DAS TRANSKRIPT ZUM PODCAST

Einblick. Zweiblick. Weitblick. Episode 25

„Cyberangriff auf den Shopfloor“

Im Zeitalter der Digitalisierung erscheint die Möglichkeit, alles mit allem zu vernetzen, sehr verlockend. Doch leider gerät man damit auch in Reichweite von Cyberkriminellen und kann Opfer existenzgefährdender Ransomware-Angriffe werden. Wie man sich dagegen schützen kann, welche Optionen es für vermeintlich unsichere Anlagen gibt und welche Strategien in der OT-Sicherheit generell sinnvoll sind, das erfahren Sie im Podcast.

Viel Spaß beim Lesen des Transkripts!

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

Katja Lübcke [00:00:11] Herzlich willkommen zurück aus der Winterpause. Ich freue mich, Sie zu einer neuen Episode „Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch“ begrüßen zu dürfen. Mein Name ist Katja Lübcke und ich begleite Sie als Moderatorin durch das heutige Gespräch. Es geht wieder um Security, dieses Mal aber um OT-Security. OT bedeutet, es geht um die Sicherheit auf dem Shopfloor, also die Sicherheit in der Produktion. Was kann man tun, um seinen Shopfloor abzusichern? Diese Frage wollen wir heute beantworten und dafür habe ich zwei Siemens-Experten an Bord. Das sind Florian Schleinkofer und Timo Bunghardt. Schön, dass ihr dabei seid. Stellt euch, wie immer, bitte einmal kurz nacheinander vor. Wer seid ihr, was macht ihr bei Siemens und was habt ihr mit OT-Security zu tun? Florian, starte gern einmal.

Florian Schleinkofer [00:00:55] Ja, Florian Schleinkofer. Ich sitze in Regensburg und bin dort ein Leiter im Service mit einem Fokus auf Digitalisierung und Beratungen für Cyber Security und Umsetzungen für Cyber Security Maßnahmen. Und das hauptsächlich für den süddeutschen Raum.

Timo Bunghardt [00:01:11] Dann würde ich mich direkt anschließen. Mein Name ist Timo Bunghardt. Ich bin OT-Security Spezialist und im Speziellen Experte für Asset Management-Systeme und ich kümmere mich unter anderem auch um die Themen Netzwerksegmentierung, Firewalling, Application Control.

Katja Lübcke [00:01:26] Wunderbar. Jetzt sind schon direkt ein paar Stichworte gefallen. Denen widmen wir uns später. Wir fangen mal mit der Basis an. Warum braucht es überhaupt OT-Security? Was kann im Worst Case passieren und welche Angriffsszenarien gibt es?

Florian Schleinkofer [00:01:40] Im Worst Case-Szenario kann es natürlich passieren, dass die Produktion beim Kunden lahmgelegt wird, dass es dort komplett zu einem Produktionsstillstand kommt, dass womöglich vielleicht sogar Daten verändert werden. Es kann passieren, dass Produkte, die für einen bestimmten Markt bestimmt sind, auf einmal geändert werden, Parameter geändert werden und falsche Produkte auf dem Markt mit landen. Im Nahrungsmittelbereich oder auch im Pharmaziebereich ist es natürlich katastrophal, wenn auf einmal falsche Inhaltsstoffe mit drin sind. Das sind die Worst Case-Szenarien, die im Bereich Cyber Security passieren können.

Katja Lübcke [00:02:13] Welche Rolle spielt dabei denn Ransomware? Beziehungsweise was ist überhaupt Ransomware?

Florian Schleinkofer [00:02:18] Ransomware ist eine Software, die den Computer verschlüsselt. Somit kann dann nichts mehr gemacht werden. Der Computer ist dann in dem Fall gesperrt. Ransomware spielt derzeit eine sehr große Rolle. Das ist, was wir derzeit sehen, eigentlich das größte Einfallstor. Sei es über die IT oder auch direkt in der OT, dass dort ein Ransomware mit zum Einsatz kommt, dass dort Rechner verschlüsselt werden. Teilweise läuft die Verschlüsselung über Wochen hinweg, sodass teilweise auch die Backups mit verschlüsselt sind. Zum Zeitpunkt X schaltet sich die Ransomware dann auf aktiv. Die Rechner werden gesperrt. Es kann dort nichts mehr gemacht werden. Die Produktion steht still und dann werden meistens Lösegeldforderungen oder Forderungen an das Unternehmen gestellt. Erst mit Eingabe eines Codes kann dann überhaupt die Ransomware wieder freigeschalten werden und die Produktion wieder weiterlaufen. Oder man hat vielleicht doch noch ein Backup was nicht verschlüsselt ist und kann es dort an der Stelle wieder mit zurückspielen, damit die Produktion wieder laufen kann.

