www.iot4industry.at

IoT4 INDUSTRY & BUSINESS

Das Magazin für IoT, Big Data und Security

Erscheinungstermin: 23. November 2023 3|2023

ENGINEERING BASE VON AUCOTEC WIRD ZUM WEGBEREITER FÜR DIE ENERGIEWENDE

Technik & Medien Verlagsges.m.b.H. • Traviatagasse 21-29/8/2, A-1230 Wien • österr. Post AG, GZ 17Z041008 M • € 9,- • Maximale Zustelldauer: 5 Werktage

Smart Parking
EIN PARKPLATZ FÜR UFOS

Im Gespräch
WEDER BITS NOCH BYTES

Im Gespräch
DIE SCHÖNHEIT DER NORM

TECHNIK & MEDIEN VERLAGSGMBH

DIE NEUE HELMPFLICHT

Cybercrime ist gekommen um zu bleiben, davon ist Andreas Willert, Consulting Services bei Pilz Österreich, überzeugt. Daher appelliert er an die Unternehmen ihre Einfallstore nicht sperrangelweit offen stehen zu lassen. Dass es neue Security-Gesetze gibt, liegt für ihn auch an der „Verschieberitis" der Verantwortlichen.

IoT 4 Industry & Business: Welcher Cyberangriff hat Sie am meisten „beeindruckt", weil er entweder besonders dreist, schädigend oder intelligent war?

Andreas Willert: Da erst seit NIS 1 in Europa die Verpflichtung besteht, über solche Angriffe zu berichten, ist das vollständige Ausmaß davor und außerhalb auch der Unionsgrenzen nicht bekannt. Außerdem ist es mitunter schwierig, industrielle Cyberangriffe von technischen Defekten zu unterscheiden. Wer wirbt schon groß und gerne damit, angegriffen worden zu sein. Aber es gibt durchaus öffentlich bekannte Fälle. Stuxnet darf da nicht fehlen, weil er schlicht der prominenteste und erste große Fall eines Cyberangriffs auf industrielle Steuerungssysteme war – zudem bemerkenswert ausgeklügelt und über die Lieferkette übertragen. Dabei wurden in den Jahren 2009 bis 2010 in einer iranischen Urananreicherungsanlage 9.000 von 10.000 Zentrifugen zerstört, was das iranische Atomwaffenprogramm um Jahre zurückgeworfen hat. Dicht gefolgt von Triton. Eine Malware, die 2017 erstmals in einer Chemiefabrik entdeckt wurde, über das lokale Netzwerk eingeschleust wurde und sicherheitsgerichtete Steuerungen zum Ziel hatte. Dann gibt es noch eine Reihe weiterer erfolgreicher Angriffe auf Produktionsunternehmen, wie beispielsweise im Jahr 2022 von Gonjeshke Darande auf ein iranisches Stahlwerk. Cyberangriffe auf industri-

elle Produktionsinfrastrukturen mit kinetic damage als Folge, sind mitunter schwierig zu identifizieren, da sie entweder unwissentlich missverstanden oder bewusst als „technische Fehlfunktion" nach außen kommuniziert werden. Last but definitely not least ist auch der Cyberangriff auf Pilz im Jahr 2019 zu erwähnen. Die Auswirkungen des vollständigen Stillstandes des Unternehmens waren, sowohl intern als auch extern für Kunden und Partner in der davor- und nachliegenden Lieferkette, drastisch. Die Angreifer haben es geschafft uns erheblichen Schaden zuzufügen. Durch die Verweigerung der Lösegeldzahlung und die enge Zusammenarbeit mit den Ermittlungsbehörden konnte das Angreifernetz zerschlagen und weitere Firmen vor demselben Schicksal bewahrt werden.

IoT: Wie groß ist die Gefahr, die von der Supply Chain ausgeht?
Willert: Die Gefahren aus der Lieferkette heraus sind vielschichtig. Der Angriffsvektor ist immens groß und vielfältig. Stuxnet kam über die Lieferkette, SolarWinds ebenfalls. Das Problem betrifft den gesamten Lebenszyklus und reicht von den Maßnahmen im Entwicklungsprozess bis zur Patchbarkeit der Produkte. Ein Kunde von uns sieht es als realistisches Szenario, dass vernetzungsfähige Industriekomponenten im Zulieferprozess unbemerkt so manipuliert werden, dass es zu einem Betriebsunfall kommen kann.

