Protect your organization from ransomware

What is ransomware?

Ransomware aims to profit from the panic of business leaders by rendering their systems unworkable, forcing them to pay a ransom for access to their encrypted data.

The underground ransomware economy

Criminals have evolved from low-tech tricksters to sophisticated, well-resourced players. The underground ransomware economy is an essential part of the larger cybercrime ecosystem.

The phases of a ransomware attack

Understanding the phases of a ransomware attack allows organizations to develop appropriate ransomware defenses. The phases are:

Initial compromise

The attacker compromises and establishes initial access to the environment. This is often achieved through vulnerabilities, social engineering, and phishing attacks.

Exfiltration

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

Ransom

The attacker makes contact, demands their ransom, and outlines their terms for delivering the decrypted data. The victim is given a limited time to pay.

How Microsoft disrupts ransomware

Microsoft security researchers have identified two key areas of focus for ransomware mitigation:

1. Strengthening the environment
2. Partnering with the security community

Best practices

Organizations can take several steps to protect against ransomware attacks:

1. Implement robust security measures
2. Educate employees on phishing and social engineering
3. Backup data regularly

Learn more about how to protect your organization from ransomware at Microsoft.com/protect