Katja Lübcke [00:03:19] Und in welchen Dimensionen habt ihr solche Ransomware-Forderungen bis jetzt schon mitbekommen? Wie hoch ist da dann ein potenzieller Schaden?

Florian Schleinkofer [00:03:27] Über die Lösegeldforderungen wird sehr viel geschwiegen. Aber wir haben da schon mitbekommen, dass es ein bisschen abhängig von der Unternehmensgröße ist. Dort sind natürlich keine Scriptkiddies oder sonstiges im Hintergrund. Das sind meistens professionell aufgestellte Organisationen, die im Hintergrund stehen. Die stellen dementsprechend, was das Unternehmen an Geld bezahlen kann, Lösegeldforderungen. Die reichen schon von ein paar 100.000 bis ein paar Millionen. Wobei das natürlich nur ein Punkt ist. Viel größer, was wir so mitbekommen, ist natürlich der Schaden durch Reputation. Ich gelange negativ in die Presse. Ich habe einen Produktionsstillstand. Ich muss womöglich 2000, 3000 Mitarbeiter für paar Wochen nach Hause schicken. Ich kann meine Produkte nicht mehr mit ausliefern. Ich habe vielleicht veränderte Produkte - was noch schlimmer ist - schon längst im Umlauf. Dann habe ich Rückrufaktionen. Das sind eigentlich die größten Schäden, die für ein Unternehmen entstehen können.

Katja Lübcke [00:04:18] Gibt es neben der Ransomware noch andere mögliche Angriffsszenarien, was die OT angeht? Oder ist das wirklich das Kernthema, was die Unternehmen umtreibt?

Florian Schleinkofer [00:04:27] Nein, es gibt da noch viel weitreichendere Angriffsmöglichkeiten natürlich. Das sind zum Beispiel Denial-of-Service-Angriffe, dass einfach ein Netzwerk von Kunden mit geflutet wird, dass da keine Meldungen mehr mit abgesetzt werden können. Es kann passieren, dass Schwachstellen in Geräten mit ausgenutzt werden. Zum Beispiel bei Geräten, die vielleicht nicht 100 % für die IT-Sicherheit ausgelegt sind oder auch etwas ältere Geräte, für die es eventuell keine Patches mehr gibt. Und diese Schwachstellen kann ein Angreifer natürlich auch nutzen und dann dementsprechend die Geräte zum Absturz bringen, Netzwerke fluten. Das sind dann noch weitere Angriffsvektoren, die bestehen.

Katja Lübcke [00:05:04] Und welche Unternehmen sollten sich jetzt angesprochen fühlen, wenn es darum geht, Angriffe zu vermeiden? Sind das eher die großen Konzerne? Sind die Kleinen und Mittelständler aus dem Schneider, weil sie vielleicht nicht im Fokus sind? Wer ist da betroffen?

Florian Schleinkofer [00:05:18] Das sind eigentlich unserer Meinung nach alle Unternehmen, die dort betroffen sind. Also querbeet vom kleinen Büro bis hin zu DAX-Konzernen. Also davon ist eigentlich inzwischen jeder betroffen und es gibt dort keinen bestimmten Fokus auf Kunden, sondern es ist wirklich jeder querbeet potenziell gefährdet.

Katja Lübcke [00:05:36] Und jetzt habt ihr ja selbst schon gesagt, dass es aktuelle Beispiele gibt. Ihr habt schon viel mitbekommen. Gibt es denn auch staatlich regulierte Anforderungen? Oder man muss für sich selbst entscheiden, ob man in die Richtung was unternimmt oder nicht?

