DAS TRANSKRIPT ZUM PODCAST

Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch
Episode 19

Cybersecurity – so hüten Sie Ihren Datenschatz

Immer mehr Geräte und Komponenten im IT/OT-Bereich sind mit dem Internet verbunden. Was höheren Komfort verspricht und sogar ganz neue Business-Modelle ermöglicht, hat aber auch eine Schattenseite. Denn jede Verbindung nach außen stellt immer auch ein potenzielles Einfallstor für Angreifer dar. Ransomware-Forderungen in Millionenhöhe, Sabotage oder das Ausspähen wertvoller Daten können die Folge sein.
Mit welchen Strategien man die Angreifer draußen und teuren Schaden vom Unternehmen fernhält, das diskutieren wir in dieser Episode mit den beiden Siemens Cybersecurity-Spezialisten Christian Goldmann und Stefan Grosser.

Viel Spaß beim Lesen des Transkripts!

Intro [00:00:02] Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch.

Katja Lübcke [00:00:11] Es ist wieder so weit. Herzlich willkommen zu unserer neuen Podcast-Episode. Hier bei Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch, sprechen wir mit Kunden über deren Anwendungen und die entsprechenden Services, die in den Betrieben

genutzt wurden. Immer mal wieder tauschen wir uns auch mit Experten und Expertinnen zu Trendthemen der Industrie aus. In der Vergangenheit waren das zum Beispiel Künstliche Intelligenz, 5G oder zuletzt sogar Quantencomputing. Heute soll es wieder um ein Trendthema gehen. Es geht um Cybersecurity, also ein Thema mit ganz großer Wichtigkeit. Was ist Cybersecurity? Für wen ist Cybersecurity relevant und wie kann man damit am besten im eigenen Betrieb starten? Stefan Grosser und Christian Goldmann sind meine heutigen Gesprächspartner zu dem Thema. Stellt euch gerne einmal selbst vor. Wer seid ihr und was habt ihr überhaupt mit Cybersecurity zu tun?

Christian Goldmann [00:01:00] Mein Name ist Christian Goldmann. Ich bin Gruppenleiter im Bereich Horizontal Cybersecurity und in der Beratung für Cyber-Themen für Industriekunden in Deutschland. Zu meinem Werdegang: Ich bin seit über 22 Jahren bei Siemens. Ich habe ursprünglich im Technical Consulting für Militärkunden begonnen. Daher kommt auch meine Affinität für das Thema Cyber. Und jetzt aktuell bin ich im Industriesektor, um den Industriekunden in Deutschland zu helfen, ihre Cyber Journey entsprechend zu bestreiten.

Stefan Grosser [00:01:28] Ja, hallo Katja, hallo Christian. Mein Name ist Stefan Grosser und ich bin in dem Team von Christian Goldmann. Ich habe den technischen Part inne. Die Basis dafür habe ich mir eigentlich am Ende des Tages schon zu Schulzeiten gelegt. Mein Schülerpraktikum damals war schon bei der Firma Siemens. Und so sollte es dann auch sein, dass ich meine komplette Ausbildung und das Studium auch bei der Siemens AG absolviert habe. Das hat dann dazu geführt, dass ich jetzt mit dem Thema Cybersecurity unterwegs bin. Es ist auf jeden Fall eine spannende Sache.

Katja Lübcke [00:01:56] Ja. Herzlich willkommen nochmal. Schön, dass zwei so alte Siemens Hasen heute dabei sind, wenn man das so sagen darf. Was versteht man denn eigentlich unter Cybersecurity? Und was macht ihr konkret im eigenen Siemens Team für Cybersecurity?

Christian Goldmann [00:02:09] Im Wesentlichen geht es bei Cybersecurity um die Sicherung der Infrastruktur. Sei es die Sicherung der eigenen Büroumgebung oder sensiblen Produktionsnetzen wie im Bereich Pharma oder im Bereich der chemischen Industrie. Im Wesentlichen werden dort Komponenten eingesetzt, die über eine gesicherte Kommunikation alle Netzteilnehmer miteinander verbinden. Wichtig dabei ist, dass bei Cybersecurity alle Komponenten über einen entsprechenden Lebenszyklus eine Systempflege erfahren. Das heißt also, Patches oder Bug Fixes werden bereitgestellt, um dann das vordefinierte Schutzniveau über den gesamten Lebenszyklus der Anlage zu gewährleisten. Wir beraten im ersten Schritt unsere Industriekunden. Das heißt, wir quantisieren über standardisierte Methoden das derzeitige Security Niveau, da viele unserer Kunden schon in der Vergangenheit eigene Security Maßnahmen ergriffen haben. Wichtig ist: Wir bringen das in den gesamten Kontext, messen das und geben dann gezielt Verbesserungspotenzial, um das Schutzniveau in der Zukunft für die Kunden entsprechend weiter zu steigern.

Stefan Grosser [00:03:16] Für diejenigen, die vielleicht mitschreiben: Das ist vielleicht auch so das erste Learning: Der ganzheitlicher Ansatz. Das ist extrem wichtig und das ist auch die Rolle, die wir haben, weil wir ja bei Siemens ganz viele Produkte im Bereich Automatisierung haben. Es ist eben nicht möglich, Security aus einem Produkt heraus zu realisieren. Es bedarf diesen ganzheitlichen Ansatz. Deswegen: wenn man irgendwo startet bei dem Thema - immer von oben nach unten und sich das Thema über alle Systeme anschauen. Das ist wirklich super wichtig.