IoT: Demnächst kommen einige neue Sicherheitsvorgaben und Verordnungen auf die Unternehmen zu. Wie behält man da den Überblick?
Willert: Ja das stimmt. Für die Industrie im Allgemeinen und für den Maschinen- und Anlagenbau im Besonderen sind beim Thema Security die EU-Richtlinie NIS 2, die neue Maschinenverordnung und der Cyber Resilience Act relevant. Bislang hat die Maschinenrichtlinie nur das Thema Safety betrachtet, jetzt kommen erstmals Security-Aspekte dazu. Das bedeutet: Die Sicherheitsfunktionen der Maschine dürfen durch unbeabsichtigte oder vorsätzliche Verfälschung nicht beeinträchtigt werden. Der Cyber Resilience Act richtet sich an Hersteller von Produkten mit digitalen Elementen. Damit ist sowohl Hard- als auch Software gemeint. Die Verordnung bezieht sich dabei sowohl auf Consumer-Produkte, als auch auf Produkte für industrielle Anwendungen, wie zum Beispiel Maschinensteuerungen. Laut Cyber Resilience Act dürfen nur noch Produkte in Verkehr gebracht werden, die ein angemessenes Cybersicherheitsniveau gewährleisten. Wenn Security-Bedrohungen eine Auswirkung auf die funktionale Sicherheit haben können, erfordert das eine Risikobeurteilung und ist auch für den CE-Kennzeichnungsprozess relevant. Die NIS 2 hat bei den wesentlichen Einrichtungen neue Bereiche wie die Verwaltung von IKT-Diensten B2B aufgenommen. Komplett neu sind die wichtigen Einrichtungen, unter die auch das verarbeitende bzw. herstellende Gewerbe fällt, also der Maschinenbau, Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, Kraftwagen, Kraftwagenteilen, sonstiger Fahrzeugbau sowie Hersteller von Medizinprodukten. Die Einrichtungen fallen in den Anwendungsbereich, wenn sie mehr als 50 Personen beschäftigen oder über zehn Millionen Euro Jahresumsatz erreichen. Der Schmäh, ein Unternehmen in eine Holding-Struktur mit mehreren Gesellschaften aufzuteilen, um sich dem Wirkbereich zu entziehen, wird übrigens nicht funktionieren.

IoT: Ab wann gilt die NIS 2?
Willert: Sie ist Anfang 2023 in Kraft getreten und muss bis 17. Oktober 2024 von den EU-Mitgliedsstaaten in nationales Recht umgesetzt sein. Das Büro für strategische Netz- und Informationssystemsicherheit („NIS-Büro") des Bundeskanzleramts ist sichtlich bestrebt das mit gesundem Augenmaß zu machen. Also die Richtlinie darf natürlich nicht aufgeweicht werden, aber es ist allen durchaus bewusst, dass man die österreichische Wirtschaft nicht mit strengeren Regeln beschädigen darf.

IoT: Bei Nichteinhaltung drohen den Unternehmen Geldstrafen. Ist das gerechtfertigt?
Willert: Ohne Strafe funktioniert es nicht. Ich kritisiere jedoch Strafen in absoluten Beträgen. Ein Strafmaß in ausschließlicher Relation zum Umsatz bzw. EBITDA fände ich vernünftiger. Wichtiger finde ich es jedoch nicht mit Strafen zu drohen, sondern in erster Linie Unternehmen dabei zu unterstützen, einen gangbaren Weg zu gehen und die Maßnahmen umzusetzen.

»

Andreas Willert
Consulting Services bei Pilz Österreich

„Intrinsisch sind sich einige bewusst, dass sie empfindlich verwundbar sind, aber man prokrastiniert und schiebt das Thema vor sich her. Aber wie bei der Gurt- und Helmpflicht müssen wir zu diesen grundlegenden Schutzmaßnahmen extrinsisch motiviert werden."

