Internationales Security Operations Center

Categories : Ex-Schutz & Anlagensicherheit, Im Fokus, Meldungen

Date : 12. April 2021

Ein internationales Security Operations Center (SOC) wird in der Schweiz von VINCI Energies und seinen Marken Axians (ICT) und Actemium (Industrietechnik) aufgebaut. Als Hub vernetzt es somit die mehr als 300 Cybersecurity-Spezialisten aus der Schweiz, Deutschland und weiteren europäischen Ländern und fokussiert sich auf die Sicherheit im Bereich Industrie 4.0. Dabei werden Kompetenzen für Informations- und Kommunikationstechnik (ICT) und industrielle Betriebstechnik (OT) gebündelt sowie die Erkenntnisse aus internationalen Wissenschaftskooperationen hinsichtlich kritischer Infrastrukturen verarbeitet. Ed wird auf dem Gelände des Kompetenzzentrums uptownBasel im zweiten Halbjahr 2021 eröffnen und die Schaltstelle zu den bereits existierenden lokalen Security Operations Centern in Deutschland, Tschechien, den Niederlanden, Portugal und Frankreich bilden. Kunden von Axians und Actemium können über Basel die Cybersicherheit ihrer digital vernetzten Unternehmen betreiben lassen und durch den internationalen Ansatz unmittelbar Informationen zu grenzüberschreitenden digitalen Bedrohungen erhalten.
Datendiebstahl, Cyber-Erpressungen, Systemausfälle, Spionage, Hackerangriffe, Attacken auf Produktionsanlagen und industrielle Steuerungssysteme – mit dem zunehmenden Vernetzungs- und Digitalisierungsgrad von Unternehmen steigt auch das potenzielle Risiko von Cyber-Angriffen. Bedrohungen wie der Erpressungstrojaner Emotet, das Schadprogramm WannaCry, der Computerwurm Stuxnet und Hacker-Angriffe auf Industrie-4.0-Infrastrukturen und -Netzwerke nahmen nach den Erkenntnissen von Branchenverbänden und Analysten in den letzten Jahren deutlich zu. Auch produzierende Unternehmen sind nach Angaben der Information Security Society Switzerland Opfer von Angriffen durch Schadsoftware geworden und erlitten teilweise Produktionsausfälle. Gleichzeitig stehen Unternehmen vor großen Chancen für ihre Wertschöpfung und Resilienz durch Fernarbeit, IoT-Szenarien und Künstliche Intelligenz. Nach Aussagen von Gartner ist bis 2025 damit zu rechnen, dass in 40% der Unternehmen ein Cybersecurity-Management-Team aufgebaut wird. Verschiedene Studien von Gartner, Forrester, IDC und IDG sagen zudem ein deutlich überdurchschnittliches Wachstum der Cybersecurity-Investments in den nächsten Jahren voraus.
Das Unternehmen investiert aus all diesen Gründen gezielt in den Aufbau eines internationalen Security Operations Center (SOC) Hubs am Standort Basel. Von dort aus wird nach der Eröffnung im zweiten Halbjahr 2021 für Kunden der VINCI Energies Marken Actemium (Industrietechnik) und Axians (ICT) der Betrieb von Cybersecurity-Schutzmaßnahmen erbracht oder gemeinsam mit den bestehenden lokalen SOCs in Deutschland, Tschechien und anderen europäischen Ländern koordiniert. Besonders für Industrieunternehmen, die über gewachsene Produktionsinfrastrukturen oder gezielte Industrie-4.0-Strategien verfügen, entsteht hier ein besonderer Mehrwert. Im SOC Basel werden alle vernetzten Sensoren, Maschinen, Anlagen und Geräte von Unternehmen überwacht, Security-Muster sowie -Anomalien analysiert und Schutzmaßnahmen eingeleitet, um potenzielle Angriffe abzuwehren. Dazu dient ein Cybersecurity-Leitstand im neuen Kompetenzzentrum, der rund um die Uhr mit Experten wie SOC-Analysten, Pentestern, digitalen Forensikern und ethischen Hackern besetzt ist. Für jeden Kunden werden dabei Prozesse auf Basis sogenannter „Security Playbooks“ definiert sowie mit Threat Intelligence Feeds und Malware-Information-Security-Plattformen im 7x24h-Service gearbeitet. Auch der Schutz von SCADA- und MES-Systemen der industriellen Produktion wird hier gezielt mitangeboten. Zusätzlich fließen neueste wissenschaftliche Erkenntnisse aus Forschung & Lehre an den Hochschulen Luzern, Nordwestschweiz und Stuttgart in die Aktivitäten ein. Cybersecurity-Spezialisten von Axians und Actemium sind dort selbst als Gastdozenten aktiv.