Katja Lübcke [00:03:44] Wer braucht denn überhaupt Cybersecurity? Oder direkt mal etwas provokant gefragt: Wer kann es sich leisten, darauf zu verzichten?

Christian Goldmann [00:03:51] Also weder Privatpersonen und noch viel weniger natürlich Behörden oder industrielle Betriebe können es sich leisten, das Thema Cybersecurity zu ignorieren oder für sich auf die Seite zu legen. Speziell ist es so, dass es Versorger gibt, die einen öffentlichen Auftrag haben, die die Versorgung der Grundbedürfnisse einer Gesellschaft realisieren. Sei es mit Stromversorgung, Wasserversorgung, Telekommunikation oder auch medizinischer Versorgung. Für diese sind entsprechende Mindestanforderungen zu erfüllen. Diese Mindestanforderungen werden auch von entsprechenden autorisierten Behörden vorgegeben und müssen dann entsprechend umgesetzt werden. Also man kann, egal wo man sich bewegt, das Thema Cybersecurity in der heutigen Zeit weder als Privatperson noch als Anlagenbetreiber ignorieren.

Katja Lübcke [00:04:37] Du hast jetzt gerade schon von Behörden gesprochen. Das heißt, nicht jeder macht Cybersecurity oder setzt Cybersecurity auch freiwillig um, oder? Es gibt schon Vorgaben?

Christian Goldmann [00:04:45] Ja, es gibt seit 2016 in Deutschland das IT-Sicherheitsgesetz, welches 2021 nochmal neu aufgelegt wurde. Das alte Sicherheitsgesetz 2.0, das kritische Infrastrukturbetreiber verpflichtet, Security Profile in der Büroumgebung und auch speziell in der Produktionsumgebung zu berücksichtigen. Und diese Security Profile werden dann auch vom BSI auf Erfüllungsgrad auditiert. Wenn man diesen Anforderungen nicht nachkommt, drohen auch jetzt nach dem IT-Sicherheitsgesetz entsprechende Pönalstrafen. Aber es geht auch weiter. Zum Jahresbeginn wurde die sogenannte NIS 2-Direktive auf EU-Ebene in Kraft gesetzt und es ist damit zu rechnen, dass ungefähr ab 2024 weitere verschärfte Sicherheitsmaßnahmen umgesetzt werden. Das heißt also, die Betreiber müssen sich zum einen auf stärkere Security Maßnahmen einstellen und diese in ihrer Infrastruktur umsetzen. Aber wichtig ist auch, dass in Zukunft zu erwarten ist, dass kleinere und mittlere Unternehmen auch unter die zukünftige Rechtsprechung fallen, sodass auch eine größere Fläche in Zukunft diese Maßnahmen in Deutschland umsetzen muss.

Katja Lübcke [00:06:03] Begegnen euch trotzdem immer noch Aussagen wie: Cybersecurity ist aber teuer und vielleicht bringt es auch gar nichts. Also vielleicht werden da gar keine

Schutzmaßnahmen überwunden. Wie überzeugt ihr eure Kunden dennoch in Cybersecurity zu investieren trotz Vorbehalten?

Stefan Grosser [00:06:22] Ich werde ja nicht flexibler am Ende des Tages, mit ganz vielen Maßnahmen, die ich da einflechte. Auf der anderen Seite schützen sie mich. Und demgegenüber stehen vielleicht hier und da auch Wissenslücken in dem Umfeld der Automatisierungstechnik. Wenn ich jetzt noch nicht in den erlauchten Kreis der KRITIS-Unternehmen dazu zähle, muss ich halt mein Maß an Cybersecurity-Maßnahmen finden. Und da gibt es ganz viele Unternehmen, die sagen: Hey, wir wollen gerne Cybersecurity machen, natürlich aber nicht um jeden Preis. Und das ist am Ende des Tages auch richtig. Es startet auch mit einer Risikoabwägung. Wenn der Betreiber oder die verantwortliche Person oder wer auch immer sagt: Hey, unsere Schutzmaßnahmen sind ausreichend - dann ist das in Ordnung. Unsere Aufgabe ist in jedem Fall immer einen Basisschutz herzustellen. Wir bewerten das Ganze zusammen mit dem Kunden und sagen dann gegebenenfalls doch noch oder weisen darauf hin: Du bist kein KRITIS, aber das, was du jetzt hier machst, ist eigentlich noch nicht ausreichend. Und dann muss man sich genau in diesem Prozess noch mal beim Kunden wiederfinden und schauen, was gegebenenfalls Verbesserungsmöglichkeiten wären. Der Return und Invest, das ist ja jetzt die Ursprungsfrage vielleicht auch gewesen, der lässt sich am Ende des Tages gar nicht so gut berechnen. Im besten Fall habe ich nämlich nie einen Angriff gehabt oder ich habe nie einen Schaden erlitten. Das bedeutet aber, der Return und Invest ist direkt da, weil die Maßnahmen, die ich getroffen habe, gewirkt haben. Aber es wird dann auch immer mal gesagt: Na, ich bin ja eh nicht betroffen. Da kommt schon keiner, der gerade mich als Kleinstunternehmen angreifen will.

