»Wir müssen die IT gegen Cyberangriffe sichern«

Ransomware-Angriffe auf sensible Infrastruktur nehmen zu. Kriminelle blockieren den Zugang zu Daten und fordern Lösegeld für die Freigabe. Dagegen hilft nur maximaler Schutz und Monitoring.

Andreas Mayer
Director Marketing
SEP

Einmal eine scheinbar harmlose Mail geöffnet und schon kann der Schaden fürs Unternehmen immens sein. Cyberkriminelle legen immer häufiger Firmenserver lahm, drohen Daten zu zerstören, die sie erst gegen Lösegeld freigeben. Ob nun Krankenhäuser, Behörden oder Kommunen: Ransomware-Angriffe sind ein elementares Problem für die IT-Sicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die IT-Sicherheitslage in Deutschland als »angespannt bis kritisch« ein. Im Schnitt wurden im Berichtszeitraum von Juni 2020 bis Ende Mai 2021 täglich 394000 neue Schadsoftware-Varianten bekannt. Die Schäden durch Erpressung und den Ausfall von Systemen seien seit 2019 um 358 Prozent gestiegen. »Angriffe treffen immer häufiger nicht nur die ursprünglich angegriffenen Unternehmen, sondern ganze Lieferketten«, warnte BSI-Präsident Arne Schönbohm. Doch was tun? Andreas Mayer, Director Marketing der IT-Datensicherungsexperten von SEP weiß, wie sich kritische Infrastruktur schützen lässt.

„Zunehmend gelingt es Cyberkriminellen, auch die Backups zu korrumpieren.

Herr Andreas Mayer, Ransomware breitet sich weiter aus. Was sind die bevorzugten Angriffsziele der Cyberkriminellen?
Also die Bandbreite deckt eigentlich alles ab, von Angriffen auf Unternehmen bis hin zu privaten Anwendern. Datenklau ist ein globales Thema, da ist keiner sicher. Deutschland gehört auch zu den führenden Ländern, was das Thema Angriffe angeht. Backups sind bei Angriffen durch Ransomware oft der letzte Anker Rettungsanker, um seine Daten wiederherzustellen. Aber zunehmend gelingt es Cyberkriminellen, auch die Backups zu korrumpieren. Das kann ein Unternehmen durch den Verlust wichtiger Daten in den Ruin führen.

Wie viel Prozent der Angriffe mit Ransomware lassen sich aufklären?
Laut BKA nur 29 Prozent aller Cybercrime-Fälle im vergangenen Jahr. Zusätzlich gibt es noch eine hohe Dunkelziffer: bis zu 91 Prozent der Vorfälle sollen gar nicht gemeldet werden. Was noch dazukommt, dass Kriminelle immer wieder die Vorgehensweise und Angriffsvarianten verändern.

Ex-FBI Director Robert Mueller sagte: »Es gibt nur zwei Arten von Unternehmen: Jene, die gehackt wurden und jene, die es werden.« Bedeutet die Aussage, dass man immer nur reagieren kann – statt vorzubeugen?
Natürlich kann man was tun, indem man entsprechende Prozesse und Abläufe definiert und Security-Lösungen einsetzt, diese ständig updated und Monitoring betreibt. Zudem muss ich eine entsprechende Backup-Lösung im Einsatz haben wie SEP, die meine gesamte IT-Umgebung abdeckt von on-premise über Cloud bis hin zu Cloud Applikationen.

Wie sollten sich Unternehmen aufstellen, um größten Schutz der Daten zu ermöglichen?
Die eingesetzte Software ist immer nur ein Teil der Geschichte. Ich muss auch schauen, dass ich gewisse Strukturen und Organisationsabläufe einbaue. Backups, sollten mehrstufig sein (3-2-1 Regel), sich auf mehrere Standorte verteilen – idealerweise, auch offline. Und dann dürfen eingesetzte Software-Lösungen keine eingebauten Hintertüren haben. Die werden von US-Herstellern gefordert, damit das FBI bei Terrorverdacht ermitteln kann. Diese Hintertüren sind aber auch potenzielle Einfallstore für Cyberkriminelle. SEP garantiert No-Backdoors und weitere Security-Sicherheitsmechanismen.

SEP Immutable Storage (SiS) bietet eine Dateispeicherfunktion, die resistent gegen Ransomware-Angriffe ist. Wo liegen die Vorteile?
Mit dem neuen SEP Immutable Storage (SiS) führen wir die Möglichkeit zur unveränderlichen Speicherung von Daten ein. Der Vorteil: Wir bieten einen besonderen und sicherer Ransomware-Schutz für Backup-Daten. Die neue Dateispeicherfunktion basiert auf Si3 NG (Deduplizierung) unter Linux. Selbst mit vollem Administrator-Zugriff auf den SEP Backup Server, können Angreifer die auf SiS gespeicherten Daten nicht löschen, verändern oder verschlüsseln. Diese Lösung schützt die Daten nicht nur vor unbefugtem Zugriff, sondern trägt zur Einhaltung von Compliance bei.

Werden die Angriffe – siehe Russland oder China – auf Konzerne eher zunehmen?
Leichter wird es wahrscheinlich nicht, weil Cyberkriminalität mittlerweile auch ein enorm lukrativer Wirtschaftszweig ist. Ich denke, die Lösung liegt wirklich in der Verquickung von mehreren Maßnahmen. Nur wer in Bewegung bleibt, seine IT regelmäßig anpasst, verfügt über den besten Schutz.

www.sep.de