Florian Schleinkofer [00:05:51] Es gibt dort eine staatliche Anforderung für die kritische Infrastruktur: Zum Beispiel Wasserversorger, Abwasserversorger, Kraftwerke, teilweise auch

Nahrungsmittelhersteller. Das ist eine kritische Infrastruktur. Dort gibt es derzeit schon staatliche Anforderungen. NIS 2.0 ist dort ein Stichwort. Da ist auch auf der EU-Ebene schon beschlossen worden, dass es hier Regularien geben soll - auch für die einzelnen Bundesländer. Es muss jetzt noch überführt werden von EU-Vorgabe in ein Bundesgesetz. Da wird vermutet, dass 5000 bis 7000 Unternehmen in Deutschland davon wieder betroffen sind und für die wird diese NIS 2-Vorgabe dann gelten.

Katja Lübcke [00:06:31] Gab es denn schon vorher Regularien oder startet das jetzt wirklich erst mit der NIS 2.0?

Florian Schleinkofer [00:06:38] Also es gab jetzt schon Kritische-Infrastruktur-Anforderungen, ansonsten ist es das NIS 2.0. Es ist also auch komplett neu, dass so viele Unternehmen davon betroffen sind und dass jetzt hier etwas mehr gemacht werden muss. Es wird also auf staatlicher Ebene erkannt, dass hier einfach sehr, sehr viele Schwachstellen sind - auch bei den Unternehmen. Und, dass es dort Vorgaben gibt, wie man das Ganze etwas besser machen kann. Und das wird in der NIS 2.0 geregelt werden.

Katja Lübcke [00:07:03] Und wie oft passieren solche Angriffe überhaupt? Wie oft bekommen wir in der Öffentlichkeit auch etwas von solchen Angriffen mit?

Florian Schleinkofer [00:07:10] Es werden zwar Angriffe auf der Seite des BSIs veröffentlicht. Vor allem für die kritische Infrastruktur, die müssen dort auch veröffentlicht werden. Aber die Dunkelziffer - was wir auch im Hintergrund mitbekommen - ist extrem hoch. Und leider werden wir auch fast wöchentlich von Unternehmen kontaktiert, dass wir ihnen helfen sollen, da ihre OT angegriffen wurde und die OT teilweise auch lahmgelegt worden ist. Teilweise war es vielleicht ein Schuss vor den Bug. Aber uns kontaktieren dort wöchentlich Unternehmen, dass wir die OT an der Stelle verbessern sollen, weil es bei ihnen im Unternehmen einen kleinen oder auch einen größeren Vorfall gegeben hat.

Katja Lübcke [00:07:47] Können die betroffenen Unternehmen sagen, wie die Angreifer hinter diesen Angriffen aussehen? Also wie darf man sich die Person vorstellen?

Florian Schleinkofer [00:07:54] Das sind meistens hochprofessionelle Organisationen. Die haben fast schon unternehmerische Strukturen. Und wenn man sich einen Ransomware-Angriff anschaut, ist der meistens nicht zielgerichtet, sondern es werden E-Mails rumgeschickt. Mit KIs werden die E-Mails immer professioneller aufbereitet. Früher kannte man vielleicht eine E-Mail: „Sie haben im Lotto gewonnen. Klicken Sie bitte folgenden Link an“. Inzwischen wird hier immer mehr Bezug auf das Unternehmen genommen und auch teilweise persönlich angesprochen. Das sind dann meistens schon professionelle Organisationen im Hintergrund, die hier massenhaft E-Mails an Unternehmen schicken, in der Hoffnung, dass irgendeiner das schon anklicken wird. Und irgendwo werde ich dann schon einen gewissen Schaden anrichten können, um dann hier ein Geld über Ransomware-Forderungen zu bekommen.

Katja Lübcke [00:08:41] Fühlt ihr bei den Unternehmen schon einen gewissen Druck? Sind die wirklich schon wach geworden in dem Bereich? Ist da ein Eigenantrieb oder braucht es wirklich erst mal die Regularien vom Staat aus, damit die Unternehmen sich damit beschäftigen, was möglicherweise passieren könnte?

Florian Schleinkofer [00:08:57] Unterschiedlich. Einige Unternehmen sind ja wirklich schon darauf vorbereitet. Man redet mit ihnen hier auf einem sehr hohen Level, wo man auch die Absicherungen auf einem relativ hohen Level betreibt. Aber leider gibt es immer noch sehr, sehr, sehr viele Unternehmen, bei denen die Hürde sehr niedrig ist und bei denen es wirklich diese Organisationen sehr einfach haben, einen Schaden mit anzurichten. Also sehe ich es positiv, dass dort in Zukunft die NIS 2.0 auf den Markt kommt und dass hier etwas mehr geregelt wird. Ansonsten ist es auch immer wieder gefährdet, auch für den Wirtschaftsstandort Deutschland, dass immer mehr Unternehmen - auch im Rahmen der Digitalisierung - gehackt werden können und so großer Schaden zugefügt werden kann.

