Microsoft

Protect your organization from ransomware

Layers of Microsoft cloud security features and other products protect your critical assets from ransomware attackers.

Use this poster as a checklist to deploy features and services for layers of protection and mitigation against ransomware attacks.

Ransomware attackers

Layers of protection and mitigation

Prevent attackers from getting in

Remote access

- ❑ Maintain software and appliance updates.
- ❑ Enforce Zero Trust user and device validation with Azure AD Conditional Access.
- ❑ Configure security for third-party VPN solutions.
- ❑ Deploy Azure Point-to-Site (P2S) VPN.
- ❑ Publish on-premises web apps with Azure AD Application Proxy.
- ❑ Secure access to Azure resources with Azure Bastion.

Email and collaboration

- ❑ Enable AMSI for Office VBA.
- ❑ Implement Advanced Email security using Defender for Office 365.
- ❑ Enable attack surface reduction (ASR) rules to block common attack techniques.

Endpoints

- ❑ Block known threats with ASR rules, tamper protection, and block at first site.
- ❑ Apply Security Baselines to harden internet-facing Windows servers and clients and Office applications.
- ❑ Maintain your software so that it is updated and supported.
- ❑ Isolate, disable, or retire insecure systems and protocols.
- ❑ Block unexpected traffic with host-based firewalls and network defenses.

Accounts

- ❑ Enforce strong MFA or passwordless sign-in for all users
- ❑ Increase password security with Azure AD Password Protection

Audit and monitor to find and fix deviations from baseline security and potential attacks

Situation

Keep them out!

Mitigation goal

Services, devices, and user accounts are hardened against typical attack vectors.

Mitigation success

It's too difficult for attackers to compromise a device or get any valid user account credentials.

Prevent an attacker from escalating their privileges

Privileged access strategy

- ❑ Enforce end-to-end session security for administration portals using Azure AD Conditional Access.
- ❑ Protect and monitor identity systems to prevent escalation attacks.
- ❑ Detect and mitigate lateral traversal with compromised devices.
- ❑ Use Azure AD Privileged Identity Management time-based and approval-based role activation.
- ❑ Use Privileged Access Management (PAM) to limit standing access to sensitive data or access to critical configuration settings.

Detection and response

- ❑ Prioritize common entry points:
  - ❑ Use integrated Extended Detection and Response (XDR) tools like Microsoft 365 Defender and Azure Sentinel to provide high quality alerts and minimize friction and manual steps during response.
  - ❑ Monitor for brute-force attempts like password spray.
- ❑ Don't ignore commodity malware.
- ❑ Monitor for an adversary disabling security (this is often part of an attack chain), such as:
  - ❑ Event log clearing, especially the Security Event log and PowerShell Operational logs.
  - ❑ Disabling of security tools and controls (associated with some groups).
- ❑ Integrate outside experts into processes to supplement expertise, such as the Microsoft Detection and Response Team (DART).
- ❑ Rapidly isolate compromised computers using Defender for Endpoint.

Situation

Oh, no! They're in!

Mitigation goal

Limit the blast radius of the attacker by protecting admin and priority accounts and quickly responding to attacks.

Mitigation success

It's too hard for attackers to get any admin or priority account credentials and perform admin tasks without being detected.

Protect your critical data from access and destruction

Secure backups

- ❑ Backup all critical systems automatically on a regular schedule.
- ❑ Protect backups against deliberate erasure and encryption:
  - ❑ Strong Protection: Require out of band steps (MFA or PIN) before modifying online backups (such as Azure Backup).
  - ❑ Strongest Protection: Store backups in online immutable storage (such as Azure Blob) and/or fully offline or off-site.
- ❑ Regularly exercise your business continuity/disaster recovery (BC/DR) plan.
- ❑ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB), and network diagrams.

Data protection

- ❑ Migrate your organization to the cloud:
  - ❑ Move user data to cloud solutions like OneDrive/SharePoint to take advantage. of versioning and recycle bin capabilities.
  - ❑ Educate users on how to recover their files by themselves to reduce delays and cost of recovery.
- ❑ Designate Protected Folders.
- ❑ Review your permissions:
  - ❑ Discover broad write/delete permissions on file shares, SharePoint, and other solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - ❑ Reduce broad permissions while meeting business collaboration requirements.
  - ❑ Audit and monitor to ensure broad permissions don't reappear.

Situation

Oh, no! They've escalated privileges!

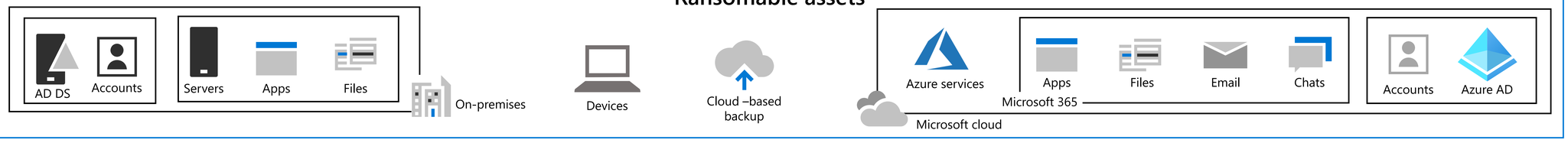
Mitigation

Minimize the financial leverage the attacker has on your organization through tight permissions, encryption, and immutable offline backups.

Mitigation success

It costs less for your organization to recover from an attack than to pay the ransom.

Ransomable assets



Rapidly protect against ransomware and extortion

Get the details on how to plan and implement the three layers of protection and mitigation against ransomware.

For additional guidance, visit aka.ms/ransomware

Microsoft