Christian Goldmann [00:07:59] Wichtig ist eben, dass wir einen risikobasierten Ansatz favorisieren. Einen absoluten Schutz wird es nicht geben und ein absoluter Schutz wird kaum finanzierbar sein. Und auch ein Dienstleister wird nie die Verantwortung für einen voll umfänglichen Schutz geben. Aber wichtig ist, dass wir uns darauf fokussieren, dem Kunden zu helfen, seine wichtigsten Goldnuggets zu identifizieren. Was sind seine schützenswertesten Elemente in seiner Infrastruktur? Diese Goldnuggets müssen dann über entsprechende Security Controls unter wirtschaftlichen Aspekten geschützt werden, um zum einen die Verfügbarkeit der Produktionsumgebung des Kunden zu schützen und einen drohenden Reputationsschaden in der Öffentlichkeit zu vermeiden. Da helfen wir den Kunden, über entsprechende Assessments auch Grundelemente und einen Grundbasisschutz zu etablieren, damit er wenigstens für sich einen Grundschutz erfährt.

Katja Lübcke [00:08:51] Spielen bei der Risikoabwägung auch schon mögliche Schadenssummen im Falle einer Cyberattacke eine Rolle? Und wie sehen die auch so aus? Was habt ihr da schon erlebt?

Stefan Grosser [00:09:01] Also wir haben da schon relativ viel erlebt. Das ist ja auch das, was am Ende des Tages an schlechter Publicity für die eine oder andere Firma im Rundfunk

mitzuhören und für jedermann sichtbar ist. Es gibt unterschiedliche Szenarien - beispielsweise die Erpressersoftware. Dort hack ich mich in das System eines Kunden ein, lege die Systeme lahm und dann werde ich dort Lösegeld erpressen. Ich versichere diesem Kunden dann natürlich auch, wenn er das Lösegeld zahlt, dass die Systeme wieder freigeschalten werden. In der Realität sieht das natürlich anders aus. Das heißt, wenn der Kunde einmal zahlt, dann zahlt er vielleicht auch das nächste Mal. Man muss immer vorsichtig sein, ob man sich auf solche Sachen einlässt. Eigentlich werden solche Ransomware Vorfälle natürlich eher zentral gemeldet und man soll diese entsprechenden Angreifer eigentlich nicht bezahlen. Aber je nachdem, welches Lösegeld dort eingefordert wird, kann es schon mal locker in die Millionen gehen. Gerade wenn es größere Unternehmen sind, dann sind das Summen, die man dort fordern kann. Auf der anderen Seite gibt es Vorfälle mit Viren, die Systeme per se lahmlegen und dann erst mal nichts mehr geht. Es geht immer auch um die Verfügbarkeit in der Prozessindustrie, in der ich verarbeitende Stoffe habe und Hochtemperaturprozesse, die dann erst mal abkühlen und ewig wieder brauchen, bis sie anlaufen. Dann ist der Schaden schwer messbar, weil er dann direkt mit dem Prozess zusammenhängt. In jedem Fall ist es immer ein massiver Störfall, wenn die Verfügbarkeit im Automatisierungsbereich so gestört wird.

Katja Lübcke [00:10:27] Und du hast jetzt gerade gesagt, dass ein Motiv so etwas wie Erpressung ist. Was wollen Hacker eigentlich noch? Geht es immer nur um Erpressung oder gibt es auch andere Hintergründe?

Stefan Grosser [00:10:37] Die direkten Angreifer, die wollen auf jeden Fall das Beste von den Firmen, die sie erpressen: nämlich deren Geld.

Christian Goldmann [00:10:45] Klar, ich meine, im Bereich Cyberkriminalität hat es verschiedene Phasen gegeben. Heute ist es das Hacking for Money, bei dem man Kundendaten oder Anlagendaten verschlüsselt und dann entsprechende Lösegelder erpresst. Aber im Ursprung hat das alles Anfang der 2000er Jahre ausgehend von individuellen Einzelpersonen angefangen. Stärker getrieben aus einem persönlichen intellektuellen Anspruch hat man erste Würmer oder erste Trojaner programmiert. Aber es darf nicht vergessen werden: auch politische Ziele werden durch entsprechende Cyberattacken umgesetzt. Und natürlich ist einer der prominentesten und einer der komplexesten Hacks in der Vergangenheit das DAX-Net gewesen. Die Manipulation der Zentrifugen. Diese drei Aspekte, also des intellektuellen Anspruchs, aber auch politisch motivierte Ziele und jetzt in der breiten Fläche die Ransomwares, die über erpresserische Methoden versuchen Opfer zu identifizieren, um damit monetäre Vorteile für sich zu erlangen. Diese drei Couleurs unterscheidet man generell.

Katja Lübcke [00:11:50] Wenn jetzt der Firmenrechner als Spambot missbraucht wird, dann kann eben auch eine Konsequenz ein Reputationsschaden sein. Ist das denn wirklich so, dass wir auch als Außenstehende immer etwas davon mitbekommen? Wie wirkt sich so ein Reputationsschaden wirklich aus? Oder ist es überhaupt immer einer? Oder gibt es da vielleicht

sogar Verständnis für, weil man weiß, dass man in der heutigen Welt angreifbarer ist? Wie nehmt ihr das rund um das Thema Reputationsschaden wahr?

