Foto: Telent

Kritische Infrastrukturen müssen besonders vor Cyberangriffen geschützt werden – gerade im Zeitalter der Digitalisierung und zunehmenden Vernetzung von Devices.

Feine Unterschiede in Sachen Cybersicherheit

Die Digitalisierung erfordert wirksame Technologien für die Cybersicherheit. Welche Rolle spielen dabei IT-, OT- und IIoT?

NICO WERNER

Kaum ein Tag vergeht, an dem nicht ein größerer Cybervorfall in Deutschland in einem strategischen Wirtschaftsbereich – von der Industrie über die Energiewirtschaft bis hin zum Finanzdienstleistungssektor – den zuständigen Behörden gemeldet wird. Ein Beispiel für die massive Bedrohung ist der Distributed-Denial-of-Service (DDoS)-Angriff auf das Onlinebanking von 820 Finanzinstituten im Juni 2021.

Bankräuber knacken heutzutage keine Tresore mehr. Schlupflöcher eröffnet ihnen das Digital Banking rund um den Globus und in Echtzeit. Die Sicherheitslage im Finanzsektor entwickelt sich ähnlich wie bei Produktionsunternehmen, die sich zur Industrie 4.0 transformieren. Ursprünglich war in den Fertigungsbetrieben die Welt der Informationstechnologie (IT) und der Operational Technology (OT) physisch streng voneinander getrennt.

220

MILLIARDEN Euro Schaden sind der deutschen Wirtschaft im Jahr 2021 laut einer Studie des Branchenverbandes Bitkom durch Cyberangriffe entstanden.

Gelangten Cyberkrimininelle ins IT-Netz, blieb ihnen der Zugang zur Produktionsumgebung verschlossen. Doch in smarten Fabriken, in denen Geräte und Anlagen über das Internet of Things (IIoT) mit industriellen Softwareanwendungen vernetzt sind, wird die Grenze zwischen den Netzwerken immer durchlässiger. Dringen Angreifer in die OT ein, haben sie oft ein leichtes Spiel, weil die Betriebsversionen von industriellen Steuerungen und Systemen häufig veraltet sind und im Gegensatz zum Büroequipment keine regelmäßigen Updates erhalten. Im Vergleich zur klassischen Unternehmens-IT können Sicherheitsvorfälle bei industriellen Systemen zu wesentlich größeren Schäden führen.

Immer mehr Schäden durch Cyberangriffe

Die Dimensionen sind besorgniserregend: Mehr als 220 Milliarden Euro Schaden sind der deutschen Wirtschaft im Jahr 2021 laut einer Studie des Branchenverbandes Bitkom entstanden. Die Summe ist damit etwa doppelt so hoch wie im Jahr 2019. Cyberangriffe verursachten bei 86 Prozent der befragten rund 1.000 Unternehmen Schäden; zwei Jahre zuvor waren es erst 70 Prozent. Eine Bank hat im klassischen Sinne natürlich kein OT-Netz wie ein Produktionsbetrieb, stattdessen ein Anwendungsnetz. Darüber laufen sämtliche Finanztransaktionen und es beinhaltet Hardware wie Geldausgabeautomaten oder Kontoauszugsdrucker. Die digitale Transformation verwebt auch hier die ehemals voneinander getrennten Office- und Payment-Netze und schafft neue Angriffsflächen.

