IT-Sicherheit 2021

Wie sich Unternehmen jetzt schützen können

Die Pandemie hat für einen kräftigen Digitalisierungsschub gesorgt und dabei gleichzeitig gezeigt, wie schnell Cyber-Kriminelle auf aktuelle Trends aufspringen. Während die Unternehmen im Schnelldurchlauf digitale Prozesse etablierten und ihre Mitarbeiter ins Homeoffice verlegten, passten sich auch die Angreifer an die neuen Gegebenheiten an.

» *Raphael Vallazza, CEO Endian*

Die IT-Risiken werden Industrieunternehmen auch in diesem Jahr und darüber hinaus beschäftigen. Mit diesen Massnahmen stärken Unternehmen ihre digitalen Abwehrkräfte:

1. Netzwerksegmentierung

Ransomware stellt nach wie vor die grösste Bedrohung für Unternehmen dar und die Zahl der Attacken ist während der Pandemie dramatisch nach oben geschnellt. Das Schadprogramm Emotet dominiert dabei die Lage und ist perfekt auf die zunehmend vernetzten Unternehmen angepasst: Es verbleibt eine Weile inaktiv in den Systemen, um bestehende Verbindungen zu finden und passende Schadsoftware nachzuladen. Somit infiziert Emotet schrittweise alle vorhandenen Systeme, um Daten anschliessend zu verschlüsseln und Lösegeld zu erpressen. Eine wirksame Schutzmassnahme gegen diese Bedrohung ist die Segmentierung der Netzwerke in kleinere Teilbereiche. Die Netzwerksegmente verhindern eine ungebremste Ausbreitung von Schadsoftware. Für eine schnelle Segmentierung des Netzwerks ohne Änderung an der Netzwerkstruktur eignet sich der Einsatz von IoT-Gateways, wie beispielsweise das Endian 4i Edge X. Es lässt sich einfach vor die einzelnen Segmente schalten, sorgt für eine sichere Kommunikation und ist mit vielen aufein-

ander abgestimmten Sicherheitsfunktionen ausgestattet.

2. Autorisierungen zentral verwalten

Schon jetzt zeichnet sich ab, dass der Trend zum dezentralen Arbeiten die Pandemie überdauern wird. Das bringt immer mehr Mitarbeitende ins Home-Office und sorgt für eine wachsende Fragmentierung der IT-Landschaften. Eine wachsende Menge externer Geräte und Nutzer sind auf einen stabilen Zugriff auf die zentralen Unternehmensressourcen angewiesen. IT-Administratoren brauchen deshalb ein zentrales Tool, über das sich alle Zugriffsrechte verwalten lassen. Darüber können sie granulare Rechte und Berechtigungen für einzelne Anwender oder Anwendergruppen in Echtzeit erteilen und widerrufen. Zudem sind Regelungen hilfreich, die festlegen, von wo und wann ein Zugriff erlaubt ist, beispielsweise während der normalen Geschäftszeiten und vom Home-Office oder dem Arbeitsplatz des Mitarbeiters aus. Ein Zugriff von einem Land, in dem die Firma keine Niederlassung hat, kann beispielsweise unterbunden werden.

3. Zwei-Faktor-Authentifizierung einführen

Trotz aller Warnungen sind unsichere Passwörter ein grosses Sicherheitsrisiko. Ein Blick auf die Top-Zwanzig-Liste der deutschen Passwörter vom Hasso-Plattner-Institut verdeutlicht die Dimension des Problems: Seit Jahren belegt die einfache Zahlenreihe 123456 den ersten Platz, gefolgt von 123456789, passwort und ähnlich einfallslosen Kombinationen, die eine automatisierte Brute-Force-Attacke in Sekundenschnelle entschlüsseln kann. Vor dem Hintergrund des Home-Office-Trends sollten Unternehmen deshalb einen Schritt weiter gehen und für die Fernzugriffe ihrer Mitarbeiter die Zwei-Faktor-Authentifizierung einführen. Hier wird beim Anmeldeprozess noch ein weiterer Faktor integriert, der eine zusätzliche Barriere für Angreifer darstellt. Am häufigsten ist die «Besitz-Komponente», bei der der Anwender über ein bestimmtes Gerät verfügen muss, beispielsweise sein Smartphone, auf das ein zeitlich begrenztes Passwort geschickt wird.

