CHECKLIST | RANSOMWARE PREVENTION BEST PRACTICES

Presented by 1st Security Insurance

Date:

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among private businesses, nonprofits, critical infrastructure organizations, and state, local and government entities.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The monetary value of ransom demands has also increased, with some demands exceeding $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data and publicly naming and shaming victims as secondary forms of extortion. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. Throughout the initial disruption and, at times, extended recovery, the economic and reputational impacts of ransomware incidents have also proven challenging for organizations large and small.

Be Prepared		
1a.	It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important for backups to be maintained offline, as many ransomware variants attempt to find and delete any accessible backups. Keeping current, offline backups is critical because there is no need to pay a ransom for data that is readily accessible to your organization.	☐
1b.	Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	☐
1c.	Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. • **Note**: Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.	☐
1d.	In addition to system images, applicable source code or executables should be available (i.e., stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly. Having separate access to needed software will help in these cases.	☐
2a.	Create, maintain and exercise a basic cyber incident response plan and an associated communications plan that includes response and notification procedures for a ransomware incident.	☐
2b.	Review available incident response guidance.	☐

Ransomware Infection Vector: Internet-facing Vulnerabilities and Misconfigurations		
1.	Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface. • **Note**: The Cybersecurity and Infrastructure Security Agency (CISA) offers a no-cost Vulnerability Scanning service and other no-cost assessments.	☐
2a.	Regularly patch and update software and OSs to the latest available versions.	☐
2b.	Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins and document readers—for known vulnerabilities.	☐
3.	Ensure devices are properly configured and security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol (RDP)—Transmission Control Protocol (TCP) Port 3389).	☐
4a.	Employ best practices for the use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security.	☐
4b.	Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multifactor authentication (MFA) and log RDP login attempts.	☐
5a.	Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the actions in 5b. and 5c. to protect their networks.	☐
5b.	Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled. • **Note**: Remove dependencies through upgrades and reconfiguration. Upgrade to SMBv3 (or most current version), along with SMB signing.	☐
5c.	Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.	☐

Ransomware Infection Vector: Phishing		
1.	Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.	☐
2.	Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.	☐
3.	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols,	☐

	adding a reporting function that allows senders and receivers to improve and monitor the protection of the domain from fraudulent email.	
4.	Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.	☐

Ransomware Infection Vector: Precursor Malware Infection		
1a.	Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables the detection of both "precursor" malware and ransomware.	☐
1b.	A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections result from existing malware infections, such as TrickBot, Dridex or Emotet.	☐
1c.	In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.	☐
2a.	Use application directory allowlisting on all assets to ensure that only authorized software can run and all unauthorized software is blocked from execution.	☐
2b.	Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.	☐
2c.	Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86) and SYSTEM32. Disallow all other locations unless an exception is granted.	☐
3.	Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.	☐

Ransomware Infection Vector: Third Parties and Managed Service Providers		
1a.	Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.	☐
1b.	If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they follow the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.	☐
2a.	Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers.	☐
2b.	Adversaries may target MSPs with the goal of compromising MSP client organizations. They may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.	☐

2c.	Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.	☐

General Best Practices and Hardening Guidance		
1a.	Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.	☐
1b.	If you are using passwords, use strong passwords and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.	☐
2a.	Apply the principle of least privilege to all systems and services so users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.	☐
2b.	Restrict user permissions to install and run software applications.	☐
2c.	Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network") and prevent access via an RDP session.	☐
2d.	Remove unnecessary accounts and groups and restrict root access.	☐
2e.	Control and limit local administration.	☐
2f.	Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.	☐
2g.	Audit user accounts regularly, particularly remote monitoring and management accounts that are publicly accessible. This includes audits of third-party access given to MSPs.	☐
3.	Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365.	☐
4a.	Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see Figure 1). This is useful in a steady state and can help incident responders understand where to focus their efforts.	☐
4b.	The diagram should include depictions of covered major networks, any specific IP addressing schemes and the general network topology (including network connections, interdependencies and access granted to third parties or MSPs).	☐
5a.	Employ logical or physical means of network segmentation to separate various business units or departmental IT resources within your organization and to maintain separation between IT and operational technology. This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See Figures 2 and 3 for depictions of a flat (unsegmented) network and a best practice segmented network.	☐

