Ausgabe
05.2021
6,90 Euro

econo

Die starken Seiten der Wirtschaft

ANPACKEN!

„Sauberer Wasserstoff bietet einen gewaltigen Hebel beim Klimaschutz“

Dr. Melanie Maas-Brunner, Vorstandsmitglied des Vereins Zukunft Metropolregion Rhein-Neckar sowie der BASF SE

WIRTSCHAFTSSTANDORT WALLDORF | LOGISTIK & TRANSPORT

HACKING |

Kritische Infrastruktur im Visier

Die Bedrohung durch Cyber-Attacken hat ein bislang nicht gekanntes Ausmaß erreicht. So die Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Doch Unternehmen sind nicht schutzlos ausgeliefert – das zeigte die Cybersecurity Conference 2021.

Bild: Pixabay

Es war nur ein E-Mail-Anhang, den der Mitarbeiter geöffnet hatte. Doch die Folgen waren dramatisch: Unbemerkt verschlüsselte eine Ransomware die Computersysteme des Unternehmens. Nicht nur Produktion, Verkauf, Kundenservice und Buchhaltung standen still. Schließlich zahlte der Geschäftsführer das geforderte Lösegeld und wartete auf die erlösende Nachricht der Erpresser. Vergebens.

Das geschilderte Szenario entstammt keinem schlechten Kriminalfilm, vielmehr ist es mittlerweile trauriger Alltag in deutschen Unternehmen. Vor kurzem schlug das Bundesamt für Sicherheit in der Informationstechnik (BSI) Alarm: Die Anzahl der Schadprogramm-Varianten sei stark gestiegen, die Lage der IT-Sicherheit in Deutschland kritisch. Kriminelle nutzten mittlerweile aufwendige Angriffsstrategien, die früher nur in der Cyberspionage zum Einsatz kamen. Cyberangriffe hätten zuletzt bei 86 Prozent der deutschen Unternehmen Schaden angerichtet.

Umso wichtiger ist Sensibilisierung und Aufklärung. Ein Ziel, das sich auch die Cybersecurity Conference auf die Fahnen geschrieben hat, organisiert von der Mannheimer SAMA PARTNERS Business Solutions GmbH. Am 21. und 22. Oktober 2021 war es im Schloss Mannheim wieder soweit. Dieses Jahr bildeten der aktuelle Stand der Bedrohungslage, Strategien und Instrumente der Cyber-Verteidigung, neue Security-Trends und zukünftige Arbeitsformen Schwerpunkte des zweitägigen Programms mit 30 Vortragenden.

„Wir wollen in den Unternehmen Awareness für Cybersecurity schaffen“, fasst Haithem Derouiche das Hauptanliegen der Konferenz zusammen. Der Geschäftsführer von SAMA PARTNERS sieht mittelständische Unternehmen prozessual oft nicht gut aufgestellt, auch lasse die technische Umsetzung zu wünschen übrig. Denn Cybersecurity koste Geld und die Expertinnen und Experten seien rar gesät. Umso wichtiger sei es, in den mittelständischen Unternehmen ein Sicherheitsbewusstsein zu schaffen und sie beim Aufbau ihrer Cybersecurity zu unterstützen.

Haithem Derouiche umreißt das ideale Vorgehen, um der jeweiligen Gefährdungslage adäquat zu entsprechen: In einem ersten Schritt gelte es, ein Security-Grundgerüst an IT-Prozessen zu etablieren und die jeweilige ISO-Konformität herzustellen. „Hier geht es unter anderem um das Passwort-, Benutzer- und Asset-Management sowie die Frage, wann

welche internen Audits stattfinden“, erklärt Derouiche. In einem zweiten Schritt werden die technischen Lösungen dann einer eingehenden Sicherheitsprüfung unterzogen, etwa durch interne und externe Penetrationstests.

Die Bedrohung schläft nie

Ein weiterer Schritt könne in der Etablierung eines Security Operation Centers (SOC) bestehen. Die Bedrohung aus dem Internet schläft nämlich nie, hat keinen Urlaub und ist nie krank. Entsprechend muss auch die Abwehr sieben Tage die Woche an 24 Stunden verfügbar sein. „Ein solches SOC überwacht nicht nur die IT-Systeme eines Unternehmens und analysiert alle Ereignisse. Das SOC stellt im Falle einer konkreten Attacke auch ein Incident-Response-Team zur Verfügung, das die Angriffswerkzeuge möglichst schnell isoliert und eine Lösung findet, um die Geschäftstätigkeit des Unternehmens zu gewährleisten“, fasst Derouiche den Ansatz zusammen.

