EnBW
Cyber Security

Programmheft zum Messestand

Inklusive Info zur NIS-2-Anforderung

Gemeinschaftsstand der EnBW Cyber Security, Exeon Analytics und TechniData IT-Gruppe

it-sa 2024, Halle 7A Stand 616

Kommen Sie auf einen Barista-Cyber-Kaffee vorbei!


Halle 7A
Stand 616

Inhalt

Editorial: Play Hard. Protect Smart.

Willkommen auf unserem Messestand auf der it-sa 2024
PLAY HARD. PROTECT SMART. – gut gewappnet gegen Cyberangriffe
In einer Zeit, in der laut der aktuellen Studie des Branchenverbandes Bitkom 7 von 10 Unternehmen bereits von Hackerangriffen betroffen waren, wird die Bedrohungslage durch Cyberattacken immer ernster. Selbst der Deutsche Bundestag ist nicht verschont geblieben. Diese kontinuierlich wachsende Gefahr macht die it-sa zum Pflichttermin für alle, die für IT- und OT*-Sicherheit verantwortlich sind.

Cyberangriffe sind heute vielseitiger und komplexer denn je. Um ihnen wirksam entgegenzutreten, braucht es spezialisierte Technologien, die gezielt auf verschiedene Bedrohungen reagieren können. Gleichzeitig ist es entscheidend, die IT- bzw. OT-Sicherheit als Ganzes im Blick zu behalten und unterschiedliche technische Lösungen intelligent zu kombinieren.

Zudem wird es mit den stetig wachsenden Anforderungen an die Cybersicherheit für Unternehmen und Organisationen immer schwieriger, alle Aspekte der IT- und OT-Sicherheit eigenständig abzudecken. Deshalb ist es ratsam, auf starke Partner zu setzen, die in ihren jeweiligen Teildisziplinen die notwendige Expertise mitbringen. Gemeinsam lassen sich so Synergien nutzen und eine umfassende Sicherheitsstrategie aufbauen.

Aus diesem Grund haben sich die EnBW Cyber Security GmbH, die Exeon Analytics AG und die TechniData IT-Gruppe GmbH zusammengeschlossen, um Ihnen auf der diesjährigen it-sa ihre wegweisende Partnerschaft zu präsentieren. Diese Kooperation vereint langjährige Expertise sowie innovative Technologien und bietet umfassenden Schutz gegen die wachsenden Bedrohungen der Cyber-Kriminalität.

Gemeinsam stark für Ihre Cybersicherheit!

Gemeinsam entwickeln wir passgenaue Sicherheitslösungen, die sowohl technologische als auch prozessuale Herausforderungen effektiv adressieren. Unsere Lösungen sind auf die spezifischen Anforderungen von Unternehmen, kritischen Infrastrukturen, Organisationen und öffentlichen Verwaltungen zugeschnitten. Sie bieten robuste sowie zukunftssichere IT- und OT-Sicherheitskonzepte.

Mit unserer Partnerschaft setzen wir neue Maßstäbe in entscheidenden Bereichen der Cyber-Security:

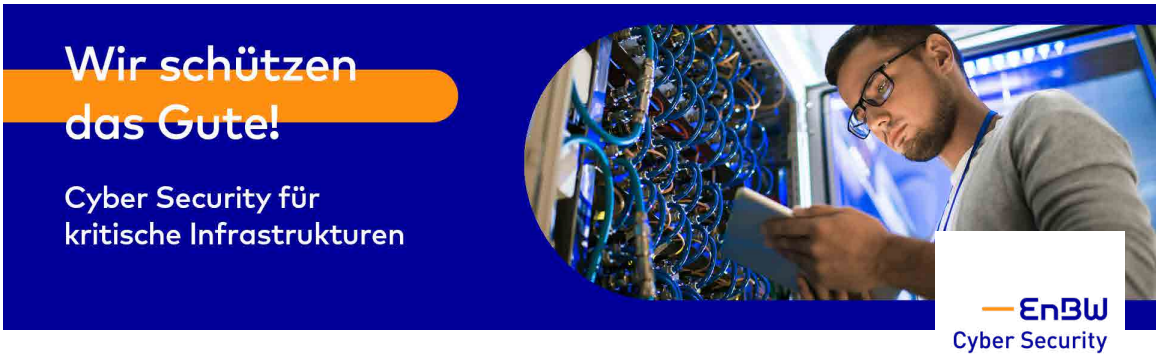
- Gesetzliche Compliance
- Schwachstellenanalysen und Penetrationstests
- Managed-Security-Services sowie Security Information and Event Management (SIEM)
- KI-basierte Netzwerkanalyse

Unsere Lösungen schützen Ihre digitalen IT- und OT-Infrastrukturen effektiv und umfassend. Als führende Experten für Cyber-Security verfügen wir über tiefgehendes Know-how und langjährige Erfahrungen in der Abwehr von Bedrohungen. Gemeinsam stehen wir für Sicherheit, Verlässlichkeit und kontinuierlichen Fortschritt in der Cyber-Security.

Besuchen Sie uns auf unserem Messestand und lassen Sie sich von den gebündelten Cyber-Security-Lösungen der EnBW Cyber Security GmbH, Exeon Analytics AG und TechniData IT-Gruppe GmbH überzeugen!
Wir freuen uns darauf, Ihnen unsere innovativen Lösungen für Unternehmen, kritische Infrastrukturen, Organisationen und öffentliche Verwaltungen vorzustellen.

* OT = Operational Technology

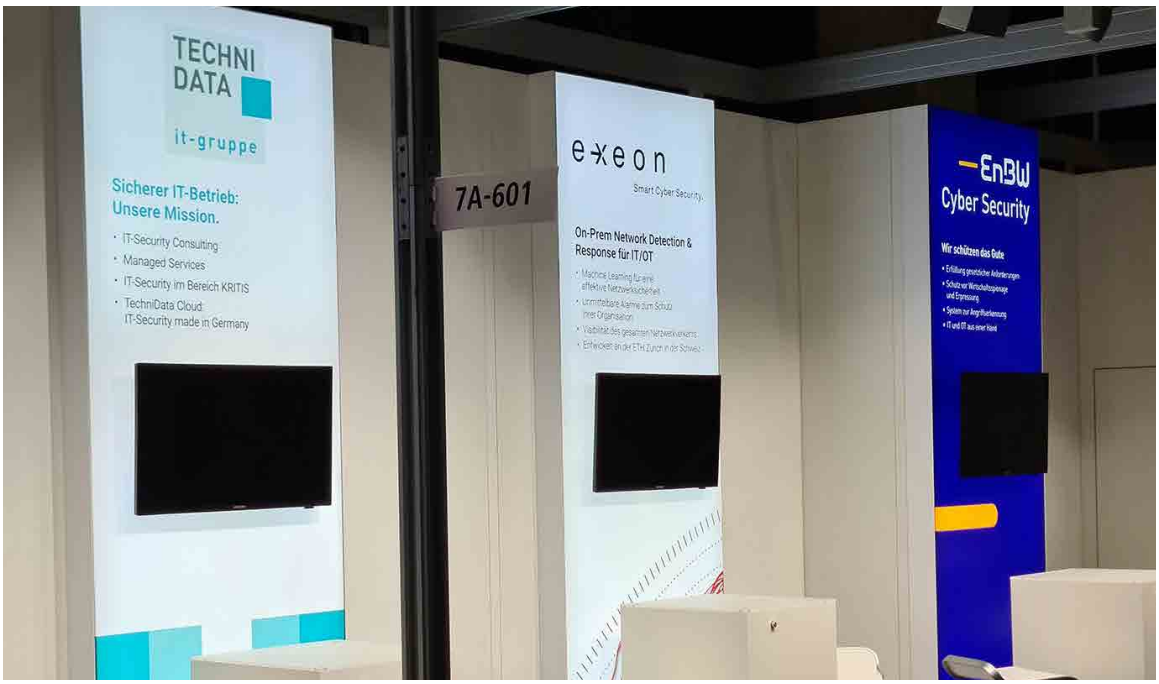
Auf einen Blick: Die Aussteller am Messestand