Im Extremfall eines großangelegten, mehrtägigen Hackerangriffs könnte sogar der globale Finanzmarkt kollabieren – so das Ergebnis einer multinationalen Simulation, an der Ende vergangenen Jahres insgesamt zehn Ländern sowie der Internationale Währungsfonds (IWF), die Weltbank und die Bank für Internationalen Zahlungsausgleich (BIZ) beteiligt waren. Zu den häufigsten Sicherheitsbedrohungen in der Bankenwelt gehört das Phishing. Mit dem „Oldtimer“ unter den Cyberangriffen gelingt es nach wie vor, über betrügerische Links von ahnungslosen Internetnutzern persönliche Daten oder Kreditkartennummern „abzufischen“. Eine ausgefeiltere Variante ist das Spear-Phishing. Dabei sammelt ein Cyberkrimineller zunächst zielgerichtet Informationen über sein Opfer, um sich dann als persönlicher Kontakt auszugeben, der etwa die Vollmacht hat, eine Überweisung zu veranlassen. Weitverbreitet sind auch DNS-Angriffe, die zu Ausfallzeiten bei Clouddiensten oder unternehmensinternen Anwendungen führen und DDoS-Angriffe, die Server durch Überlastung lahmlegen. Derartige Ausfälle können, insbesondere bei zeitkritischen Transaktionen, zu hohen finanziellen Verlusten führen, während gestohlene Daten das Image der Finanzinstitute und das Vertrauen der Kunden beeinträchtigen.

Gesetzliche Sicherheitsanforderungen

Als Reaktion auf den digitalen Diebstahl von Kartendaten hat sich die Branche bereits vor Jahren selbst Mindeststandards verordnet, wie Payment Card Industry Data Security Standard (PCI DDS). Alle Banken, Händler und sonstige Firmen, die Kreditkartendaten über Fernzugriff verarbeiten, müssen eine Multifaktor-Authentifizierung einsetzen und spezielle Prozesse etablieren, um frühzeitig Fehler bei Sicherheitskontrollsystem zu erkennen, zu dokumentieren und zu reagieren. Zudem unterliegen die Geldhäuser, auch als Betreiber kritischer Infrastrukturen, einer stetig steigenden Flut an gesetzlichen Vorschriften, wie zuletzt der im August 2021 novellierten Bankenaufsichtliche Anforderungen an die IT (BAIT). Diese enthält neue Kapitel zur operativen Informationssicherheit und zum IT-Notfallmanagement, wonach Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne einzurichten und jährlich auf Basis eines IT-Testkonzepts zu prüfen sind. Nur wer die Sicherheit stetig verbessert, kann den Wettlauf mit professionellen Cyberkriminiellen gewinnen.

Kurze Innovationszyklen bei Bankdienstleistungen sind ein Grund, warum selbst in gut gepflegten IT-Umgebungen die Verwundbarkeit durch Cyberangriffe dramatisch zunimmt. Weitere sind der Spagat zwischen Usability und Sicherheit sowie die gestiegene mobile Arbeit, die das Risiko der Angriffe von Innen erhöht. Um Schwachstellen zu erkennen, unterstützt telent seine Kunden im ersten Schritt mit einer umfassende Analyse der Netzwerke. Check-ups offenbaren detailliert, wie Netze aufgebaut sind und was darin tatsächlich passiert. Etwa, ob in einer Filiale ein privater Router installiert ist oder auf einem Geschäfts-PC Bitcoin-Mining betrieben wird. Mit dem Wissen über den aktuellen Zustand prüfen die Experten, wie gut die Netze Angriffe erkennen und abwehren: angefangen bei Firewalls über Netzsegmentierungen bis hin zu Sicherheitssystemen wie SIEM (Security Incident & Event Management) und ISMS (Informationssicherheitsmanagementsystem).

Dem schließen sich Awareness-Schulungen von Mitarbeitern und Endkunden an. Denn: Cyberangriffe sind eines der größten Risiken für das operative Geschäft. Nur mit aktuellen, hocheffizienten Sicherheitskonzepten gelingt es, diese Gefahren zu minimieren. ■

„Im Extremfall eines großangelegten, mehrtägigen Hackerangriffs könnte der globale Finanzmarkt kollabieren – so das Ergebnis einer multinationalen Simulation Ende letzten Jahres.“

Nico Werner, Head of Cybersecurity bei der telent GmbH

Foto: Telent

telent GmbH:
www.telent.de