Beazleys 360º-Konzept zum Schutz vor Ransomware

Ein Ransomware-Angriff ist einer der gefährlichsten und kostspieligsten Angriffe, denen Ihr Unternehmen ausgesetzt sein kann. Ransomware-Angriffe sind auf dem Vormarsch und werden nicht weniger. Beazley hat allein im letzten Quartal einen Anstieg von Ransomware-Vorfällen um 37 % im Vergleich zum vorherigen Quartal beobachtet. Beazleys Schaden- und Breach Response Teams stehen an vorderster Front und haben die Kenntnisse und das Fachwissen, um Ihr Unternehmen vor solchen Angriffen zu schützen. Zusammen mit unseren forensischen Dienstleistern sKPMG haben wir einen Best-Practices-Leitfaden entwickelt, der Ihnen helfen soll, solche Vorfälle zu verhindern.

Ransomware-Szenario

1

Initiale Kompromittierung Ihres Netzwerks

- Eine kriminelle Gruppe hat Ihr Unternehmen mit einer Phishing-Kampagne ins Visier genommen.
- Die Malware gelangt mittels eines bösartigen Anhangs oder Web-Links erfolgreich auf den PC eines Ihrer ahnungslosen Nutzer.

2

Malware wird installiert

- Der Nutzer öffnet einen Anhang und die Malware wird unbemerkt auf dem PC des Nutzers installiert.
- Ohne das Wissen des Nutzers und Ihrer Sicherheits- und IT-Teams haben Hacker nun in Ihrem Umfeld Fuß gefasst.
- Dies nutzen Hacker aus, um Ihr Netzwerk (immer noch unerkannt) nach anfälligen Systemen und sensiblen Daten zu erkunden. Dazu gehören die PCs anderer Nutzer, aber auch Server mit wichtigen Anwendungen und Dateien

3

Ransomware wird eingesetzt

- Die kriminelle Gruppe hat den gewünschten Zugang und ist bereit, die Falle zuschnappen zu lassen.
- Sie setzten Ransomware ein, die sich in ihrem System verbreitet und alles wahllos verschlüsselt.
- Die Angreifer haben nun durch die Verschlüsselung wichtiger Bereiche des Systems Teile Ihres Unternehmens vollständig und andere teilweise lahmgelegt.

4

Erpressung

- Die Angreifer verlangen eine bestimmte Summe Geld oder Kryptowährung für den Entschlüsselungscode.
- Der Angriff wird außerdem öffentlich bekannt und sorgt für einen Reputationsschaden.
- Der Regulierer möchte zudem wissen, ob ein falscher Umgang mit sensiblen Kundendaten vorliegt – es besteht das Risiko einer erheblichen Geldbuße.

Schutz Ihres Unternehmens vor Ransomware

Mindestkontrollen, ohne die Sie angreifbar sind

- **Einsatz und Wartung einer gut konfigurierten und zentral verwalteten Anti-Virus-Lösung:** Eine robuste Anti-Virus-Lösung ist die Grundlage eines jeden Sicherheitsprogramms.
- **E-Mail-Tagging:** Kennzeichnen Sie E-Mails externer Absender, um Mitarbeiter auf E-Mails von außerhalb des Unternehmens hinzuweisen.
- **E-Mail-Inhalt und -versand:** Strenge Sender Policy Framework (SPF) Checks bei allen eingehenden Nachrichten, um die Gültigkeit der sendenden Unternehmen zu verifizieren. Filtern aller eingehenden E-Mails nach böswilligen Inhalten, inkl. ausführbarer Dateien und Dokumenten mit aktivierten Makros.
- **Add-ons und Konfiguration für Office 365:** Aktivieren Sie in Office 365 die Zwei-Faktor-Authentifizierung (2FA) und nutzen Sie Office 365 Advanced Threat Protection.
- **Makros:** Deaktivieren Sie das automatische Ausführen von Makros. Deaktivieren Sie idealerweise das Ausführen von Makros komplett, wenn diese für Ihr Unternehmen nicht notwendig sind.
- **Patchen:** Patchen Sie umgehend kritische Schwachstellen auf Endgeräten und Servern – speziell externen Systemen.
- **Kontrolle der Mediennutzung:** Richten Sie Kontrollen für die Einführung und/oder Nutzung von Datenträgern ein, die keine angemessene Authentifizierung/Medienkennung haben.
- **Genau festgelegter und gut eingespielter Reaktionsplan auf Vorfälle:** Dies ist hilfreich, um nach einem Ransomware-Angriff die Verluste zu minimieren und den Geschäftsbetrieb rasch wieder herzustellen.
- **Sichern von wichtigen Systemen und Datenbanken:** Machen Sie regelmäßige Datensicherungen, die überprüft und sicher offline gespeichert werden.
- **Schulung Ihrer Mitarbeiter:** Die meisten Angriffe sind auf Fehler von Nutzern angewiesen. Schulen Sie Ihre Nutzer, Phishing-E-Mails mit schadhaften Links oder Anhängen zu identifizieren. Regelmäßige Phishing-Übungen sind ein guter Ansatz.