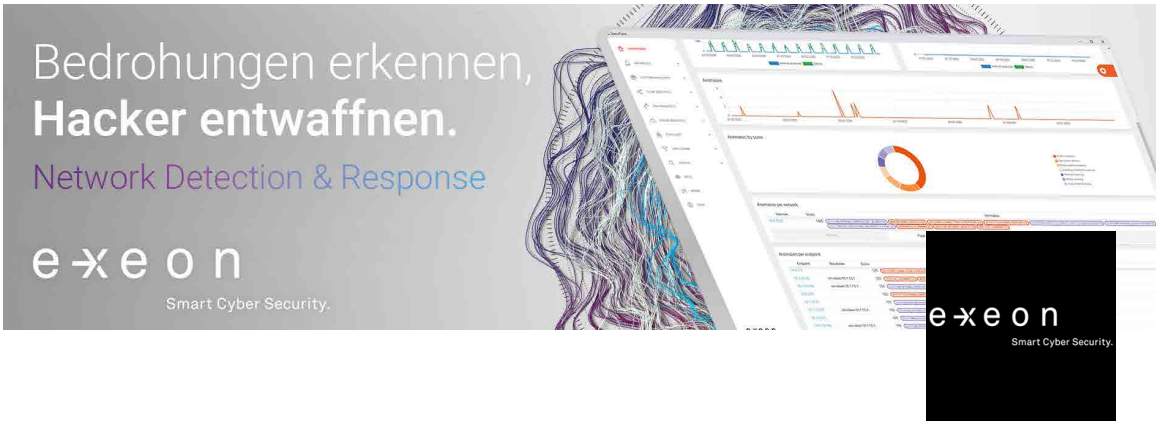


EnBW Cyber Security

Managed-Security-Services für IT und OT

Die EnBW Cyber Security GmbH bietet Beratungsdienstleistungen und Cyber-Security-Lösungen für Unternehmen und Organisationen zum Schutz vor Cyberangriffen, Wirtschaftsspionage und Erpressungen. Als Managed-Security-Service-Provider (MSSP) kümmert sich die EnBW Cyber Security um die IT- und OT-Sicherheit von Unternehmen und Organisationen. Sie sorgt rund um die Uhr dafür, dass deren Systeme und Daten sicher sind. Festangestellte Cyber-Security-Analyst*innen überwachen hierfür im eigenen Security Operation Center (SOC) Ihre Unternehmensnetzwerke auf Anomalien, um etwaige Bedrohungen unmittelbar zu erkennen und sofort darauf zu reagieren. Das Leistungsspektrum umfasst ebenfalls Beratungsleistungen nach der KRITIS-Verordnung und gemäß der NIS-2-Anforderungen, der ISO 27001 oder dem BSI-Grundschutz. Die Analyse von IT- und OT-Infrastrukturen - etwa durch Penetrationstests und Schwachstellenanalysen - komplettieren das Lösungsportfolio.





Exeon Analytics

Network Detection & Response für Unternehmen und Organisationen

Die Exeon Analytics AG ist ein Schweizer Cybersecurity-Unternehmen, das sich auf den Schutz von IT- und OT-Infrastrukturen durch KI-gesteuerte Sicherheitsanalysen spezialisiert hat. Die Network Detection & Response (NDR)-Plattform ‹ExeonTrace› bietet die Möglichkeit, Netzwerke zu überwachen, Cyber-Bedrohungen sofort zu erkennen und somit die IT-Landschaft Ihres Unternehmens effektiv zu schützen – schnell, zuverlässig und komplett hardwarefrei.

TechniData IT-Gruppe

Cloud- und Hosting-Security-Lösungen

Die TechniData IT-Gruppe bietet als Service- und Solution Provider ein umfassendes Leistungsangebot für sichere IT-Infrastrukturen - vom IT-Consulting über den IT-Betrieb bis zum IT-Support. Ausgehend von individuellen Anforderungen analysiert, plant, konzipiert und betreibt TechniData die IT-Systeme von Unternehmen und Organisationen in eigenen hochsicheren Rechenzentren in Deutschland.
Als erfahrener IT-Dienstleister und unabhängiger Cloud-Solution-Provider stellt die TechniData IT-Gruppe performante Cloud-Technologien zur Verfügung und bietet Security-Lösungen zum Schutz von Daten, Netzwerke und IT-Systemen. Mit den Services von TechniData IT-Gruppe verlassen sich die Kunden auf einen reibungslosen, zuverlässigen und wirtschaftlichen Betrieb ihrer IT-Infrastrukturen und Anwendungen.

Aus aktuellem Anlass: BKA wegen neuer Zahlen alarmiert – Cyberattacken kosten deutsche Firmen jährlich 266,6 Milliarden Euro.

Mit fortschreitender Digitalisierung und Vernetzung steigt für Unternehmen und Organisationen das Risiko von Cyberangriffen. Allein in Deutschland waren im vergangenen Jahr laut der aktuellen Studie vom 24. August 2024 des Branchenverbandes Bitkom 7 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen. Der Schaden betrug 266,6 Milliarden Euro.

Milliardenschäden durch Cyberkriminalität

Daten sind verschwunden, Passwörter funktionieren nicht mehr, oder der gesamte Bildschirm ist plötzlich gesperrt: Cyberattacken können einzelne Computer, jedoch auch ganze Netzwerke in Unternehmen und Organisationen lahmlegen.

Die Angriffe haben meist verheerende Folgen für die Betroffenen. Der Digitalverband Bitkom schätzt, dass die Cyberkriminalität in Deutschland im vergangenen Jahr Schäden im Wert von mehr als 266,6 Milliarden Euro verursacht hat.

Besonders heikel sind Attacken auf sogenannte kritische Infrastrukturen, zu denen beispielsweise die Energie- und Wasserversorgung, der Verkehrssektor sowie auch die medizinische Versorgung gehören.

Ausfälle haben hier direkte negative Auswirkungen auf das Leben von Bürger*innen. Dem Schutz kritischer Infrastrukturen kommt daher eine hohe Bedeutung zu.

Erneut über 100.000 gemeldete Cyberangriffe 2023

Laut einer Studie von Cybersecurity Ventures fand 2023 alle 39 Sekunden ein Cyberangriff statt, was über 2.200 Attacken pro Tag entspricht. Basierend auf Branchenstudien schätzen Cybersicherheitsexperten, dass jedes Jahr mehr als 800.000 Menschen Opfer von Ransomware-Angriffen, Phishing-Angriffen oder Datenschutzverletzungen werden.

Das Bundeskriminalamt (BKA) hat bundesweit im vergangenen Jahr erneut über 100.000 Cyberangriffe registriert. Die Zahlen aus der inländischen Kriminalstatistik zeigten jedoch allenfalls „die Spitze des Eisbergs“, betont BKA-Vizepräsidentin Martina Link. Denn zum Einen schätzte das BKA das „Dunkelfeld“ der Cyberkriminalität auf bis zu 90 Prozent – nur einer von 10 Fällen komme in der Regel tatsächlich zur Anzeige. Zum Anderen seien in der Statistik keine Angriffe von Tätern aus dem Ausland erfasst, die jedoch stark zugenommen hätten.

Am 13.05.2024 haben die Bundesinnenministerin Nancy Faeser und der Präsident des Bundeskriminalamtes, Holger Münch, zusammen mit der Leiterin des Bundesamt für Sicherheit in der Informationstedhnik (BSI), Claudia Plattner berichtet, wie stark Deutschland von Cyberkriminalität betroffen ist. Demnach haben Angriffe aus dem Ausland stark zugenommen.

Wer wird angegriffen?

Große und zahlungskräftige Unternehmen, Einrichtungen die stark in der Öffentlichkeit stehen wie Universitäten und Gesundheitsversorger sowie Städte und Gemeinden stehen im Fokus von Cyber-Attacken.
September 2023: Angriff auf einen Klinikverbund, bei dem Krankenhäuser weder per Telefon noch per E-Mail erreichbar waren. Auch Arbeiten auf den Intensivstationen und auf der Radiologie waren eingeschränkt.

Oktober 2023: In 72 Kommunen kam es durch einen Ransomware-Angriff dazu, dass Rettungskräfte kaum noch einteilbar waren. Standesämter und das Wohnungswesen waren teilweise nur eingeschränkt arbeitsfähig, und es kam zu Verzögerungen bei Fahrerlaubnisbehörden. Im Fokus stehen immer häufiger auch Verkehrsverbünde und Flughäfen. Bei einem Angriff auf einen Verkehrsverbund im März 2023 kam es zu Verzögerungen beim Verkauf des 49,-Euro Tickets, und entwendete Daten wurden im Darknet veröffentlicht.

Immer mehr Industrieunternehmen geraten in das Visier von Hackern

Industrieunternehmen stehen weltweit vor sich stetig verschärfenden Herausforderungen. Der Bericht „The Crisis of Convergence: OT/ICS Cybersecurity 2023" von TXOne Networks beschreibt u.a. die Zunahme von Angriffen über Ransomware-as-a-Service (RaaS), die Ausnutzung von Schwachstellen in Lieferketten und das Auftreten von staatlich finanzierten Hackern sowie anderen politisch motivierten Akteuren im Zuge geopolitischer Spannungen. Dieser Jahressicherheitsbericht untersuchte eine Reihe von Themen, die für die heutige Industrial Control Systems (ICS)-Sicherheit relevant sind:

- Ransomware
- Wartung von OT-Systemen und Bedenken hinsichtlich der Integration von Informationstechnologie (IT)
- Nationalstaatliche Cyber-Angriffe und ihre Auswirkungen
- Fehlendes engagiertes Fachpersonal zum Schutz von OT und ICS
- Fehlende OT/ICS-Investitionen in die Sicherheit

- Neue Vorschriften und Normen treiben die OT/ICS-Verteidigung voran
- Integrität von Lieferketten

Quelle: Cybersicherheits-Herausforderungen in der Industrie 2023 - TXOne Networks Bericht (security-insider.de)

Sicherheitslage in der deutschen Industrie: Einblick in OT-Sicherheitsvorfälle

Die jüngsten Erkenntnisse aus dem Bericht „The Crisis of Convergence: OT/ICS Cybersecurity 2023" von TXOne Networks werfen ein Schlaglicht auf die dringende Notwendigkeit, die Sicherheit in Operational Technology (OT) zu verstärken. Der Bericht zeigte auf, dass eine überwältigende Mehrheit von 97% der befragten Unternehmen angab, dass IT-Sicherheitsvorfälle auch ihre OT-Umgebungen beeinträchtigten. Dies unterstreicht die zunehmende Verschmelzung von IT- und OT-Systemen und die daraus resultierenden Herausforderungen an die Sicherheit.

