Microsoft

Secure Multicloud Environments

4 phases of a ransomware attack

What is ransomware?

Ransomware is a type of cyber threat in which attackers exploit a victim's data or critical infrastructure and demand monetary ransom. In recent years, ransomware attacks have become more common and increasingly sophisticated—exploding into a full-blown underground economy. Cybercriminals are economically motivated to continue ransomware attacks, as many victims, desperate to get their data back, simply pay the ransom.

The 4 phases of a ransomware attack

1 Initial compromise

The attacker compromises & establishes initial access to the environment.

Common methods include phishing, pirated software, brute force, exploitation of vulnerabilities, and credential theft.

Mitigations:

- ✓ Maintain software updates and proactively address vulnerabilities.
- ✓ Enforce multi-factor authentication and increase password security.
- ✓ Enforce Zero Trust user and device validation.
- ✓ Train employees to recognize phishing.
- ✓ Utilize threat intelligence to prevent known threats and actors.

2 Escalation

The attacker strengthens their foothold by escalating their privileges and moving laterally across the environment.

Common methods include exploiting known vulnerabilities, deploying malware, and persistence.

Mitigations:

- ✓ Enforce session security for administration portals.
- ✓ Limit account access to sensitive data with privileged access management.
- ✓ Continuously monitor resources for abnormal activity.
- ✓ Adopt best-in-class tools to detect known threats.
- ✓ Implement automation to isolate any compromised resources.

3 Exfiltration

The attacker exfiltrates target data or restricts access to critical systems in preparation for ransom.

Common methods include local deployment of malware to endpoints, defense evasion, and encryption of business critical files.

Mitigations:

- ✓ Ensure regular and thorough data backups.
- ✓ Move data to the cloud and take advantage of the greater versioning capabilities it offers.
- ✓ Review user permissions to sensitive data.
- ✓ Reduce broad read/write permissions for business-critical data.
- ✓ Designate protected folders with controlled folder access.

4 Ransom

The attacker makes contact, demands their ransom, and either acts upon their threats or withdraws.

Common methods include making contact via messaging software to make their demands—typically in cryptocurrency, making payments impossible to track and trace.

Mitigations:

- ✓ Maintain a disaster backup and recovery plan and protect backups.
- ✓ Even if the ransom is paid, there is no guarantee data will be returned or unencrypted. On average, organizations that paid the ransom got back only 65% of their data, with 29% getting no more than half their data.
- ✓ Ensure a holistic clean up and complete removal of persistence—otherwise, the attackers can and often will strike again.