Beazley's 360° approach to ransomware protection

A ransomware incident is one of the most disruptive and costly attacks your organization can suffer. Ransomware is on the rise and is showing no signs of slowing down. Beazley's claims and breach response services teams are on the front lines and have the knowledge and expertise to help you protect your organization against these attacks. Along with our forensics service providers Lodestone and KPMG, we have developed a ransomware best practices guide to help you prevent these incidents from occurring.

Ransomware scenario

1

Initial compromise of your environment

- A criminal group targets your organization with a phishing campaign.
- Malware is successfully delivered to one of your un-suspecting users via a malicious attachment or web link in an email.

2

Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC.
- Unbeknownst to the user, and your security and IT teams, the attackers now have a foothold in your environment.
- Using this foothold, the hackers explore your network (still undetected) looking for vulnerable systems and sensitive data. This includes other users' PCs but also servers supporting critical applications and file stores.

3

Ransomware is deployed

- The criminal group has achieved the access they need and are ready to spring their trap.
- They deploy a strain of ransomware which spreads across your network encrypting indiscriminately.
- The attackers have now encrypted a material portion of your estate and parts of your business are completely disrupted while other parts are partially disrupted.

4

Extortion

- The attackers demand $x million for the decryption key.
- The attack also becomes public knowledge which causes reputational damage.
- The regulator also wants to understand if there has been a mishandling of customer sensitive data – there is a risk of a significant fine.

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 serves, 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 authentication (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 network:** Prevents back-ups 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.

Lodestone

Leaders in cyber defense, our experts provide clients with the information and processes needed to address cyber threats across the spectrum—from strategic readiness through breach response.

For more information contact info@lodestone.com

KPMG

KPMG offers a wide range of services to help organizations defend against and respond to ransomware attacks.
To discuss how they can help please contact:

Matthew Martindale – Partner, Cyber Security
cyber@kpmg.co.uk

beazley