Katja Lübcke [00:09:36] Ist es denn überhaupt realistisch, dass man Systeme so gut absichern kann, dass solche Angriffe wirklich komplett ins Leere laufen?

Florian Schleinkofer [00:09:42] Ich kann nur immer die Hürde sehr hoch legen. Einen hundertprozentigen Schutz habe ich dort leider nicht. Der ist auch nicht zu erreichen. Es ist meistens immer so ein Spielchen. Die IT-Sicherheit, OT-Sicherheit wird hochgezogen. Auf der anderen Seite rüsten natürlich die Hacker auch wieder auf. Einen hundertprozentigen Schutz kann man natürlich niemals garantieren und auch nie erlangen. Ich kann nur die Hürde so hoch legen, dass es dann vielleicht schon wirklich Staaten sein müssen. Absolut höchst professionell, höchst professionell ausgerichtet auf dieses Unternehmen, sodass hier dann überhaupt noch Schaden zugeführt werden kann. Also unterm Strich kann ich nur die Hürde immer so hoch legen, dass ich eine sehr geringe Chance habe, gehackt zu werden.

Katja Lübcke [00:10:21] Ich habe in unserer Einleitung ja schon gesagt, dass wir ja schon eine Episode zu IT-Security haben. Bei der IT ist es ja relativ eindeutig, dass man etwas machen muss, weil die Bedrohungslage hier schon lange bekannt ist. Jetzt ist es bei der OT so, dass es Schwachstellen gibt, weil man denken könnte, dass an die Geräte und Komponenten in der Produktion niemand herankommt. Man ist sich da vielleicht seiner Sache etwas zu sicher. Wie unterscheiden sich denn aber jetzt IT und OT konkret, was die technische Komponente angeht?

Florian Schleinkofer [00:10:49] Die IT ist meistens ein etwas kürzerer Betriebszyklus. Ich habe meistens eher so fünf Jahre alte Geräte im Einsatz. Aber in der OT habe ich durchaus sehr, sehr lange Betriebszyklen. Ich habe dort durchaus mal Geräte, die 20, 30 Jahre oder teilweise noch länger in Betrieb sind. Die Anlagen funktionieren noch super, aber für diese alten Geräte gibt es dann leider teilweise vielleicht keine Patches mehr. Die stellen natürlich schon ein hohes Sicherheitsrisiko mit dar. Sie sind leicht zu hacken, aber dafür gibt es dann andere

Möglichkeiten, um diese alten Geräte doch noch im gewissen Rahmen betreiben zu können und auch sicher betreiben zu können.

Katja Lübcke [00:11:27] Wir haben festgestellt, dass es in der OT, also auf dem Shopfloor, viele PCs bzw. viele PC-ähnliche Systeme gibt. Was braucht man, damit man diese schützen kann? Wie ist der Weg dahin?

Timo Bunghardt [00:11:38] Also wir hatten ja jetzt gerade schon darüber gesprochen, dass wir in der OT natürlich auch teilweise veraltete Systeme haben, die wir aber vielleicht aufgrund proprietärer Software weiterhin betreiben müssen, um die Produktion am Laufen zu halten. Und deswegen ist der erste Schritt, um überhaupt zu registrieren, was wir in unserem Inventar haben, das IT-Asset-Management. Das ist die Aufnahme des Status quo an der Stelle.

Katja Lübcke [00:11:59] Und was genau habe ich dann davon? Also, dass ich wirklich praktisch eine Übersicht habe? Oder kann ich damit noch mehr erfassen als nur, dass ich hier Gerät eins, zwei und drei habe?

Timo Bunghardt [00:12:08] Um die Höhe eines Risikos und die Größe einer Schwachstelle überhaupt beurteilen zu können, brauche ich in erster Linie erstmal Informationen über das Gerät, das mir vorliegt. Und in einigen Fällen sind die Systeme in der Anlage historisch gewachsen. Umfangreiche Informationen über das System zu haben, ist dadurch der Ausgangspunkt, um jegliche weiteren Entscheidungen im Rahmen der IT- und OT-Security treffen zu können.

