SIMPLYIT LANWORKS

WIR MACHEN EXPERTENWISSEN WIRKSAM

www.lanworks.de

Wenn der Cyberangriff über Bande gespielt wird …

Was Unternehmen aus dem KASEYA Hackerangriff lernen sollten, um sich effektiv schützen zu können

Der schwere Angriff auf den US-Softwarehersteller Kaseya in den USA, dessen Auswirkungen bis nach Europa spürbar sind, zeigt einmal mehr, wie verwundbar Firmen sind und zwingt IT-Verantwortliche in Unternehmen auch zum Umbau ihrer Schutzkonzepte. Das Modell „sichere Burg“ hat ausgedient. Aber wie können Unternehmen die Resilienz Ihrer IT-Systeme fördern? Wie kann man Mitarbeiter auf einen Cyberangriff vorbereiten? Was sind die größten Schwachstellen in der Cybersicherheit und welche Notfallpläne sollten im Falle eines Cyberangriffs auf jeden Fall vorhanden sein? Im Blogbeitrag beantworten wir diese Fragen und zeigen auf, welche IT-Sicherheitsmaßnahmen im Unternehmen etabliert werden sollten, um für die Zukunft solche einzugrenzen und die Sicherheit zu erhöhen.

Der Zeitpunkt der Cyberattacke auf den US-Softwarehersteller Kaseya war genauso minutiös geplant, wie der Angriff selbst. Denn während sich die Amerikaner auf ihr langes Wochenende anlässlich des amerikanischen Unabhängigkeitstag am 4. Juli vorbereiteten und die Besetzung in den IT-Abteilungen verständlicherweise eher dünn war, nutzten die Angreifer, mutmaßlich aus Russland, eine Zero-Day-Schwachstelle in der VSA-Server-Software des US-Anbieters Kaseya aus.

Für die Attacke wurden vermutlich mit einem Schadprogramm verseuchte E-Mails genutzt, um die Ransomware REvil an 40 bis 60 Managed Service Provider (MSPs) und in der Folge an die Kunden dieser MSPs zu verteilen - insgesamt über 1.000.

Perfide Art des Hackings – ebenso wirksam wie hinterhältig

Was den Angriff so perfide wie wirksam zugleich macht, ist dass die Hacker die betroffenen Unternehmen nicht direkt angriffen. Die Hacker spielten über Bande und nutzen dabei die hohe Vertrauensstellung, die der Kaseya-Software VSA eingeräumt wurde - und zwar völlig unabhängig davon, ob sie nun bei Unternehmen direkt oder bei einem Managed Service Provider (MSP) zum Einsatz kam. Der Verschlüsselungstrojaner schlich sich dabei in automatisch ausgelieferte Updates des Softwareherstellers ein und erzeugte so eine Art Kettenreaktion bei den IT-Dienstleistern und deren Kunden, wodurch der Schaden um ein Vielfaches vergrößert wurde.

Wer nicht rechtzeitig von dem Angriff erfuhr und wessen Rechner noch lief, wurde durch das Update automatisch zum Erpressungsopfer. Daten wurden verschlüsselt und ganze Systeme lahmgelegt, wie im Falle der schwedischen Supermarktkette Coop. Die Firmen haben nun nicht nur mit einem verheerenden wirtschaftlichen, sondern auch einem Imageschaden zu kämpfen.

Was macht solche „Supply-Chain“ Angriffe so gefährlich

Diese Art der Verbreitung von Schadcode wird als "Supply Chain"-Angriff bezeichnet, bei dem der vertrauenswürdige Zugriff eines IT-Tools genutzt wird, um Zugang zu den Netzwerken möglichst vieler weiterer Unternehmen zu erhalten. Es ist ein Angriff auf die Vertraulichkeit, Integrität und Verfügbarkeit – den wesentlichen Säulen der Cybersicherheit. Und wenn wir denen, mit denen wir zusammenarbeiten (unserer Lieferkette), nicht vertrauen können, verlieren wir die Grundlage unseres Wirtschaftssystems. Eine Lektion, die man daraus lernt ist, dass niemand vor Cyberangriffen sicher ist. Man muss immer davon ausgehen, dass etwas passieren kann. Kaseya ist - ebenso wie SolarWinds, das Anfang des Jahres bei einem anderen Angriff auf die Lieferkette ausgenutzt wurde - eine seit langem bestehende und angesehene IT-Management-Lösung. Die erfolgreichen Angriffe auf diese Dienste beweisen, dass jeder Partner mit Zugriff auf Ihre IT-Umgebung schnell zu einer Schwachstelle werden kann.