In einer detaillierten Analyse der Sicherheitsvorfälle bei 54 deutschen Unternehmen innerhalb der letzten 12 Monate offenbarte der Bericht eine besorgniserregende Häufigkeit und Vielfalt von Angriffen auf OT-Systeme mit folgenden Details:

- Anfälligkeiten von nicht ausreichend gesicherten Systemen stellten mit 50% die häufigste Ursache für Sicherheitsvorfälle dar. Diese Schwachstellen sind kritische Risikofaktoren, die es Angreifern ermöglichen, in industrielle Steuerungssysteme einzudringen.

- Ransomware-Attacken, bei denen Angreifer Daten verschlüsseln und ein Lösegeld für die Freigabe fordern, machten 37% der Vorfälle aus. Sie können zu erheblichen finanziellen Einbußen und Betriebsunterbrechungen führen.

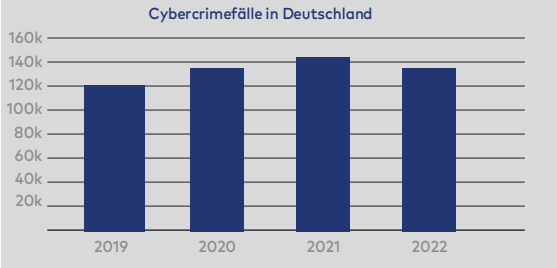
- Advanced Persistent Threats (APT)-Attacken, die durch ihre Komplexität und Hartnäckigkeit gekennzeichnet sind, wurden in 41% der Fälle identifiziert. Diese Angriffe können über längere Zeiträume hinweg unbemerkt bleiben und stellen eine fortwährende Bedrohung für Unternehmen dar.

Diese Zahlen verdeutlichen, dass die Bedrohungslandschaft für OT-Umgebungen vielschichtig ist und eine ganzheitliche Sicherheitsstrategie erfordert. Unternehmen müssen in umfassende Sicherheitslösungen investieren, die sowohl präventive Maßnahmen als auch die Fähigkeit zur schnellen Reaktion auf Vorfälle umfassen.

Die Schulung von Mitarbeiter*innen und die kontinuierliche Überwachung der Systeme sind dabei unverzichtbare Bestandteile, um die Sicherheit und Resilienz der kritischen Infrastrukturen zu gewährleisten.

Die Lage der IT- und OT-Sicherheit in Deutschland

In den CVSS-Score, einen international anerkannten Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird, fließen auch Angriffsvektoren und andere Faktoren ein. Die Kritikalität der bekannt gewordenen Schwachstellen schwankte stark. Gut drei Prozent wiesen niedrige und 45 Prozent mittlere Scoring-Werte auf der zehnstufigen Skala auf. Mit 53 Prozent - somit mehr als die Hälfte - wiesen hohe (7–9) oder kritische (9–10) CVSS-Scores auf. Der Anteil kritischer Schwachstellen lag bei rund 15 Prozent.



Neben den genannten Schwachstellen in Softwareprodukten erreichten das BSI auch Meldungen über Schwachstellen in Industrial Control Systems (ICS). ICS sind Systeme zur Steuerung industrieller Produktion, zur Automatisierungskontrolle, zur Mensch-Maschine-Interaktion und zu anderem mehr. Im Berichtszeitraum wurden dem BSI insgesamt 24 schwachstellenbehaftete ICS gemeldet.
Quelle: www.bsi.bund.de

Cyberangriffe aus China und Russland nehmen zu

Einer Beobachtung zufolge - die eine Bitkom-Umfrage bei mehr als 1.000 Unternehmen aus verschiedenen Branchen bestätigt - sind insbesondere die Angriffe aus Russland und China 2022 sprunghaft angestiegen. Demnach haben 43 Prozent der betroffenen Unternehmen mindestens eine Attacke aus China identifiziert (2021: 30 Prozent), 36 Prozent haben Urheber in Russland ausgemacht (2021: 23 Prozent). Zugleich gehen die Angreifer immer professioneller vor, wie die Studie zeigt. Erstmals liegen das organisierte Verbrechen und Banden an der Spitze der Rangliste der Cybercrime-Täter. Bei mehr als der Hälfte (51 Prozent) der betroffenen Unternehmen kamen Attacken aus diesem Umfeld. 2021 lag der Anteil hier bei 29 Prozent, vor drei Jahren noch bei 21 Prozent.

Spätestens mit dem russischen Angriffskrieg gegen die Ukraine und einer hybriden Kriegsführung, auch im digitalen Raum, ist die Bedrohung durch Cyberattacken für die Wirtschaft in den Fokus gerückt. „Die Bedrohungslage ist aber auch unabhängig davon hoch“, so Bitkom-Präsident Achim Berg. Die Angreifer werden laut Berg immer professioneller und sind häufiger im organisierten Verbrechen zu finden. Allerdings könnten Unternehmen mit Maßnahmen und Vorsorge diese Angriffe abwehren oder zumindest den Schaden begrenzen.

Zwei Drittel der Unternehmen erwarten Cyber-Attacken

Insbesondere Ransomware-Angriffe bedrohen die Existenz von Unternehmen, betonen BKA und Bitkom. Bei diesen Cyberattacken legen Schadprogramme komplette Datenbanken und IT-Systeme lahm. Laut einer globalen Studie eines IT-Dienstleisters haben mehr als 40 Prozent der nach einem derartigen Angriff erpressten Unternehmen ein Lösegeld gezahlt. Dies erfolgt jedoch oft vergeblich, weil der von den Erpressern zur Lösung angebotene Schlüssel häufig nicht funktioniert habe. „Phishing“ sei nach wie vor das „Haupteinfallstor“ für derartige Schadsoftware. Mit „Phishing“ ist das Versenden von E-Mails mit infizierten Anhängen oder Links gemeint.
Quelle: www.bsi.de

EnBW Cyber Security kennt sich mit kritischen Infrastrukturen aus

Die stetig wachsende Bedrohungslage stellt Unternehmen, Kommunen und Behörden vor immer größere Herausforderungen. Mit der Gründung des Tochterunternehmens EnBW Cyber Security GmbH hat der Konzern der EnBW Energie Baden-Württemberg AG im Mai 2022 auf die gestiegene Nachfrage nach Sicherheitslösungen zum Schutz vor Cyberangriffen reagiert. Als Betreiberin von Erzeugungsanlagen und Netzen gibt die EnBW nun ihr Know-how insbesondere in der Überwachung von sogenannten kritischen Infrastrukturen weiter. „Durch die zunehmende Digitalisierung werden Angriffe komplexer, vielschichtiger und subtiler. Der Bedarf an Sicherheitslösungen nimmt zu“, erklärt Frank Brech, Geschäftsführer der EnBW Cyber Security. „Unternehmen und Organisationen, denen es an eigenen Ressourcen und der notwendigen Expertise fehlt, benötigen hierfür einen kompetenten und erfahrenen Partner. Als Tochter eines KRITIS-Unternehmens wissen wir sehr gut, worauf es beim Schutz von Infrastrukturen ankommt“, so Frank Brech. Ziel von EnBW Cyber Security sei es, zum bestmöglichen Schutz kritischer Infrastrukturen beizutragen und somit die Versorgung der Bevölkerung sicherzustellen.

Wie unerlässlich eine geeignete Absicherung und hohe Widerstandsfähigkeit gegen Cyberangriffe insbesondere für Betreiber Kritischer Infrastrukturen sind, verdeutlicht das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) des Bundesamts für Sicherheit in der Informationstechnik (BSI). Es verpflichtet alle KRITIS-Betreiber, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen".

Verstöße gegen das IT-SiG 2.0 ahndet das BSI je Vorfall mit Geldstrafen von bis zu 20 Millionen Euro oder von bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes – je nachdem, welcher Betrag höher ist.

Umfassende Sicherheitsstrategien für KRITIS-Unternehmen

Das Lösungsangebot von EnBW Cyber Security richtet sich an KRITIS-Unternehmen aus der Energie-, Wasser-, Gesundheits- und Telekommunikationsbranche sowie an Städte, kommunale Verwaltungen und Behörden. „Aber auch Non-KRITIS-Unternehmen und Produktionsunternehmen aus dem Automobil- und Maschinenbaubereich sowie Händler*innen und Dienstleister*innen erhalten von uns auf Wunsch umfassende Sicherheitsstrategien. Von der Analyse über die Beratung bis zum fertigen Betriebsprodukt liefern wir alles aus einer Hand", erläutert Frank Brech, Geschäftsführer der EnBW Cyber Security GmbH.

Auf dem Weg zur Absicherung gegen Cyberattacken seien zu Beginn in der Regel sogenannte Penetrationstests hilfreich. „Damit testen wir zunächst die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems. Dies erfolgt mit Mitteln und Methoden, die potenziell dazu geeignet sind, unerlaubt in das System einzudringen. So spüren wir Schwachstellen in den jeweiligen Systemen auf und können dann Empfehlungen zur Behebung derselben geben", erklärt Brech.

