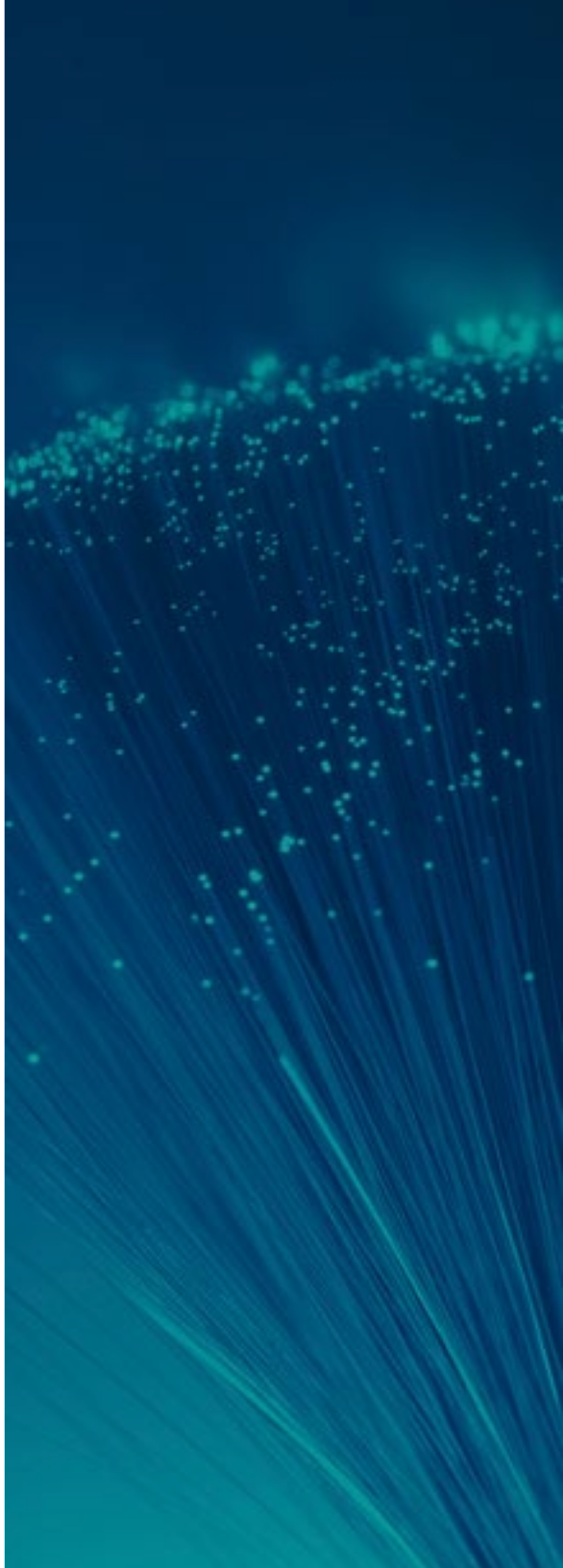
Advanced Threat Protection: This feature in Office 365 automatically screens all attachments and links included in incoming email for potential threats. Questionable material is not allowed to reach the users, reducing social engineering threats to your network.

Multi-factor authorization (MFA): Requires users to provide additional verification beyond just username and password; for example, by using a phone call or text message to confirm the user's identity.

Azure Rights Management (Azure RMS): This information protection solution uses encryption, identity, and authorization policies to help secure your files and email. It works across multiple devices, including phones, tablets, and PCs.

Microsoft OneDrive: This cloud storage solution offers several ways to help keep files safe. Files stored in OneDrive are never shared with other users unless you store them in a Public folder or you choose to share them. You can enhance security by creating a strong password, adding security to an existing Microsoft account (for example, with your alternate email address or a security question), and by using two-step verification.

Microsoft Datacenters: Microsoft leverages decades of experience building enterprise software and running global online services to create security technologies and practices that you can trust. Our datacenters are physically constructed, managed, and monitored with fences, guards, background checks, biometric access controls, security training, and the equivalent of a hard disk shredder for disposing of servers. All datacenters have 24-hour monitoring, multi-factor authentication (including biometric scanning), and an internal network isolated from the public Internet.



Industry profile: Internet Retail Company

Our last cautionary tale comes from the Internet.

You may have heard about some high-profile breaches of online retailers where the attacker is after customer data for criminal profit. Online retailers typically offer remote network access to key vendors, such as credit card services, with very few restrictions. (In some cases, it's almost employee- level access.) That's the first red flag. The second is a lack of network segregation. In other words, once someone is in, they can move freely about the hacked organizations servers.

We know of multiple cases in which attackers gained remote access to a target company's servers through their vendor connections. Once in the system, the attacker moves about masquerading as a vendor, reconnoitering systems and attempting to crack the critical ones containing financial data or accounts that can access such data. In other words, attackers hacked one company to gain access to another company with which it does business.

The stock of retail companies attacked in this way can lose significant value in a week after a breach. Compromised companies can also be hit with stiff government fines reaching into the billions—especially in regulated industries (that is, those with compliance mandates). Moreover, fines and lawsuits may be leveraged against a company that proves to have been the weak link vector of an attack. Some companies maintain insurance to handle breach issues.

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 online services and in retail.

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 both the number of users that have direct access to a customer's network, and it reduces the privileges a user within the network needs to have by limiting access to required PaaS resources only.

Multi-factor authorization (MFA): Requires users to provide additional verification beyond just username and password; for example, by using a phone call or text message to confirm the user's identity

Migrate from a remote desktop connection (RDP) server to virtual machines (VMs) in Azure: Using VMs allows you to maintain unique passwords for network segments and control access to information.

Conclusion

Protect, Detect, Respond

Protect, Detect, Respond

Ready to improve your enterprise security? We recommend taking a holistic approach. Understand how targeted attacks typically succeed. Recognize that an attack is not a matter of if, but of when. Long-term compromises to enterprise systems happen regularly, so actively look for them and take steps to mitigate risk. Know how to respond effectively and quickly to a targeted attack.

We've broken the strategy into three steps:

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

- Does that person really need access to that?
- Do I know where my data is?
- Do I know who has access to it?
- Do I know whether I am compliant where needed?
- Is my software up to date?

Step Two: Detect.
Assume you will be breached. Have a suspicious mind. Ask these questions:

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

Step Three: Respond.
Verify that you have a response process, and that it is 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 helping you keep your data and systems secure and private. To learn more about best practices for cyber-security, privacy and control, and compliance in your organization, visit www.microsoft.com/trustedcloud.

The Trusted Cloud team gratefully acknowledges Bruce Cowper, Kasia Kaplinska, Matt Kemehar, IB Terry, and Yvette Waters for sharing their time, knowledge, and talent in the development of this eBook.