Stefan Grosser [00:12:18] Na klar, das spielt natürlich auch eine tragende Rolle. Also das, was du jetzt erzählst, ist eigentlich auch das Thema Informationssicherheit. Da entfernen wir uns so langsam ein bisschen wieder von dem Thema OT Cybersecurity. Das spielt dort auch eine Rolle, klar, aber wir trennen die Bereiche. Das ist der klassische IT-Anwendungsfall. Sie müssen natürlich auch die Office- und Büroumgebungen so schützen, dass die Client Rechner der Mitarbeiter entsprechend von solchen Attacken nicht missbraucht werden. Und klar Reputation, ich hatte es ja schon erzählt: Bei allem, was in der Presse steht und jeder mitbekommt, was bleibt denn bei jedem einzelnen hängen? Die haben ein Problem, die sind unsicher. Vertrauen schürt das nicht. Deswegen ist dort jede Firma, jedes Unternehmen aktuell mit höchster Prio unterwegs und will sich bestmöglich schützen, damit diese fehlende Reputation am Ende nicht auf die eigenen Produkte von den Nutzenden umgemünzt wird. Also das will man vermeiden, auf jeden Fall.

Katja Lübcke [00:13:13] Und was sind die üblichen Knackpunkte beim Thema Cybersecurity? Also welche Präventivmaßnahmen sind aus eurer Sicht Must-haves?

Christian Goldmann [00:13:22] Also wir sehen bis heute, dass bei vielen Kunden nur eine sehr begrenzte Transparenz zu den bestehenden Netzkomponenten besteht. Oft werden diese Produktionsnetze geplant, in Betrieb gesetzt und über einen sehr langen Lebenszyklus betrieben. Anlagenteile werden über den Lebenszyklus ergänzt, modifiziert, manchmal auch stillgelegt oder substituiert. Auch das Mitarbeiterklientel ändert sich. Die Verantwortlichkeiten ändern sich über den Zeitverlauf und viele unserer Kunden haben leider über diesen langen Lebenszyklus keine echte Transparenz über die tatsächlichen Komponenten, die in ihrer Produktionsumgebung stehen. Welche Softwarestände haben wir, welche Versionierungen haben wir? Und das ist eben elementar. Ein Grundbaustein ist ein sauberes Inventory meiner Assets, die in meiner Umgebung stehen. Daraus kann ich dann im nächsten Schritt Grundfunktionen wie das Schwachstellenmanagement ableiten. Das führt mich zum Patchmanagement hin, um dann, wenn Schwachstellen erkannt wurden, diese mit einem Patch zu belegen und die Mitarbeiter dazu anzuhalten, diese Patches möglichst in zeitnahen Fenstern entsprechend der Anlage zu implementieren.

Stefan Grosser [00:14:32] Das unterstreiche ich komplett. Was ich gerne an der Stelle, Christian eigentlich auch immer, voranstelle, ist das Thema Verantwortung und die entsprechenden Rollen, die man innerbetrieblich haben muss. Es muss immer diese verantwortliche Person geben oder die Security Organisation, von denen dann diese Themen, meinetwegen auch in der Reihenfolge, dort getrieben werden. Das bedeutet nämlich auch, dass man es regelmäßig treibt und, dass es kein einmalig abgeschlossener Prozess ist. Cybersecurity ist wiederholend und muss immer wieder ausgeführt werden. Und das geht eben nur mit einer verantwortlichen Person oder Organisation.

Christian Goldmann [00:15:08] Wichtig ist das Verständnis des holistischen Ansatzes. Nämlich der Dreisprung aus technologischen Aspekten zum einen, aber auch den Mitarbeitern, die eine gewisse Awareness haben zum Thema Cybersecurity und die eine Verantwortung in vordefinierten Prozessen haben. Und daher ist eine starke Governance in einem jeden Unternehmen wichtig, um das Thema Cybersecurity ganz einheitlich zu betrachten.

Katja Lübcke [00:15:31] Ihr habt jetzt schon von dem typischen klassischen Fehler gesprochen, dass Patches nicht eingespielt werden. Was gibt es noch für weitere typische klassische Fehler?

Stefan Grosser [00:15:40] Das ist für mich schon einer der wirklich klassischsten. Wenn ich sage, ich muss das Thema permanent treiben, dann ist es eben das, was am Ende des Tages immer wieder hinten runterfällt. Eine Anlage ist in Betrieb, die verdient Geld, die wird abgeschrieben. Alles schön und gut, aber es ist schon so, dass ich das System auch pflegen muss. Ich will ja im Zuge der Digitalisierung auch all die Vorteile der Digitalisierung verwenden. Und die kommen eben mit Vernetzung, mit der Kommunikation in die Cloud, über Edge-Systeme oder Fernwartung. Ich habe automatisch den Anschluss an das Internet und habe dadurch irgendwo ein Einfallstor. Und die ach so tolle Anlage, die echt super funktioniert, ist natürlich nur so viel wert, wie auch immer wieder die bekannten Schwachstellen rausgepatcht werden. Also ich würde das schon als Nummer Eins Fehler setzen. Es ist halt aus organisatorischen Gründen und häufig aus Betreiber- oder Indikatorrolle schwierig, das dauerhaft sicherzustellen, weil die Aufgaben klassischerweise in diesem Unternehmen anders verteilt sind. Es ist auch eine Vorhersage von mir, dass es in Zukunft noch viele, viele andere OT Cybersecurity Rollen und Jobs an der Stelle geben wird, die heute so in der Breite auf jeden Fall noch nicht besetzt sind.