Kontinuierliche Überwachung von IT- und OT-Systemen

Mit dem Cyber Defence Center (CDC) und den darin enthaltenen Managed-Security-Services ermöglichen die Cybersicherheits-Spezialist*innen der EnBW-Tochter eine kontinuierliche Überwachung der IT- und OT-Systeme ihrer Kund*innen. Gemeint ist damit die permanente Überprüfung der Informationstechnik (IT) sowie der operativen Technologien (OT) mit Hard- und Software, welche etwa in der Industrie Maschinen und Geräte steuern. „Durch die zunehmende Vernetzung von IT und OT im Zuge der digitalen Transformation öffnen sich auch neue Einfallstore für Hacker", so Frank Brech. Während die Unterbrechung der Produktion von Gütern Lieferketten zum Erliegen bringen könnten, seien beispielsweise beim Ausfall eines OT-Netzwerks einer Klinik die Patientensicherheit und damit Menschenleben gefährdet. „Neben der Gebäudetechnik bieten in Krankenhäusern auch digitale und vernetzte Medizingeräte Schwachstellen, die Hacker ausnutzen können. Im schlimmsten Fall können sie den Krankenhausbetrieb empfindlich stören und versuchen, Lösegeld zu erpressen", meint Frank Brech.
Quelle: EnBW Eco*Journal

BSI-Lagebericht 2023: Bedrohung durch Cyber-Kriminalität in Deutschland auf Rekordniveau

Mit fortschreitender Digitalisierung und Vernetzung steigt für Organisationen das Risiko von Cyberangriffen. Allein in Deutschland waren in den vergangenen zwei Jahren laut Branchenverband Bitkom 7 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen. Der entstandene Schaden pro Jahr: etwa 266,6 Milliarden Euro!

Erster digitaler Katastrophenfall

207 Tage

konnten bürgernahe Dienstleistungen wie Elterngeld in Folge eines Ransomware-Angriffes nicht erbracht werden.

Phishing an Staat und Industrie

34.000 E-Mails

mit Schadprogrammen wurden durchschnittlich monatlich in deutschen Regierungsnetzen abgefangen.

Neue Varianten an Schadprogrammen

250.000 neue Varianten

an Schadprogrammen wurden durchschnittlich täglich im Berichtszeitraum bekannt.

Softwareprodukte im Fokus

27.000 Schwachstellen

stellten Einfallstore für Hacker dar, rund 24 Prozent mehr als im vergangenen Berichtszeitraum.

Aktuell: Die NIS-2-Richtlinie - Neue Chancen und Anforderungen im Bereich Cybersecurity

Mit der Einführung der neuen NIS-2-Richtlinie hat die Europäische Union einen bedeutenden Schritt zur Stärkung der Cybersicherheit ihrer Mitgliedsstaaten unternommen. Diese verpflichtet Unternehmen und Organisationen, angemessene Cybersicherheitsmaßnahmen zu ergreifen sowie schwerwiegende Vorfälle zu melden. Die EU-Staaten sind gefordert, die Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) bis zum Oktober 2024 in nationales Recht umzusetzen.

Ab Oktober 2024 wurde die NIS-2-Direktive als verbindliche Cybersicherheits-Richtlinie der EU umgesetzt. Voraussichtlich wird sie zu diesem Zeitpunkt oder in absehbarer Zeit danach in Kraft treten. Unternehmen und Organisationen in bestimmten Branchen müssen dann nachweislich angemessene Cybersecurity-Maßnahmen ergreifen und schwerwiegende Vorfälle melden.

Was ist die NIS-2-Richtlinie?

Die NIS-2-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit) zielt darauf ab, die Cybersicherheitskapazitäten und Widerstandsfähigkeit in der EU zu stärken. Diese Maßnahmen sind angesichts der zunehmenden Anzahl und Komplexität von Cyberangriffen auf kritische Infrastrukturen und Digitaldienstleister in Europa besonders wichtig.

Ein wesentlicher Aspekt der NIS-2-Richtlinie ist die Erweiterung ihres Geltungsbereichs. Während die ursprüngliche NIS-Richtlinie hauptsächlich auf Betreiber kritischer Infrastrukturen in Sektoren wie Energie, Verkehr, Banken und Gesundheitswesen abzielte, schließt die NIS-2-Richtlinie nun auch Anbieter digitaler Dienste, Hersteller medizinischer Geräte, Rechenzentren und kommunale Eigenbetriebe ein. Zusätzlich zur Erweiterung des Geltungsbereichs führt die neue Richtlinie strengere Sicherheitsanforderungen und Meldepflichten ein. Unternehmen und Organisationen müssen ein höheres Maß an Cybersicherheitsmaßnahmen implementieren und sicherstellen, dass sie auf Sicherheitsvorfälle effektiv reagieren können. Vorfälle, die erhebliche Auswirkungen auf die Dienstleistungserbringung haben, müssen innerhalb von 24 Stunden gemeldet werden.

Hohe Sanktionen bei Nichteinhaltung

Um die Einhaltung der neuen Vorschriften zu gewährleisten, sieht die NIS-2-Richtlinie strengere Sanktionen vor. Unternehmen, die die Anforderungen nicht erfüllen, drohen Geldstrafen von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes.

Ein notwendiger Schritt in der digitalisierten Welt

Die Einführung der NIS-2-Richtlinie markiert einen wichtigen Meilenstein in den Bemühungen der EU, die Cybersicherheit zu verbessern und ihre digitale Souveränität zu stärken. Angesichts der zunehmenden Abhängigkeit von digitalen Technologien und der wachsenden Bedrohung durch Cyberkriminalität ist dies ein notweniger Schritt, um die Sicherheit und Stabilität kritischer Infrastrukturen und Dienste zu gewährleisten.

Unternehmen und Organisationen in der EU müssen nun die neuen Anforderungen umsetzen und ihre Sicherheitsstrategien anpassen. Die kommenden Monate und Jahre werden zeigen, wie effektiv diese Maßnahmen zur Abwehr von Cyberbedrohungen beitragen und wie gut Europa auf die Herausforderungen einer vernetzten Welt vorbereitet ist.

Neue Herausforderungen und Chancen für Unternehmen

Die NIS-2-Richtlinie bietet sowohl Herausforderungen als auch Chancen zur Verbesserung der Cybersicherheit. Einerseits ermöglicht sie die Optimierung von Cybersicherheitspraktiken und stärkt das Vertrauen der Kund*innen. Andererseits erfordert die Umsetzung zusätzliche Ressourcen und Investitionen in die Sicherheitsinfrastruktur. Geschäftsführende und Vorstände in betroffenen Unternehmen müssen angemessene Sicherheitsmaßnahmen implementieren sowie die Einhaltung der Richtlinie sicherstellen. Bei Verstößen drohen erhebliche Bußgelder und persönliche Haftungsrisiken. Die Verantwortung umfasst sowohl die Prävention als auch die Reaktion auf Sicherheitsvorfälle. Ein aktives Risikomanagement und die kontinuierliche Überprüfung der Sicherheitsstrategien sind unerlässlich.

Fazit

Die NIS-2-Richtlinie fördert die Zusammenarbeit zwischen den EU-Mitgliedsstaaten. Ein neuer Mechanismus für den Informationsaustausch und die Koordination von Reaktionen auf Cyberbedrohungen werden somit eingeführt. Dies soll sicherstellen, dass Bedrohungen frühzeitig erkannt und gemeinsam bekämpft werden können.

Selbstcheck: Kennen Sie die NIS-2-Richtlinien im Detail?

Machen Sie direkt den Selbstcheck mit unserer NIS-2-Checkliste!

Ist Ihr Unternehmen in einem der folgenden Sektoren tätig?

Frühere NIS-Sektoren

- ☐ Gesundheitswesen
- ☐ Transport
- ☐ Wasserversorgung
- ☐ Energie
- ☐ Virtuelle Infrastruktur
- ☐ Anbieter digitaler Dienste
- ☐ Bankwesen
- ☐ Infrastruktur der Finanzmärkte

Zusätzliche NIS-Sektoren

- ☐ Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder -diensten
- ☐ Abwasser
- ☐ Chemikalien
- ☐ Gesundheitswesen (Pharmazie, Forschung und Entwicklung, kritische medizinische Geräte)
- ☐ Lebensmittelhersteller, -verarbeiter und -vertreiber
- ☐ Hersteller kritischer Produkte (medizinische Geräte, Computer, Elektronik, Automobile)
- ☐ Digitale Anbieter (Plattformen sozialer Netzwerke, Suchmaschinen, Online-Marktplätze
- ☐ Luft- und Raumfahrt
- ☐ Post- und Kurierdienste
- ☐ Öffentliche Verwaltung

Beschäftigen Sie mehr als 50 Mitarbeiter*innen oder beträgt Ihr Jahresumsatz bzw. Ihre Jahresbilanzsumme mehr als 10 Millionen Euro?

- ☐ Ja
- ☐ Nein

Erbringt Ihr Unternehmen Dienste, die als kritisch für die Gesellschaft angesehen werden (z.B. essenzielle Dienstleistungen für den Betrieb der Gesellschaft oder Wirtschaft)?

