Lizenziert für Herrn Nico Werner.
Die Inhalte sind urheberrechtlich geschützt.

06.21

56. Jahrgang
Dezember 2021
Seiten 257 – 300

www.ZIRdigital.de

ZIR

Zeitschrift Interne Revision

Fachzeitschrift für Wissenschaft und Praxis

Herausgeber:
DIIR Deutsches Institut für Interne Revision e.V.

Standards · Regeln · Berufsstand

Management · Best Practice · Arbeitshilfen

Wissenschaft · Forschung

ESV ERICH SCHMIDT VERLAG

20380

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zirdigital.de) - 10.12.2021 15:03

Lizenziert für Herrn Nico Werner.
Die Inhalte sind urheberrechtlich geschützt.

NICO WERNER

Vertraue niemandem!

Cybersecurity im Zeitalter der Digitalisierung

Nico Werner *ist Head of Cybersecurity bei der telent GmbH und war Referent bei den Digitalen Tagen des DIIR 2021.*

Ob Geschäftsführer oder Werkstudent, ob im Controlling oder in der Produktion: Unabhängig von der hierarchischen Stellung oder der Abteilung nutzen Cyberkriminelle jede Angriffsfläche, die sich ihnen bietet. Das Thema IT-Sicherheit geht deswegen alle im Unternehmen etwas an. Denn um die Gefahren zu erkennen und abzuwehren, muss man sich ihrer erstmal bewusst sein. Schließen lassen sich Sicherheitslücken am besten durch ein ganzheitliches Konzept, das neben Technologie und Prozessen auch den Menschen berücksichtigt.

1. Einleitung

„Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein." Das Zitat des US-amerikanischen Sicherheitsexperten Gene Spafford brachte es bereits im Jahr 1989 auf den Punkt – 100-prozentige Sicherheit gibt es in der IT nicht. Daran hat sich bis heute nichts geändert, im Gegenteil: Der Trend zu Industrie 4.0 bietet Cyberkriminellen immer neue Möglichkeiten. Denn um von den Vorteilen der Digitalisierung zu profitieren, müssen vernetzte Systeme miteinander sprechen. Genau darin liegt das Problem: Je mehr die Informationstechnologie (IT) und die Operational Technology (OT) zusammenwachsen, desto mehr Schlupflöcher entstehen, durch die schädliche Daten in Unternehmen eindringen oder Informationen unerwünscht nach außen abfließen. Doch wie gelingt das eigentlich?

2. Immer mehr Tore öffnen sich

Cyberkriminalität macht weder an Landesgrenzen noch an verschlossenen Werkstoren halt. Und je digitaler die Betriebe werden, desto mehr Einfallstore entstehen. Früher waren die Netze der IT und die OT physisch streng voneinander getrennt. Die Mitarbeiter in den Büros und Rechenzentren verwendeten das Unternehmens-LAN, während die Fertigung in einem eigenen, in sich geschlossenen Prozessnetzwerk arbeitete. Da dieses nicht ans Internet angebunden war, konnten Hacker es schwerlich knacken. Doch das ändert sich, je smarter die Fabriken werden, beispielsweise damit Hersteller oder externe Dienstleister einen Fernzugriff für die Wartung erhalten. Durch die Vernetzung spielt es plötzlich auch eine wichtige Rolle, dass viele industrielle Leit- und Steuerungssysteme veraltet sind und seit Längerem keine Sicherheitsupdates mehr erhalten haben. Damit haben Cyberkriminelle leichtes Spiel.

3. Hacking-Tools wirken harmlos

Schadprogramme, Hackerangriffe, Ransomware zur Erpressung von Lösegeld: Die Zahl der Cyberattacken auf deutsche Firmen und die damit verbundenen Kosten steigen von Jahr zu Jahr. Für Cyberkriminelle ist das ein lukratives Geschäft. Die Täter müssen längst nicht mehr hochbegabte IT-Nerds sein, denn Hacking-Tools und -Anleitungen sind im Internet verfügbar. Von wo Gefahr droht, ist nicht immer offensichtlich. Mögliche Hacking-Tools können so harmlose Gegenstände sein, wie die auf Messen in großer Zahl als Giveaways verschenkten USB-Sticks oder von Kunden mitgebrachte externe Festplatten, die Viren oder Schadsoftware auf das Netzwerk übertragen. Diese Entwicklung ist nur einer von vielen Gründen, die Sicherheitsstruktur gemäß Zero Trust umzubauen. Das Konzept ist ein Paradigmenwechsel, denn es macht grundsätzlich keinen Unterschied zwischen Nutzern, Geräten oder Diensten innerhalb und außerhalb des eigenen Netzwerks. Es vertraut prinzipiell keinem, prüft den kompletten Datenverkehr, und alle Beteiligten müssen sich authentifizieren. Zero Trust kann in diesem Fall gravierende Schäden oder Datenverluste verhindern, indem grundsätzlich jeder mobile Datenträger eine Datenschleuse,