Eigene Fachkräfte, Partner und externe Dienstleister müssten engmaschig kooperieren und im Falle eines Vorfalls schnell verfügbar sein, um die Spuren des Angriffs nachzuvollziehen und so dafür zu sorgen, dass Behörden und Versicherungen alle Informationen erhalten, um die Schuldigen ermitteln und den Schaden abwickeln zu können. Und auch die Geldgeber und Investoren müssten wissen, dass der entsprechende Angriff nicht aufgrund von Nachlässigkeit geschehen konnte, sondern alle notwendigen Sicherheitsmaßnahmen ergriffen wurden.

An diese Gedanken konnte Mathias Bölle nahtlos anschließen. Der Leitende Kriminaldirektor in der Abteilung Cybercrime/Digitale Spuren des Landeskriminalamtes Baden-Württemberg machte in seinem Vortrag deutlich, wie wichtig ein koordiniertes Vorgehen von Kriminalpolizei und Unternehmen ist, um Cyberkriminalität effektiv zu bekämpfen. Denn die Bedrohung sei groß: Täter gingen hoch professionell und stark arbeitsteilig vor und griffen Unternehmen aller Größenklassen mit immer ausgefeilteren Fishing-Attacken an.

Doch der Werkzeugkasten von Prävention, Detektion und Reaktion sei gut gefüllt und reiche von Firewalls, Virenscannern und der Schulung von Mitarbeitenden bis zu Intrusion-Detection-Systemen und der Überwachung des Dark Nets. Eine besondere Rolle spielten die Zentrale Ansprechstellen Cybercrime (ZAC) der Polizeien, die Unternehmen im Schadensfall beratend und ermittelnd zur Seite stehen. Und obwohl die Täter meist im Ausland säßen, würde kontinuierlicher Ermittlungsdruck die Geschäftsmodelle weniger tragfähig machen. Ein wichtiger Appell – vor dem Hintergrund, dass nur circa 25 Prozent der Angriffe zur Anzeige kommen.

Dr. Michael Ebner, Chief Information Security Officer bei der EnBW Energie Baden-Württemberg AG, zeigte in seinem Beitrag deutlich, wie wichtig diese Kooperation besonders für Sektoren und Branchen Kritischer Infrastrukturen (KRITIS) ist. Hier steht nicht der Schutz vor Datendiebstahl, sondern die Verhinderung von Betriebsunterbrechungen ganz oben auf der Prioritätenliste. Gleichwohl seien diese Attacken nicht komplett zu verhindern, vielmehr müsse man damit rechnen, dass die Angreifer in alle Systeme vordringen könnten. Für KRITIS-Unternehmen ein besonders schwerwiegendes Problem. So könne der hackerbedingte Ausfall von Stromgeneratoren, Kühlwasserpumpen oder Überdrucksystemen katastrophale Folgen für die Gesellschaft haben.

Umso wichtiger sei die Herstellung von Cyber-Resilienz durch ein gutes Risikomanagement sowie die durchdachte Planung und ständige Einübung des Ernstfalles. Besondere Wachsamkeit erforderten die zentralen Elemente der technischen Infrastruktur: Denn für viele Maschinen seien keine Updates verfügbar, Dienstleister bauten Backdoors für die Wartung ein und die Systemhärtung sei nur schwierig machbar – Probleme, die auch viele produzierende Betriebe kennen. Ebner empfiehlt vor allem, Nutzerkonten und Netzwerke zu überwachen und ein besonderes Augenmerk auf die Wartungs- und Prüfungsrechner der Service-Mitarbeiter externer Dienstleister zu richten. Und zu guter Letzt schärfte er ein, dass Cyber-Security Chefsache sein müsse: Ein CISO (Chief Information Security Officer) sei immer nur so stark, wie er von der Geschäftsführung gemacht werde.