Katja Lübcke [00:16:50] Liegt es vielleicht auch daran: Man will zwar, aber man sieht gar keine Möglichkeit, einen Patch einzuspielen. Wir haben ja ganz viele Betriebe, die wirklich 24/7 laufen, da dürfen die Maschinen nicht stillstehen. Vielleicht ist das auch ein Hintergrund?

Christian Goldmann [00:17:02] Ja, das ist genau richtig. Viele unserer Kunden haben hohe Verfügbarkeitskriterien und können die Patche zwar in ihrer Umgebung bereit halten, vielleicht auch diese Patche entsprechend für die Systemumgebung pretesten, aber das Einbringen der Patche erfolgt in der Regel immer nur bei einem entsprechenden Anlagenstillstand. Hoch verfügbare Kundenanlagen haben in der Regel nur einmal im Jahr einen Retrofit, bei dem dann entsprechend die Patche implementiert werden können. Das geht dann auch oft mit einem Reboot vom jeweiligen Applikationsserver einher. Und damit sind die Anlagen mit dem Zeitpunkt der Schwachstellenpublikation bis der Patch eingebracht wird für diese dedizierte Schwachstelle leider angreifbar. Und das kann eben entsprechend dann auch ausgenutzt werden, ja.

Stefan Grosser [00:17:49] Wobei man aber sagen muss, dass das ja auch eingepreist ist. Also bei solchen Anlagen, die 24/7 laufen, ist es natürlich trotzdem so, dass Schwachstellen bewertet werden. Und wenn man da ein sauberes Security Management System hat, greifen in der Theorie auch interne Prozesse. Das heißt, das Risiko wird abgeschätzt, und wenn die Schwachstelle so eindringlich ist, so bedrohend, dann muss der andauernde Prozess eben beendet werden. Und ich gehe in den Patching-Modus über. Das ist aber noch nicht überall Stand der Technik. Es wird nicht so umgesetzt, wird aber zunehmend so kommen. Eben weil es immer mehr Schwachstellen gibt.

Christian Goldmann [00:18:23] Wichtig ist auch, dass wenn ein Schaden an einer Anlage entstanden ist, ein sauberes Backup and Restore, also Backups, eine Art Lebensversicherung für die Betreiber sind. Das haben einige der Kunden. Aber wichtig ist bei entsprechenden Backups auch, dass das Implementieren der Backups dem holistischen Ansatz folgen muss. Das heißt, es reicht nicht, nur einen entsprechenden Server vorzusehen in der Infrastruktur, in der Automatisierungstechnik. Es müssen eine entsprechende Governance und entsprechende Regelwerke etabliert sein, um Klarheit zu haben welche Produktions- und welche Engineering-Daten archiviert werden, in welchen Zyklen und wo diese Backups entsprechend sauber archiviert werden. Auf dem Campus oder in geografisch getrennten Anlagen, geführt über einen holistischen, ganz einheitlichen Ansatz.

Stefan Grosser [00:19:10] Ich habe es tatsächlich schon erlebt, dass Kunden quasi Backups hatten, also deinem Rat gefolgt sind. Dann waren sie aber in der bedrohlichen Situation, dass sie das Backup wieder einspielen sollten und es gab weder einen Wissenden, wie man dieses Backup wieder einspielt, noch gab es das passende Engineering. Das heißt, ich muss natürlich auch tatsächlich in der Lage sein, mit den Backups umzugehen. Und das fängt schon damit an: Wo liegen die Backups?

Christian Goldmann [00:19:36] Genau, das ist dieser regulatorische Aspekt und das Training und die Awareness, sodass im Anlagenbetrieb, teilweise unter Stresssituationen, dann auch wirklich die Umsetzung klappt. Da hilft nur ein sauberes Training, das wahrscheinlich ein bis zweimal im Jahr in der Regel angesetzt werden sollte.

Katja Lübcke [00:19:52] Gibt es auch einen Trend, dass Cybercrime generell professioneller wird? Also es finden mehr Angriffe statt, aber sind die auch wirklich professioneller?

