veeam

10 Steps to Microsoft 365 Cyber Resilience

Table of Contents

1. Multi-factor Authentication 5

2. Least-privilege Access 6

3. Regular Backups 7

4. Immutable Backups 8

5. Incident Response Plan 9

6. Regular Audits and Penetration Testing 10

7. Software Restriction Policies 11

8. Monitoring and Logging 12

9. Data Separation 13

10. Encryption 14

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The Rise of Microsoft 365 Cyberattacks

Protecting Microsoft 365 data is an essential aspect of a modern cybersecurity strategy, as the suite's applications permeate the daily operations of countless businesses and operations. With a wide array of productivity tools, including Exchange, Teams, SharePoint, OneDrive, and more, Microsoft 365 contains a wealth of sensitive information and critical business data — and is the reason more organizations than ever are investing in third-party solutions or managed backup services to protect it.[1] In fact, there is evidence that ransomware is being designed for the specific purpose of infiltrating Microsoft 365 and other SaaS applications. According to a report by Coalition, there was a 12% increase in cyber claims in the first half of 2023, driven by ransomware attacks, with an average ransom demand of $1.62 million.[2] As a consequence to its widespread use, and as more employees install and use Microsoft 365 on work-from-home machines, the platform has become particularly exploitable to attackers capitalizing on this diversified infrastructure.

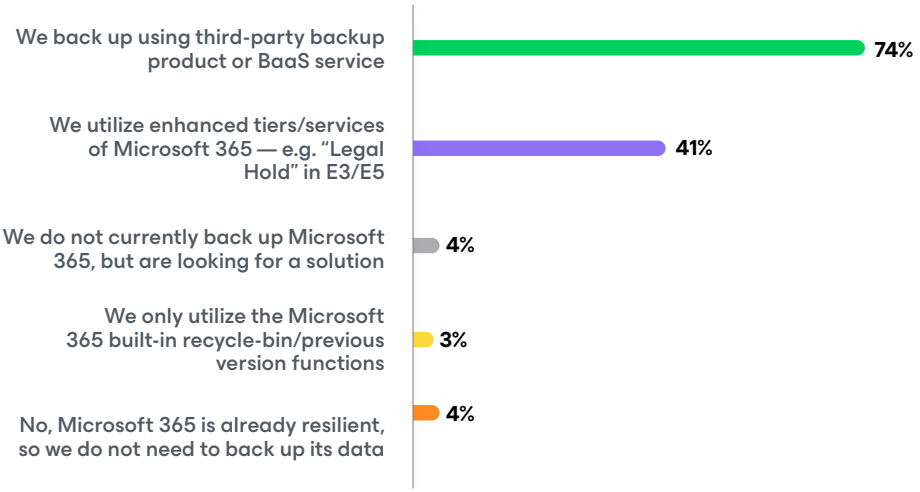
12%

increase in cyber claims in the first half of 2023

$1.62 M

is the average ransom demand

Does your organization back up the data from within Microsoft 365?



[1] 2024 Data Protection Trends Report

[2] Microsoft 365 Ransomware: Your Comprehensive Guide to Understanding, Prevention, and Recovery

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

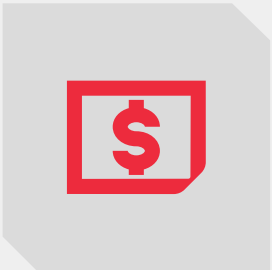
The risks associated with losing Microsoft 365 data are therefore not only complex, but very real. Data loss results in serious operational disruptions and can inflict significant financial damage due to downtime and lost productivity. In one report, IT leaders estimated the cost of downtime to be $1,467 per minute ($88,000 per hour)[3] — which, given the sheer volume of time spent and work accomplished using Microsoft 365 in the typical workday, is a cost which comes as no surprise. Further, when sensitive data is exposed, organizations face hefty compliance penalties and reputational harm — in the case of GDPR infringements, fines as high as $21 million.[4] Given that Microsoft 365 data is enormously sensitive to organizations and their employees, data loss events are more than likely to erode not only a customer's trust, but that an employee, potentially leading to a decline in business and long-term reputational damage both in and out of the company.

The possible consequences of unprotected Microsoft 365 data cannot be overstated. Breaches that expose personal information can lead to identity theft and fraud, causing harm long after the initial compromise. For businesses, the loss of intellectual property can erode competitive advantages and result in costly legal battles or fines, who may also face litigation if they are found negligent in safeguarding their customers' data.