Katja Lübcke [00:12:30] Welche Infos werden genau zu dem Gerät in diesem IT-Asset-Management aufgenommen?

Timo Bunghardt [00:12:36] Also grundsätzlich fahren wir da schon mit der Devise, dass wir versuchen, möglichst viele Informationen zu erfassen. Es gibt die Möglichkeit, in den Systemen unzählige Auswertungen zu machen und deswegen wollen wir natürlich so viele Datenpunkte wie möglich erheben. Aber um jetzt ein paar wichtige herauszugreifen, sind auf jeden Fall Netzwerkeigenschaften wie die IP-Adresse und die MAC-Adresse wichtig. Dann haben wir auch gerätespezifische Informationen, die wir über unsere Scanning Software auslesen können. Das sind der Firmwarestand, der Hardwarestand, Hersteller, Modellbezeichnung und noch viele weitere Informationen.

Katja Lübcke [00:13:07] Und ist das eine Ist-Erfassung oder erfolgen da auch regelmäßige Updates?

Timo Bunghardt [00:13:12] Beides ist möglich. Es ist natürlich wünschenswert, diesen Stand immer aktuell zu halten. Das heißt zyklisch zu scannen und zu wissen, was in den Systemen oder in der Anlage verbaut ist, ist natürlich der bestmögliche Fall. Wenn wir aber nicht in der Lage sind, in einer speziellen Anlage dauerhaft einen Scan oder einen zyklischen Scan laufen

zu lassen, haben wir in der Vergangenheit auch schon den Weg gewählt, einmalig zu scannen, damit wir alle Geräte einmal aufgenommen haben und die dann in die Security-Betrachtung mit einbeziehen können. Und sollte es noch mal notwendig werden, den Stand zu aktualisieren, muss man das halt noch mal manuell machen.

Florian Schleinkofer [00:13:43] Und es kommt vielleicht auch ein bisschen auf das Unternehmen drauf an, wie häufig dort neue Maschinen umgebaut oder eingebaut werden. Wenn sehr viel Wechsel stattfindet mit Maschinen, ist es natürlich wichtig, einen kontinuierlichen Scan und die kontinuierliche Erfassung an der Stelle zu haben.

Katja Lübcke [00:13:58] Wie genau darf ich mir das vorstellen? Also wie befüllt ihr überhaupt dieses System? Seid ihr dann vor Ort oder könnt ihr das auch irgendwie aus dem Büro heraus bei Siemens machen? Wie funktioniert das?

Timo Bunghardt [00:14:09] Also, wenn wir über Asset-Management-Systeme oder IT-Asset-Management-Systeme sprechen, dann geht es meistens um große Datenmengen und es geht um sehr viele Geräte. Das heißt, die manuelle Erfassung fällt da eigentlich schon raus. Also wir befüllen und pflegen das System, wenn möglich, programmatisch und versuchen so die Informationen zusammenzuhalten in dem System. Es würde schlichtweg zu viel Ressourcen binden, manuell vorzugehen, um die Geräteinformationen zu aktualisieren. Deswegen müssen wir den Ansatz verfolgen, dass wir das automatisch machen. In dem Fall unsere Abteilung lösen wir das bei PROFINET-Systemen mit dem Diagnose-Tool PRONETA. Da können wir dann automatisch zyklische Scans ablaufen lassen und automatisch in das Asset-Management-System speisen.

Katja Lübcke [00:14:49] Du hattest im Vorgespräch von drei Wegen gesprochen, Timo. Also das wäre dann diese Remote Installation mit PRONETA, wenn ich mich jetzt nicht vertue. Wann ist es notwendig, dass ihr vor Ort seid und du praktisch einen Rechner anschließt?

