Sicherheit
IN EINER VERNETZTEN WELT

Kommunikationsnetzwerke sind aus unserem Alltag nicht mehr wegzudenken. Unzählige Systeme sind mit dem Mega-Netzwerk Internet verbunden und können entsprechend auch von überall her angegriffen werden.

Reto Zbinden,
CEO und Rechtsanwalt,
Swiss Infosec AG

Früher konnten interne Netzwerke mittels Firewalls vor dem öffentlichen, nicht vertrauenswürdigen Internet effektiv geschützt werden. Die Methode, mittels Firewalls und weiterer vielschichtiger Zwiebelschalen die Kronjuwelen eines Unternehmens, also die wichtigen oder vertraulichen Daten, vor Angreifern zu schützen, wird ausgehebelt durch die Mobilität der Benutzer und Systeme einerseits und die Nutzung von Cloud-Diensten andererseits, gerade auch in Zeiten des Homeoffice. Die Geräte der Mitarbeitenden stehen nun im Kreuzfeuer der Angreifer. Einmal drin, kann über das Gerät das gesamte interne Netz von innen her angegriffen werden.

SCHUTZ DER SYSTEME UND DATEN

Es gelingt Angreifern immer wieder, Benutzer zu verführen, bösartige Dateien zu öffnen oder ihr Passwort gefälschten Internetseiten zu verraten. So stehen dem Angreifer Tür und Tor offen für weitere Angriffe. Diese gipfeln darin, die aufgespürten Datensicherungen und auch alle übrigen Daten zu verschlüsseln und das Opfer aufzufordern, Lösegeld für die Entschlüsselung seiner Daten zu bezahlen.

Will sich ein Unternehmen vor solchen Angriffen schützen, so muss es auf technischer Ebene den internen Anwendern und Services misstrauen. Dies wird als Zero-Trust-Modell bezeichnet. Die Identitäten aller Anwender und Systemelemente werden überprüft, die Netzwerke werden in Zonen unterteilt und der gesamte Datenverkehr verschlüsselt und laufend ausgewertet.

Zum Schutz vor existenzgefährdenden Angriffen solcher Art sind mindestens die folgenden Massnahmen dringend empfohlen:

- Ausbildung und Sensibilisierung aller Benutzer
- Einsatz von Anti-Malware-Software und laufende Aktualisierung aller Systemelemente
- Schutz und eingeschränkte Nutzung privilegierter Benutzerkonten («Administrator-Konto»)
- Abkopplung wichtiger Netzbereiche, beispielsweise der Produktionsumgebung
- Die aktuellen Datensicherungen dürfen nicht gelöscht oder verändert werden können, auch nicht durch privilegierte Benutzer

Ein Netz, das sicher ist, Werte schützt, Vertrauen stützt

UNÜBERSCHAUBARE DATENFLÜSSE

Die Vernetzung der Systeme führt zu teils unüberschaubaren Datenflüssen, auch über nationale Grenzen hinweg. Da es sich dabei auch um Personendaten handelt, muss die Persönlichkeit der betroffenen Personen geschützt werden. Sind die Personendaten einmal ausser Landes, so kann der national garantierte Datenschutz praktisch nicht mehr durchgesetzt werden. Dagegen wehrt sich der Datenschutz mit Exportrestriktionen.

DATENSCHUTZ UND DATENSICHERHEIT

Das am 25. September 2020 in den eidgenössischen Räten verabschiedete neue Datenschutzgesetz der Schweiz sieht weiterhin vor, dass Personendaten ins Ausland bekanntgegeben werden dürfen, sofern das Zielland aus Sicht des Bundesrates einen angemessenen Schutz gewährleistet. Ist dieser nicht gewährleistet, so muss der Datenexporteur den Schutz beispielsweise mit vertraglichen Datenschutzklauseln durchsetzen. Daneben sieht das neue Gesetz unter anderem auch vor, dass die Unternehmen mittels geeigneter technischer und organisatorischer Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten müssen.

Für vorsätzliche Verstösse gegen die Exportrestriktionen oder gegen die Anforderungen der Datensicherheit sieht das Gesetz auf Antrag neu Bussen bis zu 250’000 Franken für die beteiligten Personen vor. So wird auch das neue Datenschutzgesetz der Schweiz seinen Beitrag zur Verbesserung der Datensicherheit leisten. ◇