There is no way around it. A proactive approach to securing Microsoft 365 data is more than an innovative idea — it is an imperative to ensure businesses maintain continuity, uphold legal and regulatory responsibilities, and maintain customer trust.

[3] 2022 Data Protection Trends Report
[4] What are the GDPR Fines?

Cost associated with data loss



The cost of dowtime to be $1,467 per minute ($88,000 per hour)

In the case of GDPR infringements, fines as high as $21 million.

Breaches that expose persona information can lead to identity theft and fraud.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Steps to Prepare for Attacks

1. Multi-factor Authentication

Multi-factor Authentication (MFA) is an essential security measure that requires users to provide two or more verification factors to gain access to digital resources, such as email accounts, business applications, and online services. MFA significantly enhances security by adding layers of protection beyond just a password, meaning that even if a cybercriminal obtains a user's password, they still need to bypass the additional authentication factors to gain access. This is nothing short of a formidable barrier against unauthorized entry.

The benefits of MFA are many, especially in the context of Microsoft 365, where sensitive data and corporate communications are perpetual. MFA can defend against the consequences of common cyberattacks such as phishing, where attackers deceive users into disclosing credentials. This additional authentication step can be something the user knows (like a PIN or security question) or something the user has (like a smartphone or company hardware).

Even in scenarios where passwords are compromised due to weak or reused passwords, an MFA setup will continue to shield the account from unauthorized access. This level of security is critical in Microsoft 365 environments, where remote access is routine, and users may be connecting from unsecured networks or personal devices. Overall, as a simple and reassuring fact, MFA creates a dynamic defense mechanism that adapts to the evolving threat landscape.

Benefits of MFA

Defends against the consequences of common cyberattacks

Continues to shield the account from unauthorized access

Creates a dynamic defense mechanism that adapts to the threat landscape

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

2. Least-privilege Access

The principle of least privilege is a cornerstone of effective cybersecurity practices, integrally related to the concept of a Zero Trust architecture, and it is instrumental in fortifying an organization against potential cyberattacks. A Zero Trust architecture operates under the assumption that there are threats both outside and inside the network, such that no users or systems are automatically trusted.[5] This dovetails the principle of least privilege, which dictates that users should be granted minimum levels of access (or permissions) necessary to perform their job functions — and no more. For Microsoft 365, implementing these principles might mean restricting access to certain documents, folders, sites, administrative settings, and applications based on the user's role within the organization.

Adopting a least-privilege access model can severely enhance the security posture of your Microsoft 365 environment. Firstly, it minimizes the suite's potential attack surface for cybercriminals. If a user's account is compromised, the attacker is limited to the access rights of that account, which ideally should be as restrictive as possible. For example, if a user's credentials are stolen, the attacker won't be able to access sensitive information or perform administrative tasks if those rights aren't associated with the user's account. This damage limitation creates a quarantine zone for any security breaches and is pivotal in controlling the spread of an attack within an organization.

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

3. Regular Backups

As a prime target for cybercriminals, backups are extremely important for Microsoft 365 — especially when you consider Microsoft's Shared Responsibility Model[6] which states that organizations are responsible for the safety of their data. Ransomware poses a significant threat to data integrity, as attackers aim to encrypt an organization's files and demand payment to release them. Nevertheless, threats to data aren't limited to malicious attacks. Data can also be jeopardized by accidental deletions or various other mishaps. Keeping up-to-date backups allows the organization to swiftly regain access to their data irrespective of whether the loss results from ransomware, human error, or the many other critical reasons to maintain Microsoft 365 backups.[7] This not only minimizes downtime, but also sends a strong message that the organization is not an easy target for future attacks.

Implementing a regular backup routine means establishing a schedule that strikes a balance between the volume of data handled and the resources available for backup operations. This should include backing up emails, documents, contacts, calendars, and any other data stored within the Microsoft 365 suite.

Think of it like having an insurance policy. It might not be needed every day, but when disaster strikes, it can be the difference between a quick recovery and a lethal catastrophe.