Timo Bunghardt [00:15:02] Grundsätzlich würden wir in der Retrospektive bei den Fällen, in denen wir das hatten, den Fernzugriff lieber wählen, weil das einfach weit weniger Anreisezeit inkludiert. Aber wenn es möglich ist, per Fernzugriff auf die Anlage zu kommen, dann nutzen wir das natürlich. Die Voraussetzung, dass sowas funktioniert, ist natürlich, dass wir einen Zugriff bekommen, der von Kundenseite organisiert und auch abgesichert sein muss. Also wir müssen natürlich auch dafür sorgen, dass, wenn wir darauf zugreifen, wir auch von unseren Systemen aus keine Gefahr mit reinbringen. Meist lösen wir das mit temporären Zugriffen über sogenannte Jump Hosts. Dann kriegen wir entsprechend Freigaben von dem verantwortlichen Personal für die Anlage und haben ein Zeitfenster, in dem wir mit Fernzugriff die Installation von dem Scan-Tool durchführen. Das füttert dann wiederum die Informationen in das Asset-Management-System. Manchmal ist es nicht möglich, per Fernzugriff auf das System zu kommen. Zum Beispiel in vielen Unternehmen, die Teil dieser kritischen Infrastruktur sind. Da ist das öfter der Fall, weil die wollen sich so weit wie möglich abschotten, auch vom Fernzugriff. Dort lösen wir das dann entweder durch eine Vor-Ort-Installation oder einen Scan. Wir

unterscheiden das so, dass wir vor Ort entweder ein Windows-System haben, auf dem wir die Scanning-Software installieren können. Dann sprechen wir von der Vor-Ort-Installation. Oder von dem Vor-Ort-Scan, wenn wir vor Ort kein Windows-System finden und wir deswegen mit einem eigenen Rechner vor Ort den Scan einmalig durchführen.

Katja Lübcke [00:16:24] Okay, verstanden. Und jetzt habt ihr praktisch in einer Produktion via IT-Asset-Management-System alles aufgenommen. Alle Geräte sind dort erfasst. Ihr könnt dann basierend darauf ermitteln, wo Lücken sind. Was passiert dann als nächstes? Werden die Geräte komplett aus dem Netz genommen? Werden da einfach Updates draufgespielt? Was für Lösungsmöglichkeiten gibt es, wenn ihr Sicherheitslücken feststellt?

Timo Bunghardt [00:16:50] Grundsätzlich können sich sehr viele Sicherheitslücken herauskristallisieren. Welche davon aber zuerst behandelt werden, muss man sich im Detail ansehen. Es gibt vielleicht Systeme, die besonders veraltet sind und einen Firmwarestand aufweisen, den man leicht updaten könnte auf eine neuere Version. Weil man aber vor einigen Jahren schon Vorkehrungen getroffen hat und entsprechende Firewall- und Netzwerksegmentierung vorgenommen hat, kann man das Risiko, dass das System betroffen sein könnte, wiederum reduzieren. Also man muss da wirklich individuell in die Risikobetrachtung gehen. In der OT-Welt hat ein einfaches Softwareupdate, das man in der IT-Umgebung vielleicht schnell auf das System spielen könnte, große Auswirkungen. Also da können dann wirklich produktionsrelevante Systeme ihre Funktion ändern, Wechselwirkungen zwischen den Systemen entstehen bis hin zu Produktionsausfällen. Das heißt, man muss im besten Fall die Systeme gruppieren. Also man schaut sich quasi auf Basis des Asset-Management-Systems an, welche Geräte ich zu gleichem Sicherheitsbedarf gruppieren kann. Und dann muss ich mir Maßnahmen überlegen, wie ich dagegen ankomme. Und in vielen Fällen erkennt man vielleicht eine Schwachstelle, kann dann aber nicht zum Beispiel die neueste Firmware aufspielen. Stattdessen muss man andere Wege wählen, wie man das System weiterhin mit diesem Firmwarestand betreibt und dann aber andere Maßnahmen darum baut, um die Sicherheit zu gewährleisten.

Katja Lübcke [00:18:07] Im Vorgespräch ist auch der Begriff Application-Control gefallen. Wie passen denn Application-Control - bzw. erklärt gerne noch einmal, was das ist - und Asset-Management zusammen?

Timo Bunghardt [00:18:17] Application-Control nutzen wir, um zum Beispiel in einer Anlage mit einem veralteten Windows-System, zum Beispiel Windows 7, ein gewisses Sicherheitsniveau gewährleisten zu können. Das bedeutet, wenn in der Anlagenzelle proprietäre Software auf einem Windows 7-System läuft und wir nicht in der Lage sind, auf Windows 10 upzugraden, ohne die Funktion zu verlieren von dieser Software, dann müssen wir uns Lösungen überlegen, wie wir ein Windows 7-System in der Anlage betreiben können, ohne dass wir Sicherheitslücken entstehen lassen. Und die Lösung, die wir dafür parat haben, ist das Application-Control. Application-Control bedeutet, dass wir auf dem veralteten System die Anzahl der ausführbaren Dateien stark einschränken. Und dadurch können wir kontrollieren, dass nichts über das von