4. Zertifikate für sichere M2M-Kommunikation

Mit der zunehmenden Digitalisierung kommunizieren immer mehr technische Geräte miteinander. Auch bei Maschinen und Anlagen müssen Unternehmen daher sicherstellen, dass nur Geräte darauf zugreifen, die dafür zuvor eine Berechtigung erhalten haben. Zertifikate gewinnen vor diesem Hintergrund an Bedeutung, denn sie sorgen für eine sichere Machine to Machine-Kommunikation (M2M), indem sie jedem Gerät und jeder Maschine eine eindeutige Identität verleihen, mit der sie sich gegenüber anderen Maschinen, Systemen und Personen ausweisen können. Ausserdem werden Zertifikate auch für die Verschlüsselung der Kommunikation eingesetzt. Damit lässt sich beispielsweise verhindern, dass Daten bei der Übertragung an eine zentrale IoT-Plattform, gestohlen oder manipuliert werden.

Das Endian 4i Edge X erfüllt alle Anforderungen an industrielle Sicherheit und Konnektivität mit einer breiten Palette an Konnektivitätsoptionen wie Ethernet oder 4G.

5. Belegschaft sensibilisieren

Angreifer wissen, dass der Mensch meist eine sensible Schwachstelle in der IT-Sicherheit darstellt und schleusen ihre Schadsoftware deshalb oft per Mail ins Unternehmen. Die Pandemie hat diese Strategie leider noch erfolgreicher gemacht. Unsicherheit, ständig neue Informationen und die Unmöglichkeit, sich im Home-Office mal eben schnell mit den Kollegen auszutauschen, tragen zu dieser Entwicklung bei. IT-Kriminelle verschicken beispielsweise Mails, die angeblich wichtige Informationen zu den derzeit geltenden Regelungen oder wirtschaftlichen Hilfen enthalten. Sobald der Empfänger auf einen mitgesendeten Link oder Anhang klickt, installiert sich ein Schadprogramm. Auch Social-Engineering-Angriffe haben zugenommen. Hier kontaktieren Angreifer gezielt bestimmte Mitarbeiter, die sie vorab schon länger beobachten und versuchen, sie zur Herausgabe sensibler Informationen zu oder einem Geldtransfer zu bewegen. Unternehmen sollten deshalb ihre Mitarbeitenden für die unterschiedlichen Risiken sensibilisieren und entsprechende Handlungsempfehlungen ausarbeiten.

6. Netzwerke visualisieren

Administratoren müssen in den immer komplexeren Netzwerken den Überblick behalten. Eine grafische Darstellung der Netzwerkstrukturen ist dabei sehr hilfreich. Über sie lässt sich verständlich nachvollziehen, welche Sensoren, Geräte und Menschen innerhalb des Unternehmensnetzwerks miteinander kommunizieren und zu welchen Systemen sie über die Unternehmensgrenzen hinweg Kontakt haben. Eine solche Visualisierung kann auch die Grundlage für die zu Beginn beschriebene Netzwerksegmentierung sein. In transparenten Netzwerken lassen sich verdächtiges Verhalten und Anomalien in der Kommunikation schnell entdecken. Damit haben Unternehmen die Möglichkeit, Cyber-Attacken schneller zu enttarnen, noch bevor ein grösserer Schaden entsteht.

7. Notfallplan erstellen

Trotz bester Vorbereitung gibt es keinen hundertprozentigen Schutz vor Cyberattacken. Unternehmen müssen sich bewusst sein, dass selbst bei gewissenhafter Vorsorge immer ein Restrisiko bleibt. Cyberkriminalität hat sich in der vernetzten Welt zu einem lukrativen Business mit solidem Wachstum entwickelt. Angreifer wissen Schwachstellen und aktuelle Trends geschickt für sich zu nutzen und sind den Unternehmen oft einen Schritt voraus. Es empfiehlt sich daher, einen IT-Notfallplan zu entwickeln, der im Ernstfall eine Fortführung der Geschäftstätigkeit sicherstellt. «

AUTOR

Raphael Vallazza, CEO Endian


Endian

Infoservice
Endian Headquarter
Hypatiastrasse 2, I-39100 Bozen
Tel. 0039 0471 63 17 63, Fax 0039 0270 0594638
info@endian.com, www.endian.com