Stefan Grosser [00:20:01] Leider ja, Katja. Also das Thema Ransomware as a Service ist ein Geschäftsmodell. Also ich kann mir im Darknet oder je nachdem welche Quellen ich da bevorzuge, Schadcode einfach herunterladen. Ich muss nicht mal der eigentliche Urheber sein und diese Dinge wirklich selbst programmiert haben. Ich kann mir das beschaffen gegen Geld. Da geht es ja schon los, das ist ein Geschäftszweig. Und dann habe ich natürlich als derjenige mit der negativen Energie ein entsprechendes Ziel und nutze dann diesen Schadcode, um das auszusteuern. Also hier geht es am Ende um Geld und logischerweise professionalisieren sich

dann auch die ein oder anderen Organisationen, die das entsprechend professionell durchführen. Und auf politischer Ebene ist das natürlich auch heutzutage mehr und mehr ein Instrument, um einen verfeindeten Staat zu schwächen. Funktionieren dort grundsätzliche Themen wie eine Wasserversorgung oder eine Elektrizitätsversorgung nicht mehr, brauche ich keine Waffen. Das geht eben mit den Cyberwaffen, dann sieht es natürlich an der Stelle schon echt schlecht aus für die Versorgung der eigenen Bevölkerung und allem, was dahintersteht.

Katja Lübcke [00:21:04] Ich würde gerne noch mal auf die Patches zurückkommen. Ist es denn auch schon vorgekommen, dass ihr Patches einbauen wolltet, aber gemerkt habt, dass die selbst attackiert worden sind? Die sind selbst nicht sauber, sozusagen?

Christian Goldmann [00:21:16] Im OT-Umfeld ist mir das bisher nicht bewusst. Aber es war in der Tat wirklich schon so, dass zum Beispiel von Microsoft entsprechende WSUS-Server kompromittiert wurden und das Betriebssystemebene, bevor wirklich Patche ausgerollt wurden, praktisch am Verteilerpunkt schon manipuliert wurden und damit in breiter Fläche IT-Infrastrukturen leider mit dem Virenbefall konfrontiert wurden. Das heißt, man hat wirklich einen Schadcode Befall empfangen, indem man geglaubt hat, man zieht sich einen neuen Patch. Wobei halt eben leider der Patch entsprechend kompromittiert war.

Katja Lübcke [00:21:51] Und was ist mit Kunden, die schon angegriffen wurden? Könnt ihr da trotzdem noch helfen? Oder sagt ihr: Ne, jetzt ist es eigentlich zu spät. Wir können eher dabei helfen, dass es nicht noch mal passiert.

Christian Goldmann [00:22:01] Also in der Regel ist es so, wir helfen dem Kunden zum einen, wenn er frühzeitig ein atypisches Systemverhalten erkennt. Dann kann er uns bei der Siemens Hotline kontaktieren und wir schalten entsprechende Experten ein. Das sind sogenannte Instanthandler, die sich dann auf die Anlage remote verbinden, um zum Beispiel die Ausbreitung vom Schadcode einzudämmen und im nächsten Schritt die Triage beginnen. Das heißt, sie versuchen dann das Bereinigen vom Schadcode der Anlage und analysieren auch das methodische Vorgehen: Wie hat der Hack stattgefunden? Sie stellen dann in der Regel eine sogenannte Kill Chain auf. Wie war das methodische Vorgehen? Über welche Schritte hat der Hack stattgefunden? Um dann im nächsten Schritt gemeinsam mit dem Kunden zu erörtern, was zielführende Folgemaßnahmen wären, die man implementieren muss, damit ein solches Angriffsmuster oder ein ähnlich geartetes Angriffsmuster in der Zukunft nicht mehr in der Kundeninfrastruktur umgesetzt werden kann. Also da gibt es entsprechende Hilfestellungen.

Stefan Grosser [00:23:03] Das betrifft ja den Bereich Steuerungstechnik. Die Frage ist, was passiert mit dem, was im Prozess alles defekt ist. Also häufig ist es ja so, gerade in der Prozessindustrie, dass eine Reduktion der Verfügbarkeit oder ein genereller Ausfall, zu einer Verschiebung aller meiner Systeme führt, die da gerade am Laufen sind. Gerade der Hochtemperaturofen mag es nicht, wenn er einfach mal so ausgeknipst wird. Und Fließstoffe, die in Rohren feststecken, die da eigentlich verflüssigt sind, weil sie aktuell eine bestimmte

Temperatur haben. Wenn es dort Änderungen gibt, dann kann das auch mal dazu führen, dass ich am Ende nicht nur über die Wiederherstellung meiner Steuerung rede, meiner SPS, oder mein Netzwerk wieder zum Laufen bringe. Ich rede dann in der Wiederherstellung auch gegebenenfalls über den Austausch von so einem Hochofen. Oder ich muss dort mechanisch Rohre austauschen. Also da hat Siemens dann natürlich ein paar Hürden. Wir sind kein Hochofenlieferant und die passenden Rohre haben wir natürlich auch nicht immer. Unser Einsatzfall ist auf jeden Fall in der Vermittlung und in der Lösungsstrategie für all das, was die OT-Seite anbelangt. Ich wollte einfach nur darauf hinweisen, dass die Schäden, die da teilweise entstehen können, irreversibel sind.

Katja Lübcke [00:24:14] Jetzt ist es ja im besten Fall so, dass Kunden nicht erst auf euch zukommen, wenn schon alles zu spät ist, sondern wenn sie sich proaktiv mit dem Thema Cybersecurity beschäftigen und diesen ganzheitlichen Ansatz umsetzen wollen. Wie läuft denn dann die Abstimmung? Wie geht ihr da vor, wenn jetzt ein Kunde auf euch zukommt und sagt: So Siemens, hilf mir mal beim Thema Cybersecurity?