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zirdigital.de) - 10.12.2021 15:03

Lizenziert für Herrn Nico Werner.
Die Inhalte sind urheberrechtlich geschützt.

wie zum Beispiel das Produkt InDEx, durchlaufen muss. Erst wenn der Unternehmensrechner einen erfolgreich absolvierten Scan erkennt, erlaubt er den gefahrlosen Anschluss.

Gefahren lauern auch außerhalb des Firmengeländes, etwa, wenn Mitarbeiter Handys oder Laptops mit eingeschalter Bluetooth- oder WLAN-Funktion bei Bahnreisen benutzen. Die Geräte versuchen, sich mit einem bekannten Zugangspunkt zu verbinden oder mit demjenigen, der das stärkste Signal sendet. Das nutzen Täter für einen Man-in-the-Middle-Angriff, indem sie einen entsprechenden WLAN-Punkt einrichten, über den die Kommunikation läuft. Das Opfer glaubt, in einem vertrauenswürdigen Netzwerk zu kommunizieren, ohne den unsichtbaren Man-in-the-Middle zu bemerken, der beispielsweise Passwörter abgreifen und Daten abfangen kann.

Neben immer raffinierteren Cyberangriffen durch professionelle oder externe Hacker gibt es auch eine wachsende Bedrohung durch Innentäter, die absichtlich oder versehentlich sensible Informationen auf internen Unternehmenssystemen preisgeben. Konkrete Zahlen gibt es nicht, aber die Art der Angriffe lässt Rückschlüsse auf Insiderwissen von Mitarbeitern zu, etwa bei Denial-of-Service-Attacken auf nur intern bekannte IP-Adressen. Dabei wird das System mit so vielen Anfragen bombardiert, dass es zusammenbricht und für normale Anfragen zunächst außer Gefecht gesetzt ist.

4. Gesetzliche Anforderungen steigen

Angesichts der steigenden Zahl von Cyberattacken stellt sich mittlerweile nicht mehr die Frage, ob ein Unternehmen angegriffen wird, sondern wann. Ohne Vorkehrungen bleiben Kriminelle in Netzwerken oft zu lange unbemerkt. Das neue IT-Sicherheitsgesetz 2.0 legt deswegen den Schwerpunkt auf die Angriffserkennung und erhöht die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), damit es Sicherheitslücken detektieren und Cyberangriffe abwehren kann. Betreiber von Kritischen Infrastrukturen (KRITIS) müssen in der Lage sein, einen Angriff mit geeigneten Technologien zu erkennen. Dafür brauchen sie ein Monitoring-System, wie zum Beispiel SIEM (Security Information und Event Management), das mithilfe künstlicher Intelligenz potenzielle Bedrohungen identifiziert, um schnell reagieren zu können. OT-Systeme sind allerdings noch nicht auf aktive Monitoring-Tools ausgelegt und fahren sich herunter, wenn die Anwendung

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zirdigital.de) - 10.12.2021 15:03

Lizenziert für Herrn Nico Werner.
Die Inhalte sind urheberrechtlich geschützt.

Abb. 1: *Der Mensch ist im Dreiklang der Cybersecurity das schwächste Glied; Quelle: telent*

zu scharf eingestellt ist. Im Sinne der Sicherheit lassen sich die Mauern zwar unendlich hochziehen, doch wenn Mensch und Maschine dann nicht mehr arbeiten können, ist nichts gewonnen. Ein ganzheitliches Sicherheitssystem hält deswegen die Waage zwischen Security und Usability.