- ☐ Ja
- ☐ Nein

Wenn Sie eine der oben genannten Fragen mit „Ja“ beantworten können, fällt Ihr Unternehmen unter die NIS-2-Richtlinie.

Wenn Sie sich zu diesem Zeitpunkt im Geltungsbereich befinden, müssen Sie Ihre Kontaktdaten angeben:

- Teilen Sie der European Union Agency for Cybersecurity (ENISA) den Namen Ihres Unternehmens sowie die Adressen der Hauptniederlassung und anderer rechtlicher Niederlassungen in der EU mit.
- Stellen Sie der ENISA Ihre aktuellen Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern, innerhalb von 12 Monaten zur Verfügung.
- Ausländische Unternehmen, die nicht in der EU ansässig sind, jedoch Dienstleistungen erbringen (z.B. Anbieter von Datenzentren und Inhalten), müssen der ENISA einen repräsentativen Ansprechpartner vor Ort benennen.
- Aktualisierungen müssen innerhalb von drei Monaten erfolgen, wenn eine Änderung (der Adresse oder des Vertreters) wirksam wird.

Auch, wenn Sie nicht in den Geltungsbereich fallen, können Sie sich beteiligen und wichtige Vorfälle oder Cyber-Bedrohungen auf freiwilliger Basis melden.

Im Rahmen der neuen Richtlinie wird gefordert:

- Meldung eines bedeutenden Sicherheitsvorfalls innerhalb von 24 Stunden nach seiner Entdeckung
- Übermittlung einer ersten Bewertung innerhalb von 72 Stunden nach der Entdeckung des Vorfalls
- Vorlage eines ausführlichen Abschlussberichtes innerhalb eines Monats nach der Entdeckung.

Gemäß Artikel 21 der NIS-2 sollten die Mitgliedstaaten sicherstellen, dass bedeutende und wichtige Einrichtungen robuste Systeme, Strategien und bewährte Verfahren für das Risikomanagement einführen. Diese sollten eine Vielzahl von Maßnahmen und Disziplinen im Bereich der Cybersicherheit abdecken, einschließlich:

- Risikoanalyse und Sicherheit von Informationssystemen
- Bearbeitung von Zwischenfällen und Berichterstattung
- Business-Kontinuität, z.B. Backup-Management und Notfallwiederherstellung
- Krisenmanagement
- Sicherheit in den Lieferketten
- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Systemen
- Grundlegende Praktiken der Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptographie und Verschlüsselungstechnologien
- Personelle Sicherheit, Zugangskontrollen und Asset-Management
- Zero-Trust-Zugang (Multi-Faktor-Authentifizierung, kontinuierliche Authentifizierung)
- Seien Sie sich bewusst, dass die Zusammenarbeit, der Informationsaustausch und die Meldung von Vorfällen an die Behörden immer wichtiger werden.

Portrait: EnBW Cyber Security - Wir schützen das Gute!

Mit der EnBW Cyber Security GmbH als neuer Konzerntochter reagiert die EnBW auf die gestiegene Nachfrage nach Sicherheitslösungen. Kund*innen profitieren von einem umfassenden Lösungsportfolio – von der Analyse über die Beratung bis zur Umsetzung.

Die Bedrohung durch Cyberkriminalität steigt: allein in Deutschland waren in den vergangenen zwei Jahren laut Branchenverband Bitkom 7 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen. Der entstandene Schaden pro Jahr: etwa 266,6 Milliarden Euro. Unternehmen, Organisationen und Behörden wissen um den Handlungsbedarf. Vielen fehlt es jedoch an eigenen Ressourcen und der notwendigen Erfahrung, um ihre Infrastrukturen selbst zu schützen. Mit der Gründung der EnBW Cyber Security GmbH reagiert die EnBW auf diese Situation.

Die 100-prozentige EnBW-Tochter hilft Unternehmen, Behörden und Organisationen dabei, die für sie passende Sicherheitsstrategie zu finden und umzusetzen. „Durch die zunehmende Digitalisierung werden Angriffe komplexer, vielschichtiger und subtiler, der Bedarf an Sicherheitslösungen nimmt zu“, erklärt Geschäftsführer Frank Brech. „Unternehmen brauchen hier einen kompetenten und erfahrenen Partner. Als Tochter eines KRITIS-Unternehmens, wissen wir worauf es ankommt.“

Schutz von IT und OT

Das Unternehmen mit Sitz in Karlsruhe, analysiert IT- und OT-Prozesse sowie Architekturen von kritischen und nicht-kritischen Infrastrukturen. Diese werden auf Abweichungen von einem zuvor erlernten „Normalzustand“ untersucht. Vor allem die OT – also spezielle Betriebstechnik aus dem KRITIS- und Produktionsbereich – wird immer häufiger zum Ziel von Attacken. „IT und OT müssen in punkto Sicherheit zusammenhängend betrachtet werden – nur dann ist ein Unternehmen umfassend geschützt“, sagt Frank Brech.
Die Expert*innen von EnBW Cyber Security bringen dieses Wissen mit und sind zum Teil seit mehr als 10 Jahren in der Informationssicherheit tätig.

Kund*innen profitieren von umfassenden Lösungen

Das Angebot der EnBW-Tochter richtet sich u.a. an KRITIS-Unternehmen aus der Energie-, Wasser-, Gesundheits- und Telekommunikationsbranche sowie zunehmend an Städte, Kommunale Verwaltungen und Behörden. Ebenso stehen Produktionsunternehmen aus dem Automobil- und Maschinenbaubereich im Fokus. Kund*innen erhalten umfassende Lösungen von der Analyse über die Beratung bis zum fertigen Betriebsprodukt – alles aus einer Hand. Angeboten werden zum Beispiel sogenannte Penetrationstests.
Hierbei spüren Expert*innen einmalig je Testvorgang Schwachstellen in den Systemen auf und geben Empfehlungen zur Behebung. Mit dem Cyber Defence Center (CDC) und den dort erbrachten Managed-Security-Services ermöglichen die Cyber-Security-Spezialist*innen auch eine kontinuierliche Überwachung der IT- und OT-Infrastrukturen ihrer Kund*innen.

Kooperation mit dem Land Baden-Württemberg

Zu den Partnern von EnBW Cyber Security zählen seit 2020 auch das Innenministerium des Landes Baden-Württemberg sowie das Landeskriminalamt in Stuttgart: im Rahmen einer Public-Private-Non-Profit-Partnership arbeiten die Beteiligten im Kampf gegen Cyber-Kriminelle eng zusammen.
Seit Oktober 2021 bilden die Partner zudem Studierende an der DHBW Heilbronn und DHBW Mannheim im Studienzweig Wirtschaftsinformatik mit Vertiefung in Cyber Security aus. Es ist das erste Mal, dass auf Behörden-, Verwaltungs- und Wirtschaftsebene eine solche Initiative gestartet wurde, um dem zunehmenden Fachkräftemangel entgegenzuwirken.

Beratung und Cyber Risk Assessment

Viele Unternehmen oder kommunale Verwaltungen kennen die Bedeutung der IT-Sicherheit. Doch häufig stehen zu wenig Ressourcen zur Verfügung, um Aufgaben der Cyber-Security sicher zu stellen und ohne Unterbrechung des Tagesgeschäftes wahrzunehmen. Hier unterstützt die EnBW Cyber Security ihre Kund*innen bei der Auswahl organisatorischer und technischer Maßnahmen sowie beim Erstellen von Sicherheitskonzepten und Notfallplänen.

In einem ersten Schritt geht es zunächst darum, sich einen Überblick zu verschaffen. Die erfolgt beispielsweise mit einem IT-Quick-Check, um Schwachstellen und mögliche Handlungsbedarfe zu identifizieren. In einem Folgeschritt werden Vorkehrungen getroffen, z.B. mit einem Cyber-Rating, das eine Ad-Hoc Bewertung über die freizugänglichen Unternehmensinformationen beinhaltet.

Um Schwachstellen aufzuspüren, können mittels eines sogenannten Penetrationstests die Simulation eines Angriffs auf die IT-Systeme sowie eine Auswertung der Schwachstellen vorgenommen werden. Für kommunale Verwaltungen und Behörden bietet EnBW Cyber Security umfassende Beratungsdienstleistungen zur Umsetzung des BSI-IT-Grundschutzprofils bis zur Bereitstellung eines bedarfsgerechten Informationssicherheitsbeauftragten (ISB) an.

Schwerpunkt Managed-Security-Services

Viele Organisationen verfügen nicht über das technische Know-How und die personellen Ressourcen, um die Absicherung ihrer IT- und OT-Infrastrukturen selbst vorzunehmen. Als Managed-Security-Service-Provider (MSSP) bietet die EnBW Cyber Security daher ihren Kund*innen einen Managed-Security-Service im eigenen Security Operation Center (SOC) mit deutschsprachigen Analysten.

Die Dienstleistungen umfassen die kontinuierliche Überwachung des Datenverkehrs über eine Network Detection and Response Lösung (NDR) bis hin zur Erkennung und dem Monitoring von potenziellen Sicherheitsvorfällen über ein Security Information and Event Management (SIEM). NDR stellt dabei eine sinnvolle Erweiterung ggf. bereits vorhandener Sicherheitslösungen wie Firewall, Endpoint Detection and Response (EDR) sowie SIEM dar. Dies sorgt für ein erhöhtes Sicherheitsniveau.