Kommendes Jahr bietet Pilz den neuen Experten-Lehrgang „CESA – Certified Expert for Security in Automation" an, der ein zertifiziertes Industrial-Security-Know-how vermitteln wird.

IoT: Warum braucht es überhaupt gesetzliche Maßnahmen? Wissen die Unternehmen nicht selbst, worauf sie aufpassen sollen?
Willert: Intrinsisch sind sich einige bewusst, dass sie empfindlich verwundbar sind, aber man prokrastiniert und schiebt das Thema vor sich her. Aber wie bei der Gurt- und Helmpflicht müssen wir zu diesen grundlegenden Schutzmaßnahmen extrinsisch motiviert werden. Ich vermute, dass die Verbindung der Netzwerktechnik mit der physischen Welt für Nicht-Security-Personen so weit vom Tagesgeschäft entfernt ist, dass für sie das Risiko nicht wirklich nachvollziehbar und greifbar ist. Ich kann verstehen, dass Cybersecurity-Maßnahmen keine Produkte erzeugen und daher nicht ganz oben auf der Agenda stehen. Nur stelle ich mir die Frage, weshalb vor allem Produktionsunternehmen lange Zäune um ihr Grundstück aufstellen und Schlösser in ihren Türen einsetzen, aber die Systeme und deren Ports klaffen in Serversuchmaschinen offen wie Scheunentore. Es geht aber mit Sicherheit nicht darum uns das Leben zu erschweren, sondern unsere Wirtschaft und Produktion auf einem Mindestmaß gegen eine immer größer werdende Bedrohung zu schützen. Zumindest soweit, damit Skriptkiddies und Bots nicht durch das offene Scheunentor hineinstolpern können.

IoT: Für ein betroffenes Unternehmen bedeuten die geforderten Maßnahmen sehr viel Arbeit und auch Fachkenntnis. Gibt es genügend Unterstützung wie Schulungen?
Willert: In den Unternehmen wird es sicherlich einen eigenen Chief Information Security Officer oder eine ähnlich verantwortliche Person geben müssen, die sich mit dem Thema auseinandersetzt. Oder man holt sich über externe Profis die maßgeschneiderte Beratung. Bei Pilz gibt es ab dem ersten Quartal 2024 einen neuen Experten-Lehrgang, den „CESA – Certified Expert for Security in Automation", der ein zertifiziertes Industrial-Security-Know-how vermittelt und sich stark an die IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme" anlehnt.

IoT: Mittlerweile kann man Ransomware-as-a-Service beziehen. Warum kann man so wenig dagegen tun?
Willert: Richtig, es gibt im Darknet verschiedene Anbieter, die ein vollständiges Framework anbieten. Das ist ähnlich wie man Homepages oder Websites erstellen kann, ohne HTML und CSS zu beherrschen. Der Unterschied: Die Anbieter der Ransomware verlangen eine „Umsatzbeteiligung" am Lösegeld. Und nicht jeder Cyberangriff passiert zwangsläufig gezielt. Oft geschieht das aufgrund eines automatisierten Prozesses, der einfach frei zugängliche Dienste oder Server sucht und attackiert. Und zum Thema „Etwas dagegen tun": Es passiert etwas. Das US-Außenministerium hatte für Schlüsselfiguren der berühmten Ransomware-as-a-Service-Gruppe „REvil" ein Kopfgeld in der Höhe von zehn Millionen US-Dollar für Hinweise ausgesetzt. Aber bei diesen Summen sehen wir, in welchen Größendimensionen sich das Thema bewegt. Cybercrime ist komplex, es ist schnell. Phishingseiten sind für wenige Stunden online, ziehen Kundendaten ab und sind dann wieder offline – um woanders wieder aufzutauchen. Es ist ein Wettlauf gegen die Zeit. Zusätzlich kommt die technische Komplexität hinzu, die im steten Wandel ist. Daher die Conclusio für uns: Es wird weder besser noch anders. Die gute Nachricht: Man kann schon mit relativ überschaubaren technischen und organisatorischen Maßnahmen die Barrieren so hoch legen, dass man einen Großteil der Angreifer ausschließt, nämlich die die „zufällig" vorbeischauen.

www.pilz.at