5. Schäden werden gravierender

Die digitale Transformation verknüpft alles mit jedem und wird in wenigen Jahren IT- und OT-Netze komplett miteinander verweben. In dieser durchlässigen Welt des Industriellen Internet of Things (IIoT) nutzen Cyberkriminelle die IT als Einfallstor, um in die OT einzudringen. Was das bedeutet, zeigt sich auch an möglichen Auswirkungen. Verglichen mit der klassischen Unternehmens-IT führen Sicherheitsattacken auf industrielle Systeme zu Schäden in ganz anderen Dimensionen, wenn etwa eine Fertigungslinie stillsteht, eine fehlgesteuerte Anlage Menschen verletzt oder durch den Angriff auf eine kritische Infrastruktur ein Stromnetz offline geht. Jede erfolgreiche Industrie-4.0-Strategie muss deswegen der Cybersecurity hohe Priorität einräumen und

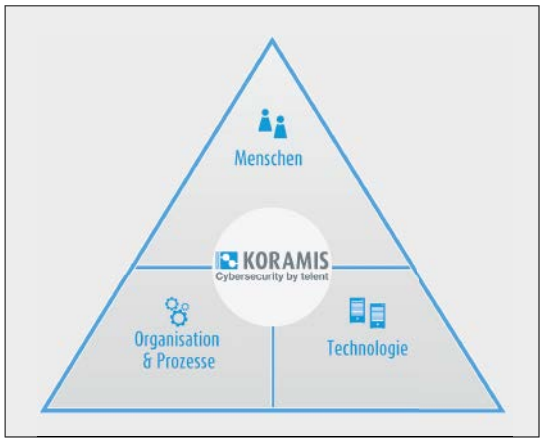

Abb. 2: *Ein ganzheitliches IT-Sicherheitskonzept bezieht Menschen, Prozesse und Technologie ein; Quelle: telent*

Sicherheit ganzheitlich im Dreiklang von Technologie, Prozess und Mensch denken. Statische Sicherheit nach dem bisherigen Prinzip Security as a Function, das alleine auf der technischen Ebene ansetzt, reicht bei Weitem nicht mehr aus.

Um das Thema Sicherheit effektiv umzusetzen, fehlen Unternehmen oft die personellen Kapazitäten oder das qualitative Know-how. Schließen lässt sich diese Lücke durch die Automation der Sicherheit. Dabei verändert sich der Blickwinkel: weg von Security by Function, hin zum ganzheitlichen Security by Design. Dieses Prinzip integriert Sicherheit zusätzlich in schriftlich definierten Prozessen, zum Beispiel zur Risikoanalyse oder Qualitätssicherung, und bildet Rollen, Verantwortlichkeiten und Tätigkeiten innerhalb der Organisation sowie die benötigten Technologien ab. Das setzt von Anfang an ein durchdachtes Sicherheitskonzept voraus, das ausgehend von der Aufgabe der Technik unter anderem die Voraussetzungen für die prozesskonforme Anwendung durch die Nutzer analysiert. Zero Trust drückt sich an dieser Stelle darin aus, dass beispielsweise von Herstellern implementierte Standardprotokolle abgeschaltet werden, wenn sie für die eigentliche Aufgabenerfüllung nicht notwendig sind.

6. Mitarbeiter gezielt im Visier

Jede Cybersecurity-Strategie ist nur so gut wie ihr schwächstes Glied. Im ganzheitlichen Dreiklang sind das nicht die Technologien und Prozesse, sondern der Mensch (vgl. Abbildung 1). Cyberkriminelle machen sich das zunutze und ziehen alle Register des Social Engineering. Sie erzeugen geschickt Stresssituationen über Gefühle, wie Angst oder Empathie, etwa indem sie bei einem Telefonat im Hintergrund Babygeschrei vom Band abspielen, sodass die Angerufenen aus Mitgefühl unbedacht Informationen preisgeben.

Ein ganzheitliches IT-Sicherheitskonzept bezieht Menschen, Prozesse und Technologien ein (vgl. Abbildung 2). Regelmäßige Awareness-Trainings können über die Risiken aufklären und die Aufmerksamkeit gegenüber den Gefahren hochhalten. Allerdings vernachlässigen viele Unternehmen es sträflich, ihre Mitarbeiter entsprechend zu schulen. Die Führungsebene ist hier in der Verantwortung: Cybersecurity ist Chefsache! Und je durchlässiger die Trennlinie zwischen IT und OT in der Industrie 4.0 wird, desto wichtiger wird ein zeitgemäßer Schutz gegen ausgefeilte Cyberkriminalität gemäß dem Motto: Zero Trust – Vertraue niemandem!

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zirdigital.de) - 10.12.2021 15:03