„Mit unserem Security Information and Event Management (SIEM) können die Analyst*innen in unserem Cyber Defense Center (CDC) alle Vorgänge im IT- und OT-Netz unserer Kund*innen überwachen und Protokolldaten aus verschiedenen Bereichen des jeweiligen Unternehmens an einem zentralen Ort sammeln. Damit werden Auffälligkeiten und Abweichungen von üblichen Mustern erkannt. Mit Blick auf eine zuverlässige Absicherung der IT- und OT-Infrastrukturen unterstützen wir gemeinsam Unternehmen aus der kritischen Infrastruktur, Industrie und Produktion sowie Kommunen und Behörden“, führt Frank Brech weiter aus.

Überwachung von IT- und OT-Infrastrukturen

Mit dem CDC und den darin enthaltenen Managed-Security-Services ermöglicht die EnBW Cyber Security eine permanente Überwachung der IT- und OT-Infrastrukturen ihrer Kund*innen. IT und OT werden somit kontinuierlich mit Hard- und Software kontrolliert. Die OT steuert etwa in der Industrie Maschinen und Geräte. Gerade durch die zunehmende Vernetzung von IT und OT im Zuge von digitalen Transformationen öffnen sich neue „Einfallstore“ für Angreifer.

Technologische Partnerschaften

Zusammen mit unseren Technologiepartnern Exeon Analytics (Schweiz) und Elastic (Niederlande) im Bereich IT-Security sowie Nozomi Networks (Schweiz) im Bereich OT-Security sorgen wir für einen reibungslosen Betrieb unseres SOC und somit für die Sicherheit unserer Kund*innen. Die Überwachung des Netzwerkverkehrs erfolgt dabei über die NDR-Lösung ExeonTrace, zusammen mit der SIEM-Lösung „Elasticsearch®“.

Die Kombination dieser technischen Lösungen ermöglicht es der EnBW Cyber Security, die IT- und OT-Sicherheit ihrer Kund*innen ganzheitlich zu betrachten und somit noch deutlich besser abzusichern. EnBW Cyber Security bietet somit die Kombination der IT- und OT-Netzüberwachung aus einer Hand – als flexibles Managed-Service-Modell.

Auf einen Blick

Derzeit ist die EnBW Cyber Security der einzige Managed-Security-Service-Dienstleister eines großen Energieversorgers mit Kompetenzen in der Absicherung kritischer Infrastrukturen.

Das Unternehmen bietet sein Know-How sowie seine Cyber-Security-Lösungen für KRITIS und Non-KRITIS-Unternehmen sowie Behörden und Kommunen an.

Interview: Cyber Security ist Chefsache

Telekommunikationsdatennetze sowie Kritische Infrastrukturen sind in immer größerem Maß von automatisierten Systemanbindungen abhängig. Mit der zunehmenden Digitalisierung und Vernetzung steigt auch das Risiko, Ziel eines Cyberangriffs zu werden. Nicht erst die Ukrainekrise hat das Thema Cybersecurity deutlich stärker in den Fokus der Unternehmen und Unternehmensleitungen gebracht. Die typische Aussage „uns kennt ja keiner, es wird uns sicher nicht treffen“ fällt immer weniger. Lesen Sie zum Thema unser Interview mit Frank Brech, Geschäftsführer der EnBW Cyber Security GmbH.

Frank Brech, warum ist Cybersicherheit für Unternehmen, Behörden und Kommunen eine tägliche Herausforderung und zur Chefsache geworden?

Frank Brech: Cybersicherheit ist längst in der Mitte der Gesellschaft angekommen. Sie entscheidet darüber, ob unser digitalisierter Alltag funktioniert. Die zunehmende Digitalisierung in allen Branchen erhöht die Anfälligkeit gegenüber Cyberattacken. Den Angreifenden stehen dabei immer leistungsfähigere Werkzeuge und Methoden zur Verfügung. Gleichzeitig steigt die Abhängigkeit von automatisierten Pro- zessen und Systemen immer weiter an.

Die Frage ist daher nicht ob, sondern wann man gehackt wird. Oft sind Angreifer schon längst in das Unternehmensnetz eingedrungen, bisher nur noch nicht entdeckt worden. Sie dringen in Netze ein und analysieren erst einmal in Ruhe, wo z.B. die Backups oder sensible Kundendaten liegen. Dann richten sie gezielt größtmöglichen Schaden an. Laut Branchenverband Bitkom waren in den vergangenen zwei Jahren allein in Deutschland 7 von 10 Firmen von Datendiebstahl, Spionage oder Sabotage betroffen. Der hierdurch entstandene, jährliche Schaden wird auf 266,6 Milliarden Euro geschätzt. Wir verzeichnen eine stetig wachsende Bedrohungslage. Diese stellt Unternehmen und Behörden vor immer größere Herausforderungen.

Wie ist das Verhältnis von Datenschutz und Datensicherheit?

Frank Brech: Über 70% der erfolgreichen Cyberattacken erfolgen immer noch über den „Faktor Mensch“. Mit sogenannten Phishing-Mails werden Mitarbeiter*innen dazu gebracht, ihre Login-Daten

Frank Brech
Geschäftsführer EnBW Cyber Security GmbH

und Passwörter preiszugeben. Einfache Passwörter tun ihr Übriges, um Angreifern leichtes Spiel zu ermöglichen. Hier helfen Phishing-Aktionen und Schulungen, damit Mitarbeiter*innen immer wieder sensibilisiert werden. Als Geschäftsführer bzw. Vorstand eines Unternehmens achten Sie wahrscheinlich darauf, dass regelmäßig Brandschutzübungen stattfinden. Wie viele Cyberschutzübungen haben Sie schon durchgeführt?
Wenn z.B. in der Übung der Zugriff auf die Daten im Rechenzentrum nicht mehr möglich ist, müssen Sie sehr schnell die Frage beantworten können, wo die Backupdaten liegen und wie man darauf zurückgreifen kann.

Wann immer für die Speicherung, das Auslesen oder die Weiterverarbeitung von personenbezogenen Daten informationstechnische Systeme zum Einsatz kommen, gibt es zahlreiche technische Berührungspunkte zwischen Datenschutz und Datensicherheit.

Vor dem Hintergrund der fortschreitenden Digitalisierung, dem flächendeckenden Rollout von Intelligenten Messsystemen und darauf aufbauenden neuen Wertschöpfungsnetzwerken müssen Fragen des Datenschutzes bei der Datennutzung frühzeitig

beantwortet werden. Die Lösung ist das Wissen, welche Gefahren drohen und wie man ihnen begegnet. Essenziell für den eigenen Schutz sind die aktuelle und zukünftige Gesetzeslage sowie branchenspezifische Standards und Normen. Damit lernen wir, Gefährdungen und Risiken einzuschätzen und Versäumnisse zu vermeiden. Demnach sind Unternehmen und Behörden selbst für den Schutz vor existierenden Gefahren im beruflichen Alltag und der Sensibilisierung ihrer Mitarbeiter*innen verantwortlich.

Welche Schäden durch Cyberattacken sind am häufigsten?

Frank Brech: Schäden entstehen durch Datendiebstahl in Verbin-dung mit Erpressungen, Produktionsausfällen, dem Abgreifen von Patentinformationen sowie Image- und Reputationsschäden. Auch die Erpressung mit gestohlenen oder verschlüsselten Daten ist weit verbreitet. Zunehmend werden auch datenschutzrechtliche Maßnahmen bekannt, (z.B. das Abziehen von Kundeninformationen) oder Patentrechtsverletzungen (auch schon vor der Anmeldung). Imageschäden bei Kund*innen oder Lieferant*innen sind ebenso nicht zu unterschätzen genau so wie eine negative Medienberichterstattung. Ein wesentlicher Faktor sind zudem die Kosten für Ermittlungen und Ersatzmaßnahmen sowie die Kosten für Rechtsstreitigkeiten.

Wie können präventive Maßnahmen ergriffen werden?

Frank Brech: Um Aktivitäten der Angreifer frühzeitig erkennen zu können, helfen Techniken zur Anomalieerkennung. Das können Systeme zur Logdaten- oder Netzwerksverkehrsanalyse sein. Solche Systeme erkennen z.B., ob Daten aus dem Unternehmen ins Internet/Darknet abfließen und schlagen Alarm. Der Einsatz solcher Systeme wurde bis Mai 2023 im IT-Sicherheitsgesetz 2.0 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für KRITIS-Unternehmen und im Telekommunikationsgesetz (TKG) für große TK-Netzbetreiber verpflichtend gefordert. Idealerweise läuft die Überwachung der Alarme solcher Module in einem SOC (Security Operation Center), quasi ein NOC (Network Operation Center) für IT-Netze. In einem SOC werden zuerst automatisiert Alarme herausgefiltert, die keinen Angriff oder keine Anomalie bedeuten. Alle weiteren Alarme werden von IT-Analyst*innen bewertet. Im Falle eines potenziellen Angriffs melden diese dann Handlungsempfehlungen an die IT-Bereiche, um z.B. erkannte Angreifer zu isolieren. Nun stellt sich für Unternehmen und Organisationen die Frage, ob sie ein eigenes SOC aufbauen und betreiben oder sich hierfür einen Managed-Security-Service aus einem externen SOC einkaufen.