[6] Shared Responsibility in the Cloud

[7] 7 Critical Reasons for Microsoft 365 Backup

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

4. Immutable Backups

Immutability plays a pivotal role in securing an organization's digital assets against alteration or deletion, whether by cyberthreats or human error. For Microsoft 365, where vast amounts of data are routinely generated, shared, and stored, ensuring that backup copies are impervious to change is a critical element of a robust threat-mitigation strategy. Immutability guarantees that once information is backed up, it remains in a pristine state and is unalterable for a set period of time.

For organizations using Microsoft 365, immutable backups stand as a shield against ransomware attacks, which target not only live operational data but also backup repositories. In fact, according to one survey, almost all ransomware attacks (93%) specifically target backups.[8] For further security measures, an immutable backup copy of the data is important. By creating and enforcing retention policies that protect backup data from being overwritten or tampered with, businesses can defend their continuity practices against unwanted encryption or destruction of data. Immutability ensures that, despite any security breaches affecting current data stores, the organization can restore operations from a clean, unaltered backup.

93%

of ransomware attacks specifically target backups.

[8] 2023 Ransomware Trends Report

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

5. Incident Response Plan

An incident response plan is a well-structured one. It details the processes an organization must follow when faced with various cybersecurity incidents, serving as playbooks for identifying, containing, eradicating, and recovering from security threats, and ensuring all stakeholders are informed and prepared to act.

For organizations using Microsoft 365, the foundation of a strong incident response plan includes identifying critical assets within the Microsoft 365 ecosystem. This means pinpointing where sensitive data is stored, whether it is within OneDrive, SharePoint, Exchange Online, or elsewhere. Once these assets are identified, the plan should define potential threats and create a prioritized list of risks, alongside strategies for mitigating them. This includes the use of integrated monitoring and detection tools, immediate containment strategies, threat eradication, robust communication between parties, and the identification and recovery of any lost or compromised data.

The glue that holds an incident response plan together is thorough preparation. This goes beyond technical tools, training and collaboration of IT and security teams, but for all employees. For those using Microsoft 365, organizations should conduct regular education sessions tailored to its intricate ecosystem. Employees using applications within Microsoft 365 like Outlook and Teams must be equipped with the knowledge to discern and react to suspicious activities, which can come in the form of seemingly legitimate messages, fake meeting invitations from coworkers, or authentic-looking emails from company leaders. People can be a cybersecurity weakness for any organization, but well-trained employees have the potential to form a formidable barrier against threats.

An incident response plan start with

Comprehensive Incident Response Framework

Identifying Critical Assets

Importance of Employee Preparedness

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6. Regular Audits and Penetration Testing

Regular audits and penetration testing are integral components of maintaining a resilient Microsoft 365 environment. In fact, Microsoft 365 itself provides an array of built-in tools for auditing and threat detection,[9] serving as a baseline to fortify its environment against various security threats. These practices serve as proactive measures, enabling firms to identify and rectify problems before they can be exploited as attackers.

Audits of the Microsoft 365 ecosystem involve systematic review of various aspects such as user permissions, data access controls, and security settings. While at times complicated, regular audits help ensure that system configurations remain aligned with best practices and organizational security policies; it is a healthy habit to build and maintain. Since Microsoft 365 encompasses a variety of services, these audits must be comprehensive and cover each service to prevent overlooked vulnerabilities.[10]

Often referred to as "ethical hacking," penetration testing complements regular audits by enabling organizations to evaluate the effectiveness of their security measures. This involves simulating cyberattacks on the Microsoft 365 infrastructure to identify weaknesses that real-world attackers could exploit. For applicable organizations, penetration tests should probe all layers of their Microsoft 365 ecosystem — from the phishing resistance of employees to the resilience of technical tools such as firewalls, threat detection systems, and incident response plans. Insights gathered from these tests guide organizations in fine-tuning their training programs and security strategies, allowing them to develop more comprehensive and effective defenses when a cyberthreat inevitably arises.

[9] Microsoft 365 Guidance for Security & Compliance

[10] Microsoft 365 Native Security: Unlocking Compliance and Monitoring Features

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

7. Software Restriction Policies

A software restriction policy (SRP) is a security feature that organizations can use to identify and control the execution of software on specified hardware. For enterprise organizations using Microsoft 365, implementing such can act as a critical defense mechanism for protecting the many devices for which they are responsible. As Microsoft 365 contains an array of distinct tools, it also invites an array of distinct, exploitable threat vectors. By dictating which software can and cannot run on a system, SRPs effectively reduce the attack surface available to malicious actors.