> „Mit unserem neuen SOC bieten wir ein umfassendes und tiefes Spezial-Know-how für Cyber-Bedrohungen unserer Zeit. Wir erkennen, analysieren, beheben und dokumentieren dort rund um die Uhr die Security-Vorfälle für unsere Kunden. Durch unsere hohe Präventionsquote und den Fokus auf ICT & OT Security schaffen wir am Standort Basel ein europaweit führendes Zentrum

für Cyber-Sicherheit im Zeitalter der Industrie 4.0.“
- Stefano Camuso, CEO Axians & Actemium Schweiz

Bereits heute verfügen Axians und Actemium in der Schweiz und in Deutschland über mehr als hundert Cyber-Security-Kunden, darunter diverse Automobilzulieferer, Pharma- und Medizintechnikunternehmen, Verpackungsindustrie, Banken und Versicherungen sowie Energieversorger wie z. B. die E.ON Tochter Avacon. Für viele dieser Kunden stehen die Vergabe von Managed-Security-Verträgen zur Erhöhung ihres Schutzstandards an, welche Axians und Actemium mit ihrem deutsch-, englisch- und französischsprachigem IT & OT SOC Basel gezielt adressieren. Eine besondere Innovation besteht dabei in einer eigenen anonymisierten Security-Datenbank, welche Security-Muster und -Vorfälle sammelt. Damit ermöglichen die Unternehmen durch statistische Analysen und Früherkennung ihren Kunden eine überdurchschnittlich hohe „Threat Intelligence“.
Jacques Diaz, CEO Axians Deutschland ergänzt: „Besonders durch die länderübergreifende Zusammenarbeit unserer Cybersecurity-Teams, die in Basel koordiniert werden, profitieren Kunden von einem der schlagkräftigsten Managed-Security-Angebote im deutschsprachigen Raum. Die Security-Bedrohungen sind zunehmend international und von wachsender Tragweite. Daher werden unsere sehr erfolgreichen Security Operations Center in Hamburg und Ulm je nach Kundenwunsch nahtlos mit dem internationalen SOC Hub Basel zusammenarbeiten. Auch unsere besonderen Stärken im Schutz von Unternehmensnetzwerken und Carrier-Netzen in Deutschland werden zu einem weiteren überproportionalen Wachstum des Managed-Cybersecurity-Geschäfts beitragen.“
Das neue Center wird voraussichtlich ab Ende August 2021 in Betrieb genommen und im dritten Quartal 2021 eröffnet. Aktuell wird neben dem baulichen Fortschritt die Personalbasis für Managed-Cybersecurity-Projekte durch eine Recruiting-Offensive weiter ausgebaut, um den Standort zum führenden Security Operations Center in Europa zu machen. Auf dem Gelände der ehemaligen Elektrizitätsgesellschaft und Lokomotiven-Produktion Alioth entsteht derzeit durch die uptownBasel AG ein neues Innovationszentrum, in dem bis 2027 insgesamt 2000 neue Arbeitsplätze angesiedelt werden sollen. Bereits ab Sommer 2021 werden die ersten 400 Ingenieure erwartet.
„Der Campus steht für die digitale und vernetzte Industrie, die grenzüberschreitend eng verbunden ist. Dass nun VINCI Energies bei uns das Cybersecurity Centrum für die Schweiz baut, und damit die Wirtschaftsabläufe und Verbindungen auf einen Schlag sicherer macht, ist für uns eine große Ehre und erfüllt uns mit Stolz“, sagt Hans-Jörg Fankhauser, verantwortlicher Arealentwickler vom Campus uptownBasel in Arlesheim.
Bei diesem Center handelt es sich um den physischen Standort eines Cyber Security Teams. Das Team übernimmt die Verantwortung für das Monitoring und die Analysen der IT/OT-Systemumgebung der Kunden sowie die Drei-Schichten-Sicherheits-Architektur (Daten, Logik, Präsentation / Frontend). Außerdem erkennt es Cybersecurity-Vorfälle, verhindert diese aktiv oder reagiert darauf. Ein SOC-Team besteht in der Regel aus Security-Analysten, -Technikern, -Managern sowie Industrie-Experten und einem zentralen Eingangspunkt für Kunden. Security-Vorfälle werden von einem kundenspezifischen Response-Team schnell bearbeitet. Ein häufiger Grund für die Auslagerung von SOC-Diensten ist, dass Unternehmen diese seltene Kombination von Spezialkompetenzen selbst nicht vorhalten wollen oder können.