In der Regel wird der Aufbau eines eigenen SOC‘s am nur schwer zu rekrutierenden Fachpersonal scheitern. Zusätzlich spielt die Unternehmensgröße eine Rolle. Große Carrier bzw. TK-Netzbetreiber haben eventuell genügend Fach-Know-how an Bord, um ein eigenes SOC zu betreiben. Für die meisten Unternehmen wir der Einkauf eines Managed-Security-Service eines externen Anbieters die beste Wahl sein.

Welches Lösungsportfolio bietet hierfür die EnBW Cyber Security?

Frank Brech: Aufgrund des Fachkräftemangels haben es Unternehmen und Behörden schwer, eigene Cyber Security Spezialist*innen in ausreichender Anzahl einzustellen. Daher geht der Trend branchenübergreifend eindeutig zum Managed Security Service, den wir in unserem eigenen Cyber Defence Center anbieten. Dort nutzen wir führende Technologien aus Europa, die zum Beispiel Netzwerkverkehr sowie IT- und OT-Daten analysieren und auf Anomalien überprüfen. Auf Wunsch unserer Kund*innen finden die Analysen in deren Netzen statt, so dass keine Daten das jeweilige Netz verlassen. Für Kund*innen, deren Systeme und Daten sich bereits in der Cloud befinden, bieten wir selbstverständlich entsprechende Lösungen an.

Die Versorgung mit unentbehrlichen Gütern und Dienstleistungen stellen in Deutschland sogenannte Kritische Infrastrukturen (KRITIS) sicher. Gehören KRITIS-Unternehmen daher zur ersten Zielgruppe von EnBW Cyber Security?

Frank Brech: Ja genau, wir haben das Thema KRITIS quasi in unserer „DNA“. Viele Mitarbeiter*innen von EnBW Cyber Security kommen aus der EnBW und wissen, was beim Schutz Kritischer Infrastrukturen wichtig ist. Insofern sprechen wir auch die Sprache unserer Kund*innen und können diese passgenau beraten. Das vom BSI eingeführte IT-Sicherheitsgesetz 2.0 mit Handlungsvorgaben für KRITIS-Unternehmen muss seit Mai 2023 umgesetzt sein.

Dort ist z.B. die Einführung von Systemen zur Anomalieerkennung vorgeschrieben. Die im Oktober 2024 in Kraft tretende NIS2-Richtlinie wird die Zahl der KRITIS-Unternehmen um 30.000 – 40.000 Unternehmen erhöhen und neben den Vorgaben auch eine Managementhaftung bei Nichtumsetzung beinhalten.

Unsere Kund*innen haben oft nicht das Personal bzw. genügend Ressourcen, um solche staatlichen Vorgaben fristgerecht umzusetzen. Wir helfen ihnen dabei, diese Auflagen zu erfüllen und somit hohe Strafzahlungen im Falle der Nichteinhaltung zu vermeiden.

Feature: Unsere Referenten und Vorträge

Täuschend echte Phishing-Kampagnen, Ransomware-Erpressungen und die Gefahr von Angriffen aufgrund staatlicher Konflikte: die zunehmende Vernetzung, immer mehr Schwachstellen in Software-Produkten und der Faktor Mensch als Risiko treiben das Stress-Level in die Höhe. Erfahren Sie in spannenden und inspirierenden Vorträgen bei uns am Messestand (Halle 7A Stand 616) von Branchenkennern und Cyber-Security-Spezialist*innen, welchen Herausforderungen sich IT und OT zukünftig stellen müssen und welche Lösungen sich bieten.

NIS-2, DORA & KRITIS? Anforderungen aus den neuen Compliance-Regularien.

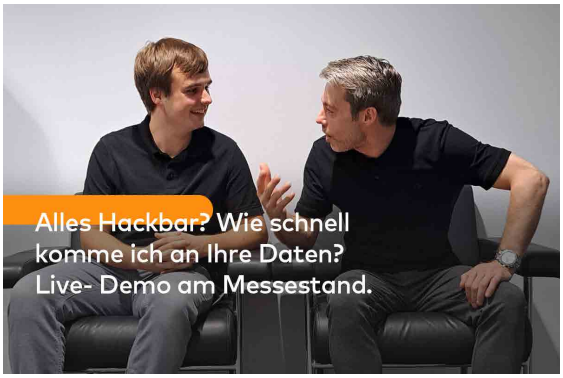
Bernd Mussgnug, Marketing Manager der EnBW Cyber Security GmbH im Gespräch mit Frank Brech, Geschäftsführer EnBW Cyber Security GmbH

Mit der Einführung der neuen NIS-2-Richtlinie hat die Europäische Union einen bedeutenden Schritt zur Stärkung der Cybersicherheit ihrer Mitgliedsstaaten unternommen. Die EU-Staaten sind gefordert, die Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) bis zum Oktober 2024 in nationales Recht umzusetzen. Diese verpflichtet Unternehmen und Organisationen, angemessene Cybersicherheitsmaßnahmen zu ergreifen sowie schwerwiegende Vorfälle zu melden. Aber was bedeutet NIS-2 und die KRITIS Verordnung konkret für Ihr Unternehmen? Wie können Sie haftbar gemacht werden? Erfahren Sie in der Key-Note Ansprache von Frank Brech alles Wissenswerte zu den rechtlichen Anforderungen von Unternehmen bezüglich Cyber-Security.

Alles hackbar? – Wie schnell kommen wir an Ihre Daten? - Live-Demo am Messestand.

Marco Fischer und Lukasz Wrobel,
Cyber-Security-Analysten der EnBW Cyber Security GmbH

Was viele nur aus Kinofilmen über Hacker kennen, ist heute im Zeitalter der Digitalisierung längst Realität. Industriespionage durch kriminelle Gruppen im Cyberspace greift auch in Deutschland immer weiter um sich. Die große Gefahr dabei: Fast jedes Unternehmen kann unsichtbar und unbemerkt ausspioniert werden. Marco Fischer und Lukasz Wrobel nehmen Sie mit in die Welt der verdeckten Informationsbeschaffung. Diese Methodik bleibt im normalen Netzwerkverkehr unbemerkt, da keine direkten Datenpakete zum Ziel geschickt werden. Die gewonnenen Daten sind dabei enorm und können erheblichen Schaden anrichten, wenn sie in die falschen Hände geraten. Unsere Mission ist es, Ihnen die notwendigen Kenntnisse zu vermitteln, um sich selbst und Ihr Unternehmen besser zu schützen!



Malware und Ransomware - Die Gesichter der Bösen.

Thomas Englert,
Cyber-Security-Analyst der EnBW Cyber Security GmbH

Ransomware-as-a-Service zeichnet sich als neuer Trend ab. Bei dem Geschäftsmodell vermieten Ransomware-Entwickler ihre Schadsoftware ähnlich wie Softwareentwickler von SaaS-Produkten. Damit bekommen Personen Zugriff auf Services und schadhafte Software ohne jegliche Kenntnisse von Softwareentwicklung. Wer steckt wirklich hinter den Kriminellen, die seit Jahren massiven Schaden an unserem Wirtschaftssystem betreiben? Thomas Englert beschreibt in seinem Vortrag das Thema Ransomware as a Service (RaaS) am Beispiel Lockbit bis ins kleinste Detail.

Cybersicherheitsvorfall! Und nun? – Effektive Krisenkommunikation statt Headless-Chicken-Modus.

Patricia Biernacki,
Referentin für Cybersicherheit in Kommunen bei der Cybersicherheitsagentur Baden-Württemberg (CSBW)

Nichts geht mehr? Erstmal durchatmen. Wie Sie dann den Headless-Chicken-Modus überwinden und worauf es bei der Kommunikation ankommt, um eine solche Krise gut zu bewältigen, steht im Fokus dieses Vortrags.

Ob Organisation, Technik oder Inhalte:
Sie bekommen Tipps für den Tag X.

Echte Cyber-Angriffe und Lessons-Learned-Lösungsansätze

Dr. Stefanie Frey und Michael Bartsch
beide Geschäftsführung der Deutor Cyber Security Solutions GmbH

Dr. Stefanie Frey und Michael Bartsch von der Deutor Cyber Security Solutions GmbH erläutern anhand eines echten Cyber-Angriffs die Auswirkungen auf die Geschäftsprozesse und zeigen Lösungsansätze auf. Die Timelines aus echten Angriffen - von der Infektion bis zur Erpressung - verdeutlichen, wie Täter vorgehen und wie die Wirkung auf Unternehmen, Organisationen und Behörden ist. Es ist das Gegenstück zu den Vorträgen aus dem Live-Hacking und fokussiert sich auf die Geschäftsprozesse sowie die organisatorischen Maßnahmen.
Der Vortrag verdeutlicht, wie schnell und schwerwiegend ein Cyber-Angriff sein kann, indem die Timelines aus realen Fällen vorgestellt werden. Der im Vortrag dargestellte Angriff begann mit einer Phishing-E-Mail, die einen infizierten Anhang enthielt, und endete mit einem Produktionsausfall, dem Verlust von Kundenvertrauen, einem Imageschaden und einem hohen finanziellen Schaden.
Der Vortrag bietet zudem Lösungsansätze, wie man sich vor Cyber-Angriffen schützen und im Ernstfall reagieren kann. Best Practices und Empfehlungen der Deutor Cyber Security Solutions GmbH werden vorstellt.