In constructing an SRP for a Microsoft 365 environment, the aim is to ensure that only trusted applications, scripts, and processes are allowed to execute, including whitelisting and blacklisting threat vectors as needed. For maximum effectiveness, SRPs should be configured with least-privilege access in mind, and regularly updated to reflect changes in the software used by an organization. This includes updates to Microsoft 365 tools, the addition of new software, or the discontinuation of legacy applications.

By hindering malware from leveraging common exploitation techniques, SRPs are highly effective in disrupting the chain of infection and maintaining a quarantine zone. Integrating SRPs into a cybersecurity strategy is a forward-leaning approach that helps shield an organization's infrastructure from the execution of untrusted software — something that, as enterprises grow and hire new employees, is an ever-growing possibility.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

8. Monitoring and Logging

Monitoring and logging constitute a vital step in ensuring the security and integrity of any Microsoft 365 environment. By keeping a vigilant eye on system activities and maintaining comprehensive records of events, organizations can detect potential security incidents in real time, diagnose system issues, understand the scope of breaches, and improve overall security posture.

For Microsoft 365 administrators, importing logs into a capable Security Information and Event Management (SIEM) system can greatly simplify this process. Azure Sentinel, for example, is a Microsoft-native SIEM that uses an array of pre-built data connectors to stream an organization's log data directly into the SIEM application. This data is then normalized to achieve consistent datasets and monitored through built-in analytics tools.

Effective monitoring should cast a wide net to detect range of possible of anomalies indicative of a security threat — from failed log-in attempts (suggesting a brute-force attack) to unusual download patterns (suggesting unwanted data exfiltration) to many others. Comprehensive logging is equally important, serving as the documentation of all monitored activities. Such logs should capture enough detail to allow the reconstruction of events across an entire incident — before, during, and after. This becomes invaluable in post-incident forensic analysis, but also assists in compliance audits and the refinement of security measures over time. Logging must be carefully configured to ensure that the gathered data is actionable, providing clear and relevant information without the noise that can be generated from over-ambitious scope.

Over time, the insights gleaned from monitoring and logging provide organizations with the data necessary for making proactive policy changes and streamlining security updates.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

9. Data Separation

Privilege separation is a widely applicable and effective strategy used by organizations to enhance their security infrastructure and is highly applicable when integrating data-driven services like Microsoft 365. Strategies such as multi-tenant architectures, administrative boundaries, and conditional account restriction focus on structuring data and its privileges to reduce unauthorized access and limit potential damage from security breaches. By keeping different sets of data apart and dividing networks into discrete segments, organizations significantly reduce the initial risk of security breaches and effectively quarantines outbreaks should they occur.

The use of privilege separation policies within Microsoft 365 allows organizations to maintain strict access rules. As we spoke of in our previous section, the best of these rules ensure that users, administrators, and services receive only the permissions necessary to perform necessary tasks and no more — e.g., the principle of least privilege and Role-Based Access Control (RBAC).

For organizations that operate in multiple jurisdictions or have distinct business units, separating Microsoft 365 tenants through a multi-tenant architecture can help isolate data and control access. This refers to the creation of distinct administrative boundaries per tenant. Doing so isolates environments to their own data, user accounts, and access controls, and ensures that security and compliance requirements are met individually and that a breach or security issue within one tenant does not compromise the integrity of others.

Within these administrative boundaries, conditional access policies and account restrictions add another layer of defense and can be directly implemented into Microsoft 365. These policies allow organizations to define and implement context-based rules for any given account, allowing an organization's security rules to be optimized to an account's risk level, geographic location, or dynamic irregularities such as suspicious logins or downloads.

Methodical separation can, as such, be applied to all levels of an organization's hierarchy and provides a robust foundation for securing Microsoft 365 data and other digital assets. As strategic compartmentalization not only mitigates the risk of unauthorized access but also provides layered safeguards and fallbacks against security breaches, data and privilege separation have rightly earned their status as a reliable approach for organizations to fortify their cyber defenses, maintain business continuity, and ultimately take strides toward achieving cyber resiliency within their Microsoft 365 environment.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

10. Encryption

Encryption is a fundamental security measure that serves as a primary line of defense in the protection of sensitive information, ensuring that only authorized parties with the correct decryption key can access the original information, and applies to data regardless of its use, movement, or location. As it pertains to Microsoft 365, encryption provides a layer of security that helps businesses safeguard their communications, documents, and other data — no matter where they reside within their cloud infrastructure.