Christian Goldmann [00:24:34] In der Regel ist unsere Einheit dafür verantwortlich, in zweiter Linie hinter dem operativen Vertrieb die Kunden frühzeitig abzuholen. Das heißt, wir klären die konkreten Kundenanfragen. Oft kommen die zu dedizierten Schwachstellen in Komponenten. Aber wir beraten natürlich auch die Kunden. Wir erstellen Netzkonzepte für verschiedenste Produktionsumgebungen, sei es im Kraftwerk, sei es in der Produktion, sei es in der Lackiererei und positionieren unsere Offerings, um eben ein entsprechendes angepasstes Schutzniveau in der Produktionsanlage sicherzustellen.

Katja Lübcke [00:25:10] Welche Rolle spielt das Thema Verantwortung? Also was ist der Beweggrund eines Kunden, sich für Siemens zu entscheiden, auf Siemens zuzukommen?

Stefan Grosser [00:25:19] Also die Frage ist natürlich für ein Unternehmen wie Siemens, die allein mit der Simatic seit über 65 Jahren quasi am Markt unterwegs sind. Wer, wenn nicht Siemens, ist sich der Verantwortung im Bereich Automatisierungstechnik bewusst? Wir haben jetzt schon eine Reihe an Steuerungsgenerationen bei uns auch hinter uns gelassen. Wir sehen aber auch heute noch im Feld ganz viele Steuerungen, also gerade so eine S5 Steuerung. Die ist da echt noch weit verbreitet und ich glaube, man kauft Siemens das auch einfach ab, dass er beim Thema Automatisierungstechnik der Ansprechpartner ist. Wir haben da ein sehr breites Portfolio. Auch neben unseren Steuerungen, also was den Bereich Antriebstechnik, Visualisierung etc. anbelangt. Und wenn ich an der Stelle über Cybersecurity spreche, dann ist es in der OT super essenziell, dass man sich mit Automatisierungstechnik auskennt. Ich denke, da ist Siemens schon die erste Adresse.

Christian Goldmann [00:26:09] Und darüber hinaus ist natürlich, so wie der Stefan sagt, unsere Kompetenz im Bereich Automatisierungstechnik. Aber wirklich auch über Domänengrenzen hinweg. Sei es jetzt für den Industriebereich oder für die Energieerzeugung,

Energieverteilung oder auch Gebäudeautomatisierung. Also das sind alles kritische Infrastrukturen, in denen wir etablierte Lösungen aufbereiten. Das ist ein Aspekt, und das ist eine unserer Kernkompetenz. Das ist eben das, für das Siemens steht. Aber wichtig ist natürlich auch, dass wir eines der größten Enterprise-Netze sind. Wir müssen eben auch eine sehr hohe Sorge dafür tragen, dass unsere eigene Siemens-Infrastruktur entsprechend geschützt wird. In unserer Büroumgebung und in unseren Siemens-Werken. Und in den Siemens-Werken haben wir fast die gleichen Verfügbarkeitskriterien wie unsere Kunden. Wir sind den gleichen Cyberrisiken ausgesetzt und haben dadurch eben auch die Notwendigkeit, eigene Offerings zum eigenen Schutz zu etablieren. Die reifen bei uns in der internen Anwendung und wenn sie einen gewissen Reifegrad erreicht haben, können wir auch diese Offerings über die Geschäfte draußen in unseren Automatisierungslösungen vermarkten, um dem Kunden den optimalen Schutz ihrer Anlage zu gewährleisten. Also die Automatisierungstechnik als Kernkompetenz gepaart mit Cybersecurity-Erfahrung im inneren Schutz und dann Offerings bereitstellen, die dem Kunden über ihren Lebenszyklus entsprechend helfen. Das ist, sag ich mal, dieses Differenzierungsmerkmal, das wir als Unternehmen entsprechend bieten können.

Katja Lübcke [00:27:40] Und muss die Sicherheit schon in die Hardware eingebaut sein oder reicht das eigentlich auf Softwarebasis?

Stefan Grosser [00:27:46] Also Security by Design ist eigentlich, ich würde sagen, das Must-have, das man heute mitbringen muss. Das heißt, es geht nicht nur über Software. Das Produkt selbst muss schon gewisse Fähigkeiten und Eigenschaften mitbringen, sonst wird es echt schwierig.

Christian Goldmann [00:27:59] Ein Siemens-Produkt oder eine Siemens-Lösung wird nur dann freigegeben, wenn die Security-Mindestanforderungen bei Marktfreigabe hinreichend berücksichtigt wurden. Dann werden auch im späteren Anlagenbetrieb über den Lebenszyklus Security Innovations bereitgestellt und auch entsprechende Systempflege, um aktuellen Angriffsmustern entsprechend zu begegnen.

Katja Lübcke [00:28:21] Und mit Blick in die Zukunft: Was denkt ihr, welche Bedrohungen erwarten uns da noch? Wie bereitet ihr euch darauf vor, sich das entsprechende Know how anzueignen und Ähnliches?