Programm:

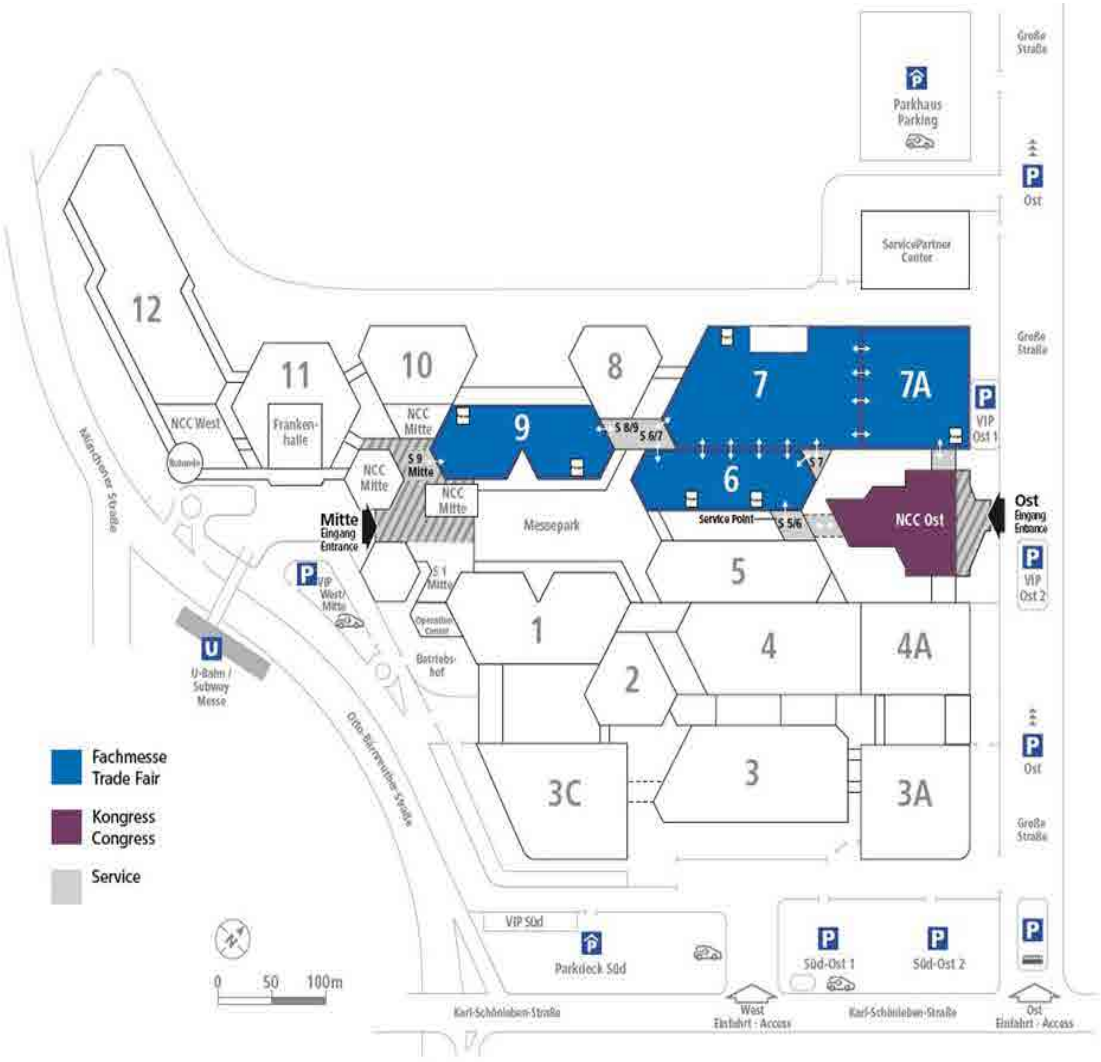
Dienstag, 22. Oktober 2023

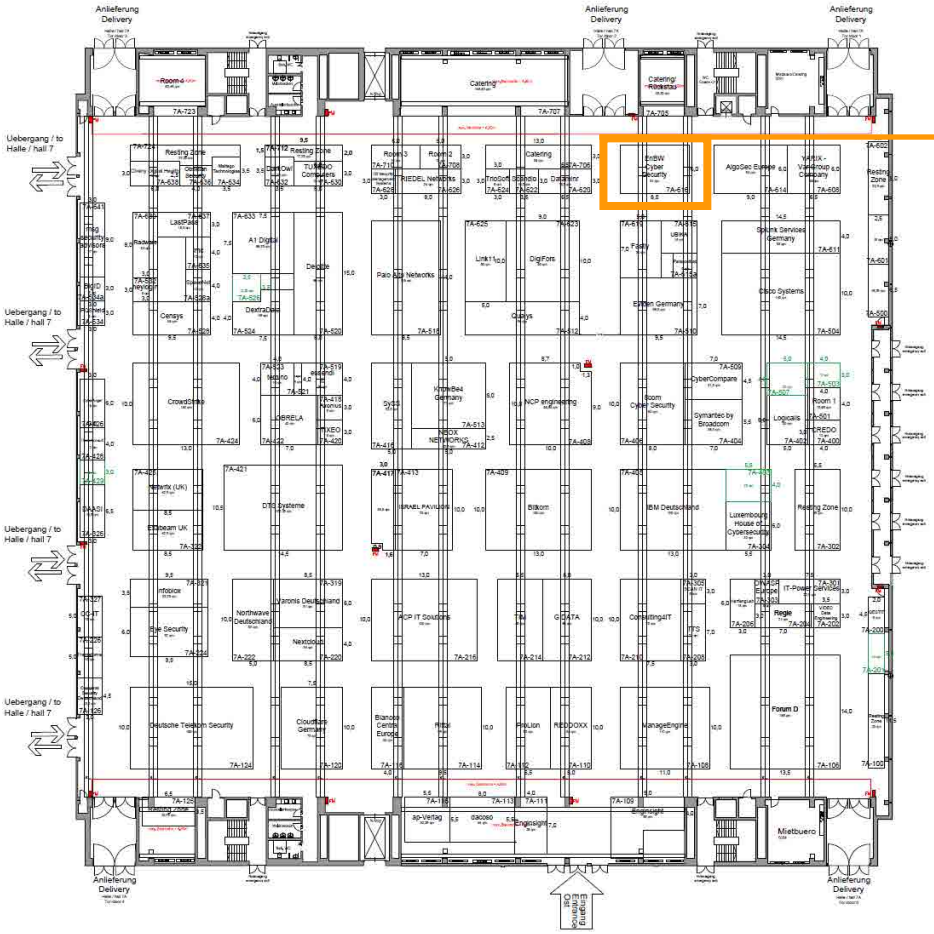
15:45 Uhr	NIS-2, DORA & KRITIS? - Anforderungen aus den neuen Compliance-Regularien (Interview und KeyNote)	Frank Brech, Geschäftsführer der EnBW Cyber Security GmbH
16:30 Uhr	Alles hackbar? Wie schnell kommen wir an Ihre Daten? – Live-Demo am Messestand (Live-Performance)	Marco Fischer und Lukasz Wrobel, Cyber-Security-Analysten, EnBW Cyber Security GmbH
17:15 Uhr	Malware und Ransomware – Die Gesichter der Bösen (Vortrag)	Thomas Englert, Cyber-Security-Analyst, EnBW Cyber Security GmbH

Mittwoch, 23. Oktober 2023

11:00Uhr	Alles hackbar? Wie schnell kommen wir an Ihre Daten? – Live-Demo am Messestand (Live-Performance)	Marco Fischer und Lukasz Wrobel, Cyber-Security-Analysten, EnBW Cyber Security GmbH
16:30 Uhr	Cybersicherheitsvorfall! Und nun? – Effektive Krisenkommunikation statt Headless-Chicken-Modus (Vortrag)	Patricia Biernacki, Referentin für Cybersicherheit, Cybersicherheitsagentur Baden-Württemberg (CSBW)
17:15 Uhr	Echte Cyber-Angriffe und Lessons- Learned-Lösungsansätze (Vortrag)	Dr. Stefanie Frey und Michael Bartsch, Geschäftsführung der Deutor Cyber Security Services GmbH

Ihr Weg zu uns: Sie finden uns in Halle 7A Stand 616





Halle 7A
Stand 616

EnBW Cyber Security
Exeon Analytics
TechniData IT-Gruppe


CYBER
NIGHT
Dienstag, 22. Oktober 2024 - ab 19 Uhr
Standparty in Halle 7A Stand 616


Halle 7A
Stand 616

Unsere Mission

Wir analysieren und überwachen Ihre IT- und OT-Infrastrukturen und machen sie jeden Tag sicherer.

Quelle: www.pexels.com


EnBW
Cyber Security

Wir schützen das Gute!

EnBW Cyber Security GmbH
Ein Unternehmen der EnBW

Durlacher Allee 93
76131 Karlsruhe

Telefon 08000 574847

cybersecurity@enbw.com
www.enbw-cybersecurity.com
https://www.linkedin.com/company/enbw-cyber-security-gmbh