uns Erlaubte hinaus ausgeführt werden darf auf diesem System. Das bedeutet, die Software, die wir zwingend brauchen, die können wir erlauben lassen auf dem Gerät. Alle anderen Softwares werden automatisch geblockt. Da reden wir vom sogenannten Whitelisting und das verwalten wir dann zentral auf dem Server. Sollte sich eine Ransomware in einem Netzwerk versuchen auszubreiten, dann kann diese Datei auf diesem System nicht ausgeführt werden und wir stoppen an dieser Stelle die Verbreitung oder auch generell die Angriffsfläche auf dem System. Wie Application-Control und Asset-Management zusammenpassen? An der Stelle würde ich sagen, das Asset-Management ist auch da wiederum der Ausgangspunkt, um entscheiden zu können, welche Systeme ich überhaupt mittels Application-Control absichern kann? Oder gibt es eine Gruppe von Systemen, die ich so zusammenfassen kann, dass man mit Application-Control das Sicherheitsniveau signifikant anheben kann?

Katja Lübcke [00:19:49] Und konkret gesprochen: Welche Voraussetzungen braucht ein System, damit du Whitelisting durchführen kannst?

Timo Bunghardt [00:19:55] Ich würde sagen, auf der einen Seite gibt es die Anforderung, dass wir genug Rechenkapazität auf dem System brauchen. Wobei das mit den Lösungen, die wir einsetzen, ein sehr geringer Anteil des Systems ist, den wir da in Anspruch nehmen. Darüber hinaus brauchen wir zum Aufsetzen des Systems natürlich die Möglichkeit, dass wir die Clients in dem System, auf denen diese Applikationen geblockt werden können, die kommunizieren mit einem Server im Netzwerk, um diese Whitelists abzufragen und so konstant alle erlaubten Applikationen auf dem Rechner zu überwachen.

Florian Schleinkofer [00:20:28] Generell ist zu ergänzen: Application-Control ist eine Lösung für PC-basierte Systeme. Also alles, was auf Windows oder auf Linux an der Stelle mitläuft.

Katja Lübcke [00:20:37] Und welche Maßnahmen zur Risikoreduktion gibt es noch neben dem Application-Whitelisting bzw. gibt es überhaupt noch welche und wenn ja, wie funktionieren die und was ermöglichen die?

Florian Schleinkofer [00:20:48] Es gibt natürlich noch weitere Maßnahmen, die ich mit umsetzen kann. Ein Punkt wäre zum Beispiel eine Netzwerksegmentierung. Also, dass ich einfach mein komplettes Netzwerk, meine komplette Fertigung mit aufteile in kleine Segmente. Wenn vielleicht eins betroffen ist, dann bloß 1/10 meiner Fertigung steht und nicht die gesamte Produktion an der Stelle mit steht. Eine weitere Maßnahme ist natürlich auch die Anomalie-Erkennung. Ich zeichne dort im Passiv kontinuierlich den Netzwerk-Traffic mit auf. Ich analysiere ihn, lasse ihn analysieren über Spezialsoftware, eventuell auch mit einem IT-Spezialisten im Hintergrund und bewerte: Ist das jetzt ein guter Verkehr, hatte ich den schon in der Vergangenheit immer oder versucht hier gerade jemand, ein Hacker, mein Netzwerk mit auszuspionieren, vielleicht schon erste Daten, erste Installationen durchzuführen auf meinen Rechnern? Das erledige ich mit einer Anomalie-Erkennung. Das ist der Fachbegriff dafür. Das sind jetzt zwei weitere Beispiele, um die Maßnahmen zur Risikoreduzierung einzuführen.

Katja Lübcke [00:21:47] Wenn wir mal allgemein an das Thema Digitalisierung denken, dann wird da ja oft gesagt, man muss am besten alles vernetzen. Und Cyber-Security sagt ja eigentlich „möglichst gar nichts vernetzen". Wie passt das zusammen?