Christian Goldmann [00:28:33] Wir müssen uns bei dem Thema Cybersecurity innovativ einbringen, um auch neue Themen wie die Digitalisierung voranzutreiben. Es ist ein elementarer Baustein, um das Vertrauen der Kunden in unsere Lösungen entsprechend abzusichern und wir müssen dafür Sorge tragen, dass auch unsere Produkte neuen Angriffsmustern und neuen Angriffsszenarien standhalten. Wir verfolgen diese ganzen Trends bis hin zu eigener Cybersecurity-Forschung in enger Zusammenarbeit mit Instituten, mit Universitäten weltweit und richten uns nach neuen Technologien aus, wie beispielsweise Zero

Trust Quantum Kryptographie. Wir versuchen eben diese neuen Ansätze in Form von Prototypen zu entwickeln und dann mit ausgewählten Kunden in die Serienreife zu treiben.

Stefan Grosser [00:29:21] Vielleicht auch von mir noch ein paar zukünftige Bedrohungen, die ich da ein Stück weit auch allgemeiner Natur sehe. Also gerade das Thema Social Attacks und inwiefern so was vielleicht auch ausgenutzt werden kann. Man selbst als Mensch wird ja ein Stück weit immer gläserner hinsichtlich aller Plattformen, die es da so gibt im Social Media Bereich. Also ich meine die Erkenntnisse, die man daraus über Tools ziehen kann. Das wird definitiv auch ausgenutzt werden. Wir sehen jetzt schon verstärkt, dass nicht nur ganz große Organisationen und Firmen angegriffen werden, sondern dass hier auch der Bereich KMU, also kleine und mittelständische Unternehmen, immer mehr in den Beschuss geraten. Also wir haben KRITIS-Unternehmen, die werden natürlich auch heute schon angegriffen. Im Zuge aller politischen Verschiebungen und wer weiß, was da noch so passiert, sind da auch immer mehr Angriffe zu verzeichnen. Aber auch wie gesagt, KMUs und gerade hier ist es eine Bedrohung, wenn ich Wissenslücken habe, wenn ich mich nicht mit dem Thema immer wieder beschäftige. Das ist halt der Punkt. Ich muss mich wirklich hinsetzen. Ich brauche die Verantwortung, muss da eine eigene Organisation schaffen, Wissen aufbauen, lesen, lesen, lesen, sich austauschen mit anderen, einfach am Ball bleiben. Wenn ich das eine Weile nicht gemacht habe, dann werde ich durch irgendwas überholt, was ich einfach noch nicht auf dem Schreibtisch hatte bisher.

Christian Goldmann [00:30:34] Diese KMUs sind mittelständische Unternehmen, Kleinunternehmen, die nicht die Kraft haben, sich entsprechend Cyber-Expertise in den eigenen Reihen vorzuhalten. Und denen können wir natürlich auch dann entsprechende Unterstützung bieten. Sei es in Form von Beratung oder sei es auch in Form von Remote Managed Services. So können wir den Kunden wenigstens ihre Security Ereignisse in ihrer Infrastruktur transparent machen und sie dann auch proaktiv informieren, dass ein Angriff stattgefunden hat, um ihnen dann im Anschluss entsprechende Hilfestellung zu geben. Aber wichtig ist, dass diese KMUs oft nicht die Kraft haben, aber trotzdem sehr hochwertige Patente haben, einen sehr hohen Marktansatz haben, aber mit dem Thema Cyber überfordert werden. Da können wir mit unserer Breite und unserem Wissen entsprechende Hilfestellungen leisten.

Katja Lübcke [00:31:23] Ihr habt jetzt sehr umfänglich betont, dass es wirklich wichtig ist, zuallererst überhaupt ein Bewusstsein für Cybersecurity zu bekommen und auch wahrzunehmen, dass es eben Bedrohungen gibt, die die eigene Produktion beeinträchtigen können. Und wir hoffen, dass wir mit dieser Podcastepisode etwas dazu beitragen können. Danke für eure Erläuterungen, warum Cybersecurity egal bei welcher Betriebsgröße, wichtig ist und wie man auch am besten anfangen kann, egal ob mit oder ohne Hilfe von Siemens. Vielen Dank für eure Zeit.

Stefan Grosser [00:31:52] Ja, danke, Katja, auch für die Einladung. Also wir waren gerne ein Teil der Sendung.

Christian Goldmann [00:31:56] Ja, vielen Dank, Katja, auch von meiner Seite. Es hat uns Spaß gemacht. Das war eine sehr gute Diskussion und hat hoffentlich einige Aspekte zum Thema Cybersecurity für die Kunden und Zuhörer gebracht. Und gerne sind wir auch bereit, in der Zukunft mal wieder ein Update zum Thema Cyber euch und eurer Community bereitzustellen.

Katja Lübcke [00:32:13] Ja, herzlichen Dank! Und für Sie als Zuhörer und Zuhörerin: mitschreiben müssen Sie generell bei unseren Episoden nicht. Sie finden wie immer ein Transkript dieser Episode in unserer Service Digithek. Da besteht auch die Möglichkeit, dass Sie mit unseren Experten und Expertinnen in den Dialog treten. Sie finden den Link, wie Sie da hinkommen, in den Shownotes. Und dann freue ich mich, wenn Sie auch beim nächsten Mal wieder reinhören, wenn es heißt: Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch.

Erfahren Sie mehr:
www.siemens.de/service-digithek