Viele der Vortragenden betonten den leergefegten Fachkräftemarkt. Cybersecurity-Expertinnen und -Experten sind sehr gefragt. Umso wichtiger ist es, die kommende Generation für die Thematik zu begeistern. Deshalb fand parallel zur Konferenz der Hackathon „Capture the Flag“ statt, in dem die Teilnehmenden ihre Fähigkeiten in 18 Challenges aus den Kategorien Kryptographie, Forensik, Pwn, Steganography und Web Exploitation unter Beweis stellen konnten. „Wir wollen möglichst viele Menschen dafür gewinnen, dass sie ihre Fähigkeiten für das Gute einsetzen und nicht, um die eBay-Konten der Nachbarn zu hacken“, fasst Haithem Derouiche den Anspruch des Hackathons schmunzelnd zusammen. *Stefan Burkhardt*

Zweitägiges Programm: Ende Oktober fand die Cybersecurity-Conference im Schloss Mannheim mit insgesamt 30 Vortragenden statt. Hier ist ein Vortrag im imposanten Rittersaal zu sehen.
Bild: Burkhardt

INTERVIEW |

Zugriff trotz Firewall

Das Kompetenzzentrum IT-Sicherheit am FZI Forschungszentrum Informatik in Karlsruhe untersucht IoT (Internet of Things)-Produkte auf Sicherheitslücken und unterstützt Unternehmen bei der Konzeption sicherer Geräte. Der Leiter des Zentrums Ingmar Baumgart erklärt Schwachstellen und Lösungsansätze.

Inwiefern können IoT (Internet of Things)-Produkte ein Sicherheitsrisiko für Unternehmen darstellen?
Ingmar Baumgart: Zum einen sind viele IoT-Produkte in der Lage, mit Sensoren wie etwa Mikrofon, Kamera und GPS auch sehr sensible Daten aufzuzeichnen. IoT-Produkte können aber oft auch steuernd in die Umgebung eingreifen. Wenn es einem Angreifer gelingt, diese Geräte zu übernehmen, kann er zum Beispiel Türen öffnen oder schließen, Brandmeldesysteme manipulieren oder bestimmte Pumpen einer Produktionsanlage steuern. Dann sind massive Auswirkungen vorprogrammiert.

Zur Person: Ingmar Baumgart. Bild: FZI

Wie kommt es zu diesen Sicherheitslücken bei IoT-Produkten?
Baumgart: In sehr vielen Fällen sind es Implementierungsfehler in der Software. In der Desktop-Welt werden für Betriebssysteme und Anwendungen Updates ausgerollt, sobald eine entsprechende Sicherheitslücke entdeckt wurde. Diese Updates sollten eigentlich auch bei IoT-Produkten erfolgen, da ansonsten die Sicherheitslücken bestehen bleiben. Oft ist das aber nicht der Fall.

Was könnten die Entwickler der IoT-Produkte tun, um die Sicherheit der Geräte zu verbessern?
Baumgart: Sie sollten bereits bei der Entwicklung dieser Produkte bedenken, welche Angreifer in Frage kommen, wie hoch das entsprechende Schadenspotenzial ist und welche Schutzziele erfüllt werden müssen, damit dieser Schaden nicht eintritt. Wenn man solche Überlegungen erst an den Schluss der Produktentwicklung stellt, ist es schwierig, die Anforderungen noch nachträglich zu erfüllen.

Was sollten Unternehmen bedenken, die IoT-Produkte einsetzen?
Baumgart: Man sollte sich zunächst bewusstmachen, dass jedes dieser Produkte Sicherheitslücken haben kann. Ein besonderes Risiko stellt die ständige Erreichbarkeit der IoT-Produkte über das Internet dar. Eine Vielzahl von Angreifern kann so weltweit Zugriff auf diese Produkte erlangen. Man muss sich deshalb zunächst einmal fragen, ob man die Kommunikationsmöglichkeiten nicht sinnvoll einschränken kann. Dann sollte man prüfen, in welchem Kontext ein bestimmtes IoT-Produkt eingesetzt wird, wie sensibel die Daten sind, die von diesem Produkt erfasst werden können und wie kritisch es wäre, wenn ein Angreifer die Kontrolle über ein solches Produkt erlangt. Das ist eine klassische Risikoabwägung.

Und noch ein wichtiger Punkt: Unternehmen haben meist eine Firewall, die das eigene Netzwerk gegenüber dem Internet schützt. IoT-Produkte bauen jedoch oft durch die Firewall eine Verbindung zum Hersteller auf. Gibt es dort Sicherheitslücken, können Angreifer über diese Verbindung trotz Firewall Zugriff auf das Unternehmens-Netzwerk erlangen.

Interview: Stefan Burkhardt