Phishing emails and infected websites are often the subtle precursors to serious ransomware attacks. In recent years, RobbinHood ransomware has infamously devastated organizations, costing them millions of dollars in ransom, downtime, and recovery efforts — all because of an infected email was unwittingly downloaded and the malware was introduced to the system.

Built-in tools such as Microsoft 365's sensitivity labels help prevent this by adhering to strict protocols that can automatically encrypt documents and emails, thus preventing initial infection by distrusting suspicious emails and warning the user of potentially dangerous senders. These labels can be configured with rights management policies, allowing administrators to determine who can access data and how it can be used; it is a level of content classification and protection governed centrally by the organizations, allowing IT administrators to arbitrate the handing, sharing, and manipulation of data. That way, well-intentioned users have multiple safeguards in place to prevent the introduction or spread of malware (and not hindering workflows in the process).

Effective encryption ultimately forms the bedrock upon which privacy and regulatory compliance are built. Organizations that effectively utilize Microsoft 365's encryption capabilities in parallel to their already-existing security policies are far more cyber resilient than those who do not. Solid encryption practices are pivotal in the safeguard of valuable data against ransomware and cyberthreats, thereby underpinning privacy, ensuring regulatory compliance, and supporting a secure, collaborative workspace.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Microsoft 365 Cyber Resilience Begins with Backup

As we consider the future landscape of data management and security, Backup as-a-Service (BaaS) has emerged as a preferred method for protecting SaaS Apps like Microsoft 365. BaaS is a cloud-based approach that provides organizations with a remote, online system for backing up and storing their data. Integrating BaaS with a Microsoft 365 strategy aligns with the need for robust, scalable, and flexible data protection solutions — all critical components for ensuring organizational resilience.

Backup services allow businesses to outsource their backup needs to specialized providers, who offer end-to-end solutions that can automate backup processes, reduce the amount of necessary on-premises infrastructure, and provide top-tier security measures — all while providing them direct access and control over their data. For Microsoft 365 users, BaaS means enhanced data safety, operational efficiency, and peace of mind.

Securing a Microsoft 365 ecosystem is a multifaceted endeavor that requires organizations to engage in both strategic preventative measures and effective incident response plans. The journey to Microsoft 365 cyber resiliency is ongoing and requires a commitment to the effective use of technological advancements. Fortunately, there are dedicated backup vendors custom-built for Microsoft 365 data.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365* enables radical resilience for Microsoft 365 data, with a modern twist. The industry's leading Microsoft 365 backup solution — Veeam Backup *for Microsoft 365* — is now delivered as a service.

Simplify your backup strategy with software, backup infrastructure, and unlimited storage in an all-in-one cloud service that allows you to leverage powerful data protection and security technology within a simple, seamless user experience.

Veeam Data Cloud *for Microsoft 365* is a backup service providing comprehensive data protection and data recovery for **Microsoft Exchange, SharePoint, OneDrive for Business and Teams**, giving you complete control of your Microsoft 365 environment.

→ Request a demo of
Veeam Data Cloud *for Microsoft 365*

With **Veeam Data Cloud *for Microsoft 365***, you get:

- **Trusted, industry-leading technology:** The most comprehensive data protection solution with over a decade of continuous innovation built to scale.
- **Modern, secure, and intuitive platform:** Easily create backup jobs, complete restores, and gain Microsoft 365 insights from within a modern, web UI.
- **All-inclusive service:** Software, backup infrastructure, and unlimited storage bundled together with ongoing maintenance covered by the experts.

Be Prepared, Stay Informed

Your journey towards Microsoft 365 cyber resilience doesn't end here — it is just getting started. Expand your understanding, refine your strategies, and stay ahead of the curve in 2024. Let us help you transform challenges into opportunities by checking out our expanded collection of resources:

- 8 Benefits of a Backup Service for Microsoft 365
- Microsoft 365 Backup for Dummies
- Microsoft 365 Recovery Best Practices

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

About Veeam Software

Veeam®, the #1 global market leader in data protection and ransomware recovery, is on a mission to help every organization not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 74% of the Global 2000, who trust Veeam to keep their businesses running. Radical Resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.