5b.	Network segmentation can be rendered ineffective if it is breached through user error or nonadherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).	☐
6a.	Ensure your organization has a comprehensive asset management approach.	☐
6b.	Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).	☐
6c.	Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organizationwide coordination.	☐
6d.	Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet.	☐
7a.	Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.	☐
7b.	Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities. • **Note**: PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques and procedures of a threat actor's PowerShell use.	☐
7c.	Ensure PowerShell instances (use most current version) have module, script block and transcription logging enabled (enhanced logging). • **Note**: The two logs that record PowerShell activity are the "PowerShell" Windows Event Log and the "PowerShell Operational" Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs as large as possible.	☐
8a.	Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide. The following list contains high-level suggestions on how best to secure a DC: • Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible. • Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated into newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft, when configuring available security features. • Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.	☐

	• Access to DCs should be restricted to the administrators' group. Users within this group should be limited and have separate accounts used for day-to-day operations with nonadministrative permissions. • DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Updated servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.	
8b.	CISA recommends the following DC Group Policy settings (this is not an all-inclusive list, and further steps should be taken to secure DCs within the environment): • The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible. • Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection. • Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.	☐
8c.	Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred: • Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact on the organization as a whole. • Maintain and back up logs for critical systems for a minimum of one year, if possible.	☐
9.	Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal versus anomalous account activity). Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.	☐

Source: Cybersecurity and Infrastructure Security Agency (CISA)

APPENDIX

FIGURES

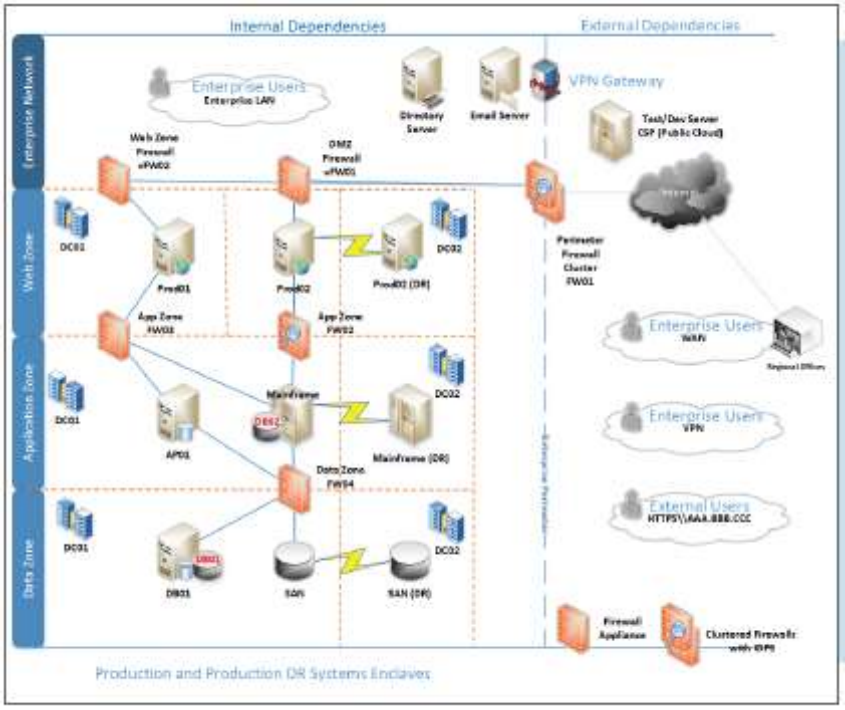

Figure 1. Example Network Diagram

Figure 2. Flat (Unsegmented) Network

Figure 3. Segmented Network