Grundlegende Maßnahmen für besseren Schutz

- **Erstellen einer sicheren Basiskonfigurierung:** Malware verlässt sich darauf, Lücken ausnutzen zu können. Eine Basiskonfigurierung, die technischen Standards wie den Benchmarks des Centers for Internet Security (CIS) entspricht, kann beim Schließen solcher Lücken hilfreich sein.
- **Filtern von Web-Browsing-Daten:** Web-Filterprogramme können Nutzer daran hindern, schädliche Webseiten aufzurufen.
- **Verwenden von geschützten DNS:** Hilft beim Blockieren von bekannten schadhaften IP-Adressen im Internet.
- **Zugang effektiv managen:** Ransomware muss sich in Ihrem Unternehmen nicht verbreiten. Ergreifen Sie im gesamten Unternehmen geeignete Maßnahmen für den allgemeinen Benutzer- und Systemzugang und sorgen Sie für einen privilegierten Zugriff auf wichtige Bereiche (Server, Endgeräte, Anwendungen, Datenbanken, etc.). Verwenden Sie gegebenenfalls Multi-Faktor-Authentisierung (MFA) – beispielsweise Remote Access/VPN, externe Anwendungen, etc.
- **Regelmäßige Überprüfung der Datensicherung:** Dies reduziert im Falle einer Wiederherstellung nach einem erfolgreichen Ransomware-Angriff die Ausfallzeiten und den Datenverlust.
- **Trennung der Sicherungskopien vom Firmennetzwerk:** Verhindert im Falle eines erfolgreichen Angriffs auf das Hauptnetzwerk eines Unternehmens, dass Sicherungskopien durch Ransomware zugänglich sind und entschlüsselt werden.
- **Vorteile getrennt gespeicherter Sicherungskopien:** Hindert böswillige Personen am Zugang und Entschlüsseln von Sicherungskopien.

Verfahren, die den besten Schutz bieten

- **Endpoint Detection and Response (EDR) Tools:** EDR-Lösungen durchsuchen Server, Laptops, Desktops und mobile Geräte nach bösartigen oder ungewöhnlichen Aktivitäten. Diese Tools ermöglichen eine fast umgehende Reaktion von geschulten Sicherheitsexperten. Werden EDR-Tools effektiv eingesetzt und überwacht, sind sie die beste Abwehr gegen Ransomware und andere Malware-Angriffe.
- **Umfassende zentrale Log-Überprüfung:** Zentrale Sammlung und Überwachung von Log-Protokollen, idealerweise unter Verwendung eines Security Information and Event Management (SIEM) Systems, das Bedrohungen Ihrer internen Abwehrmechanismen entdeckt.
- **Inanspruchnahme von Informationsdiensten für externe Bedrohungen:** Diese externen Services bieten Informationen über neue Angriffstaktiken, Techniken und Vorgehensweisen sowie Zugriff auf Datenbanken mit bekannten gefährliche Webseiten, E-Mail-Anhängen, etc.
- **Verschlüsselung von Datensicherungen:** Verhindert im Falle eines Vorfalls die Verwendung von gesicherten Daten durch Kriminelle.
- **Netzwerkisolierung:** Implementieren Sie Zugangskontrollen innerhalb der Netzwerkumgebung, um den Zugang/Datenverkehr zu begrenzen. Gut konfigurierte Firewallregeln stellen sicher, dass nur der gewünschte Datenverkehr von einem Segment zum anderen fließen kann.

KPMG

KPMG bietet eine breite Palette an Dienstleistungen, um Unternehmen vor Ransom-Angriffen zu schützen oder auf diese zu reagieren. Weitere Informationen erhalten Sie von:

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

beazley