

# 5

## TECHNICAL STEPS TO PREPARE FOR A RANSOMWARE ATTACK



### 1.

#### BUILD RESILIENCE CONTINUOUSLY – PREVENTION IS ALWAYS BETTER THAN CURE



Enable MFA for all remote access, or access to platforms like Microsoft 365



Limit local administrator rights – grant it only to users who need it



Deploy Microsoft's Local Administrator Password Solution (LAPS) to ensure accounts have unique credentials on every device



Enable Windows Defender Credential Guard (if available)



Create a rolling schedule for pentesting your networks, infrastructure, systems



Run compulsory security awareness training programs

### 2.

#### IMPLEMENT DATA BACKUP PROCESSES



Regularly backup critical data offsite



Test restore processes continually

### 3.

#### DEFINE, MAINTAIN AND TEST THE FOLLOWING STANDARD OPERATING PROCEDURES (SOPS):

Configure a network share as "read-only" for all users

Isolating hosts from the network entirely

Disable user and service accounts and disconnect all sessions

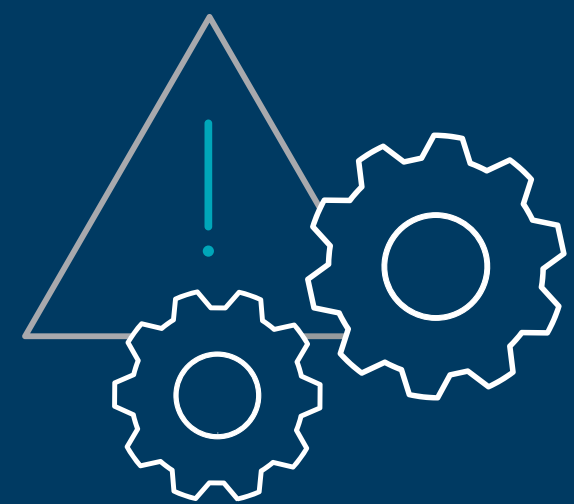
Block the following on endpoints, servers, and network systems:

- Domain
- Hash
- IP or range of IPs
- URL pattern

Execute signed powershell scripts on all hosts at scale

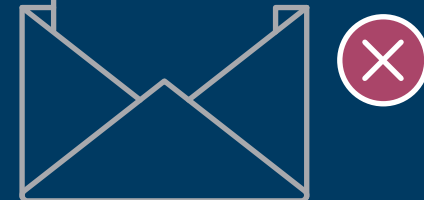
Collect and retrieve forensic artifacts at scale

Redeploy and reconfigure all I.T. systems at scale



Remove emails from mailboxes based on:

- Attachment name
- File extensions
- Sender email
- Sender IP source
- Email subject



### 4.

#### HAVE THE FOLLOWING DOCUMENTS AVAILABLE AS HARD COPIES AND OFFSITE



Critical assets list



Network diagrams



Mobile phone contact lists



### 5.

#### INTEGRATE A RANSOMWARE ATTACK SCENARIO INTO YOUR BUSINESS CONTINUITY PLANNING



Plan for the potential disruption of all critical I.T. systems:

- Emergency communication means planned
- Emergency procedures stored in an alternative location



Plan for response when most critical applications are affected