Alliant

Management Professional Solutions

Protecting Your Organization Against Ransomware

MINIMUM PROTECTION

- **Deploy and maintain a well configured and centrally managed End-Point Protection (EPP) solution:** A robust EPP/anti-virus solution is a basic component of any security program.
- **Email tagging:** Tag emails from external senders to alert employees of emails originating from outside the organization.
- **Email content and delivery:** Enforce strict Sender Policy Framework (SPF) checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro enabled documents and links to malicious sites.
- **Office 365 add-ons and configuration:** Enable two-factor authentication (2FA) on Office 365 and use Office 365 Advanced Threat Protection.
- **Macros**: Disable macros from automatically running. Ideally disable them from running at all if your business does not need them.
- **Patching**: Conduct regular vulnerability scans and rapidly patch critical vulnerabilities across endpoints and servers – especially externally facing systems.
- **Remote Access**: Do not expose Remote Desktop Protocol (RDP) directly to the Internet. Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled VPN.
- **Media usage controls:** Put in place controls on the insertion and/or use of media which does not carry appropriate authentication/media identifiers.
- **Well-defined and rehearsed incident response process:** Helps mitigate losses and rapidly restore business operations after a ransomware attack.
- **Back-up key systems and databases:** Ensure regular back-ups which are verified and stored safely offline.
- **Educate your users:** Most attacks rely on users making mistakes, train your users to identify phishing emails with malicious links or attachments. Regular phishing exercises are a great way to do this.
- **Firewalls:** Use network and host-based firewalls with well considered rule-sets, for example, disallow inbound connections by default.

STRONGER PROTECTION

- **Establish a secure baseline configuration:** Malware relies on finding gaps to exploit. A baseline configuration for servers, end-points and network devices that conforms to technical standards such as Center for Internet Security (CIS) benchmarks can help plug those gaps.
- **Filter web browsing traffic:** Web filtering solutions will help prevent users from accessing malicious websites.
- **Use of protective DNS:** Helps deny access to known malicious domains on the Internet.
- **Manage access effectively:** Ransomware doesn't have to go viral in your organization. Put in place appropriate measures for general user and system access across the organization: privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce multi-factor authetication (MFA) where appropriate (remote access VPN, externally facing applications, etc.)
- **Regular testing of back-ups:** Reduces downtime and data loss in the case of restoring from back ups after a ransomware attack.
- **Disconnect back-ups from organization's nework:** Prevents backups from being accessed and encrypted by ransomware in case of a successful attack on an organization's main network.
- **Separately stored, unique back-up credentials:** Prevents bad actors from accessing and encrypting back-up data.

BEST PROTECTION

- **End-point detection and response (EDR) tools:** EDR solutions monitor servers, laptops, desktops and managed mobile devices for signs of malicious or unusual user behavior/activity. These tools also enable near immediate response by trained security experts. When effectively deployed and monitored, EDR tools are one of the best defenses against ransomware and other malware attacks.
- **Intelligent email evaluation:** Automatically detonate and evaluate inbound attachments in a sandbox environment to determine if malicious prior to user delivery.
- **Centralized log monitoring:** Centralized collection and monitoring of logs, ideally using a Security Information and Event Management (SIEM) system, identifies threats which breach your internal defenses.
- **Subscription to external threat intelligence services:** Provides access to external services that can provide details of developing attacker tactics, techniques and procedures. They also provide access to databases of known bad websites, mail attachments, etc.
- **Encrypted back-ups:** Prevents use of back-up data by bad actors.
- **Network segregation:** control access and/or traffic flow within the network environment. A well-configured firewall rule set will ensure that only the required traffic can flow from one segment to another. Furthermore, segregate end of life/support systems/software as a priority.
- **Web isolation:** Use of a web-isolation and containment technology to create a secure Internet browsing experience for your users.
- **Application permissions:** Only permit applications trusted by your organization to run on devices.

Alliant

CYBER GLOSSARY

- **Domain Keys Identified Mail (DKIM):** is an email authentication method that allows senders to associate a domain name with an email message, thus vouching for its authenticity. A sender creates the DKIM by "signing" the email with a digital signature. This "signature" is located in the message's header.
- **Domain-based Message Authentication, Reporting & Conformance (DMARC):** is an email authentication protocol that uses Sender Policy Framework (SPF) and DKIM to determine the authenticity of an email message.
- **Endpoint application isolation and containment technology** is a form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. Application containment is used to block harmful file and memory actions to other apps and the endpoint. Application isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.
- **Endpoint Detection and Response (EDR),** also known as endpoint threat detection and response, centrally collects and analyzes comprehensive endpoint data across your entire organization to provide a full picture of potential threats.
- **Multi-Factor Authentication (MFA):** is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or handprint). MFA for remote email access can be enabled through most email providers.
- **Next-Generation Anti-Virus (NGAV):** is software that uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to detect and prevent malware and fileless non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected.
- **Offline/Air-gapped backup solution:** refers to a backup and recovery solution in which one copy of your organization's data is offline (i.e., disconnected) and cannot be accessed. If a file or system of files has no connection to the internet or a LAN, it can't be remotely hacked or corrupted.
- **Powershell:** is a cross-platform task automation and configuration management framework from Microsoft, consisting of a command-line shell and scripting language. It is used by IT departments to run tasks on multiple computers in an efficient manner. For example, Powershell can be used to install a new application across your organization.
- **Privileged Account Management Software (PAM):** is software that allows you to secure your privileged credentials in a centralized, secure vault (i.e., a password safe). To qualify as PAM, a product must allow administrators to create privileged access accounts; offer a secure vault to store privileged credentials; and monitor and log user actions while using privileged accounts.
- **Protective DNS Service (PDNS):** refers to a service that provides Domain Name Service (DNS) protection (also known as DNS filtering) by blacklisting dangerous sites and filtering out unwanted content. It can also help to detect & prevent malware that uses DNS tunneling to communicate with a command-and-control server.
- **Remote Desktop Protocol (RDP):** connections is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.
- **Security Information and Event Management system (SIEM):** is a subsection within the field of computer security, wherein software products and services combine security information management and security event management. SIEM provides real-time analysis of security alerts generated by applications and network hardware.
- **Security Operations Center (SOC):** is a centralized unit that deals with security issues on an organizational and technical level.
- **Sender Policy Framework (SPF):** is an email authentication technique used to prevent spammers from sending messages on behalf of your domain. With SPF, your organization can publish authorized mail servers.
- **Vulnerability management tool:** is a cloud service that gives you instantaneous, global visibility into where your IT systems might be vulnerable to the latest internet threats and how to protect against them. The tool is an ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation and defense tactics to protect your organization's modern IT attack surface from cyber threats.

Alliant