Wie also schützt man sich wirksam vor Ransomware und Cyberangriffen - Zero Trust ist die Antwort

Es ist von entscheidender Bedeutung, dass Sie die **Zero-Trust-Strategien anwenden**, um das Geschäftsrisiko durch diese Angriffe zu mindern. Es sollte weder einen vertrauenswürdigen Partner noch einen vertrauenswürdigen Mitarbeiter oder ein vertrauenswürdiges Gerät geben.

Der Zugriff auf Ressourcen sollte auf einer dynamisch kontrollierten **Least-Privilege-Basis** erfolgen. (mehr hierzu finden Sie auch in unserem Blogartikel „Catch me if you can“)

Selbst mit vertrauenswürdigen Tools und Partnern müssen Unternehmen davon ausgehen, dass jede Verbindung ein potenzieller Angriff sein könnte. Es gilt Kontrollen um **Identitäts- und Zero-Trust-Richtlinien** so aufzubauen, dass die Benutzer sich sicher direkt mit Anwendungen und niemals mit Netzwerken verbinden. Mit **Zero-Trust** können Sie die Angriffsfläche grundlegend eliminieren, indem Sie Unternehmensressourcen für Angreifer unsichtbar und unangreifbar machen - im Gegensatz zu herkömmlichen Netzwerksicherheitsansätzen, die Bedrohungen aus vertrauenswürdigen Quellen Tür und Tor offenlassen.

Um in Zukunft besser gegen Cyberangriffe geschützt zu sein, sollte IT-Sicherheitsverantwortliche in Unternehmen folgende Regeln anwenden:

- Setzen Sie eine starke Integritätskontrollstrategie ein.
- Verlangen Sie eine starke Authentifizierung (MFA) für Administrations- oder Entwicklungsaktionen
- Überprüfen Sie regelmäßig die verschiedenen Komponenten Ihres Informationssystems oder lassen Sie diese überprüfen. Hier hilft ein **leistungsstarkes Identity- und Accessmanagement mit integrierten Identity Governance** Funktionalitäten. (Lesen Sie hierzu auch unseren Blogartikel „sichere Identitäten“)
- Reduzieren Sie so weit wie möglich die Berechtigungen und den Umfang von Code, der von Dritten stammt – **Stichwort „Least Privilege Prinzip“**
- Erhöhen Sie die Cyber – Resilienz, indem Sie ein Business Continuity Planning (BCP) oder ein Emergency Response Planning (ERP) implementieren, um im Falle eines Vorfalls schnell und effizient reagieren zu können. (mehr hierzu finden Sie auch in unserem Blogartikel „Cyber-Resilienz - Bullshit Bingo?")

Die Lanworks AG mit ihrer über 20-jährigen IT- Consulting Engineering Expertise in den Bereichen Endpoint Management, Identity- und Access Management sowie Backup und Systemrecovery unterstützt Sie gerne bei der Erstellung und Umsetzung solcher ganzheitlichen Sicherheitskonzepten – genau abgestimmt auf Ihre speziellen Bedürfnisse.

Faktor Mensch – Mitarbeitende als Schutzwall gegen Cybercrime

Mit dem Einsatz der technologischen Schutzmaßnahmen lassen sich wertvolle Netzwerke und kritische Daten auf jeden Fall besser schützen, jedoch sollte der Faktor Mensch nicht unterschätzt werden. Letztendlich müssen Unternehmen dafür sorgen, dass sich die Mitarbeitenden nicht nur der aktuellen Gefahrenlage bewusst sind, sondern auch in die Lage versetzt werden, Angriffsmuster frühzeitig zu erkennen und entsprechend zu handeln. Hierzu bedarf es eines umfassenden Schulungsangebotes. Vielen Firmen, insbesondere kleinen und mittelständischen Unternehmen, fehlt es nicht nur an qualifiziertem Personal, sondern auch an notwendigem Know-How, um ein solches Schulungskonzept zu realisieren. Hier sind sie auf die Zusammenarbeit mit Dienstleistern angewiesen. Die Lanworks AG kann auf Basis ihrer langjährigen Erfahrung im Kampf gegen Cyberkriminelle ein umfassendes Trainingsangebot für Angestellte realisieren.