Der Mensch im Mittelpunkt der IT-Sicherheit

Die zunehmende digitale Vernetzung stellt die IT-Sicherheit kontinuierlich vor neue Aufgaben. Für Anpassungsbedarf sorgt auch die Novellierung des IT-Sicherheitsgesetzes.

Von François Baumgartner

Angreifer nutzen gezielt Schwachstellen von Programmen aus, die Cybersysteme und physische Infrastrukturen vernetzen. Foto: fgnopporn - adobe.stock.com

OSTBAYERN. Ab dem 30. Juni wird es für Finanz- und Versicherungsinstitute sowie für die Gesundheits-, Transport- und Verkehrsbranche in Deutschland ernst. Denn dann läuft die zweijährige Frist zur Umsetzung der jüngsten Änderungsverordnung des IT-Sicherheitsgesetzes ab. Die betroffenen Branchen müssen zu diesem Zeitpunkt nachweisen können, dass ihre IT-Infrastruktur alle Änderungsvorschriften vollständig erfüllt.

Eva-Maria Scheiter, Spezialistin für Governance, Risk Management und Compliance bei NTT Security, rät betroffenen Organisationen deshalb, Prozesse und etablierte Vorgaben zu prüfen und sich im Zweifel kompetente Beratung ins Haus zu holen. Die Expertin empfiehlt zudem, Prozesse zur obligatorischen Meldung von IT-Sicherheitsvorfällen festzulegen und gleichsam wie bei einer Feuerübung mit den Mitarbeitern zu trainieren.

Datenschutzexperten gefragt

Dass der Faktor Mensch im Mittelpunkt des neuen IT-Gesetzes steht, bestätigt auch Michael Grotherr, Vice President for Sales Central Europe bei Cornerstone On Demand: „Jedes größere Unternehmen sollte einen Datenschutzbeauftragten im Einsatz haben, also einen Experten, der sich auch mit den Details auskennt. In manchen Bereichen ist er inzwischen ohnehin Pflicht. Bei kleinen Unternehmen hingegen gewinnen externe Auditoren an Bedeutung.“ Die internen und externen Experten für Regeltreue sind bestens mit Gesetzen, Richtlinien und Standards vertraut und kooperieren eng mit der jeweiligen IT-Abteilung eines Unternehmens. Das ist vor allem im Zuge der digitalen Transformation von Unternehmen sehr wichtig.

„Ein Data Scientist braucht den Zugang zu auswertbaren Daten. Dies lässt sich mit Zugangsregeln und der vorhandenen Infrastruktur gut lösen. Sobald aber persönliche Daten im Spiel sind, gilt die Datenschutzgrundverordnung. In diesem Fall muss gewährleistet sein, dass personenbezogene Daten nur anonymisiert zur Verfügung gestellt werden“, weiß Jan Vollmer, CEO von Old World Computing in Bochum. Old World Computing ist ein Spezialist für technische Datenschutzlösungen sowie für Lösungen zur Datenanalyse.

Neben der Gefahr des internen Missbrauchs von Daten drohen zudem Gefahren von außen, aus dem Cyberspace. Josef Meier, Director Sales Engineering von Fortinet, bringt die aktuelle Herausforderung auf den Punkt: „Cybersysteme und physische Räume verschmelzen mehr und mehr. Angreifer suchen nach Möglichkeiten, Schwachstellen von Programmen auszunutzen, die auf die digitale Vernetzung von Cybersystemen und physischen Infrastrukturen abzielen.“ Grundlegende Elemente der Cybersecurity wie Transparenz, Automatisierung und agile Segmentierung, also die Unterteilung des Unternehmensnetzes in einzelne Bereiche, die nicht oder nur bedingt miteinander vernetzt sind, sind nach Ansicht des Experten wichtiger denn je. Diese Elemente werden im neuen IT-Sicherheitsgesetz gestärkt.

Mikrovirtualisierung als Lösung

Wie wichtig gerade die Segmentierung ist, zeigt eine kürzlich erfolgte Cyberattacke auf die US-amerikanische Stadt Baltimore: Kriminelle haben rund 10 000 Rechner in Ämtern und städtischen Einrichtungen mit der Erpressungssoftware „Robin Hood“ infiziert. Die Kryptografie-Anwendung verschlüsselt Daten, blockiert den Zugriff auf Computer und fordert für die Entschlüsselung ein Lösegeld. Der Bürgermeister habe richtig gehandelt, indem er nicht auf die Forderungen eingegangen sei, sagt Jochen Koehler vom Sicherheitsanbieter Bromium. „Es gibt keine Garantie dafür, dass nach Zahlung die betroffenen Daten oder Geräte tatsächlich wieder freigegeben werden“, erklärt Koehler. Wer Zahlungsbereitschaft signalisiere, werde oft mit noch höheren Geldforderungen erpresst. Um sich wirksam gegen Cyberangriffe zu wehren, ist das rechtzeitige Installieren von Patches und Updates wichtig. Darüber hinaus rät Koehler zur Isolation von Applikationen mithilfe der sogenannten Mikrovirtualisierung. Diese Methode abstrahiert Anwendungen und Unterprozesse von der Hardware und führt sie in isolierten Umgebungen aus. So kann beispielsweise eine Browserabfrage oder das Öffnen eines E-Mail-Anhangs unabhängig vom verbundenen Netzwerk stattfinden.