Florian Schleinkofer [00:22:00] Ja, das ist richtig. Ich will natürlich einerseits die Vorteile der Digitalisierung nutzen. Ich will dort meine Anlagen in Echtzeit vielleicht sehen. Ich will dort meine Anlagen vielleicht auch aus der Ferne steuern. Ich will dort vielleicht auch Servicetechnikern aufgrund des Fachkräftemangels Fernzugänge geben. Aber das Ganze ist natürlich nur unter dem Kompromiss, dass es auch sicher funktioniert. Also kein Unternehmen wird sagen: „Ich mache die Digitalisierung", wenn es dort an der Stelle unsicher ist. Jedes Unternehmen sagt: „Ich will die Vorteile der Digitalisierung nutzen". Und dann kommt das Aber. Aber es muss natürlich dort auch an der Stelle sicher funktionieren. Und deswegen bekommt dort die Cyber-Security im Rahmen der Digitalisierung immer einen höheren Stellenwert.

Timo Bunghardt [00:22:39] Also, wenn ich dafür sorge, dass ich per Jump Host in meine Anlage reinkomme und ich entsprechende Sicherheitsmaßnahmen getroffen habe, dass nur ich für einen gewissen Zeitraum auf diese Anlage zugreifen kann und mir entsprechende Daten auch nur an meinen User geschickt werden, dann reduziere ich natürlich das Risiko auch trotz vernetzter Anlage. Und ich meine, dadurch, dass die Vernetzung gestiegen ist, hat man ja trotzdem die Möglichkeit, sich sicherheitsrelevante Vorfälle melden zu lassen. Also die Vorteile von der Vernetzung kann man auch im Security-Kontext nutzen.

Katja Lübcke [00:23:07] Was findet ihr denn üblicherweise vor, wenn ihr zum Kunden geht? Ist da die Produktion immer gut abgesichert und ihr macht eigentlich nur noch Kleinigkeiten, also ein Feintuning? Oder kommt ihr oft in eine total chaotische Situation, wo ihr das Gefühl habt „Ach Gott, jetzt müssen wir hier aber mal bei Null anfangen"?

Florian Schleinkofer [00:23:24] Das ist querbeet. Wir kommen teilweise zu Unternehmen, wo man wirklich bei Null anfangen muss und man sich schon fragt: „Wie konnte da in der Vergangenheit nichts passieren oder so wenig passieren"? Aber natürlich kommen wir auch zu Unternehmen, bei denen die Cyber-Security schon einen hohen Stellenwert erreicht hat und man wirklich schon auf einem höheren Niveau diskutiert und man kleines Feintuning an der Stelle noch betreibt. Also querbeet, da ist alles mit dabei.

Katja Lübcke [00:23:49] Wie würdet ihr überhaupt die Bereitschaft der Kunden einschätzen, dann auch etwas zu verändern? Also sind zum Beispiel - wir haben ja über querbeet gesprochen- die Chaos-Kunden auch bereit, alles neu aufzubauen oder anzupassen? Oder sagen da auch manche: „Ach nee, wisst ihr was, das Risiko ist mir nicht groß genug. Ich gehe es mal ein". Und wie beratet ihr die dann?

Florian Schleinkofer [00:24:10] Die meisten Unternehmen sehen dann schon ein, dass hier was gemacht werden muss. Und wir können sie auch überzeugen und über Beispiele

aufzeigen, dass der Standard, den sie derzeit für IT-Sicherheit haben, vielleicht gerade nicht dem Stand der Technik entspricht und dass hier etwas gemacht werden muss. Ansonsten drohen sehr hohe Schäden, wenn ich dort gehackt werde. Leider gibt es natürlich aus meiner Sicht auch ein paar beratungsresistente Unternehmen, die sagen: „Nee, passt schon, ich gehe das Risiko ein". Meine persönliche Meinung dazu ist aber, es sollte hier schon sehr viel gemacht werden. Und es passiert zum Glück derzeit noch so wenig für das, was man draußen wirklich im Feld sieht und wie wenig Maßnahmen hier durchgeführt werden, um die IT-Sicherheit zu erreichen.

Katja Lübcke [00:24:55] Wie viel Uraltsysteme sind denn überhaupt noch in den Shopfloors zu finden? Also sind die wirklich alle schon knapp an ihrer 30-Jahr-Grenze oder haben viele schon auf neuere Geräte umgerüstet?

Florian Schleinkofer [00:25:06] Klar findet man noch Systeme die 30 Jahre oder teilweise noch älter sind, auch S5en in der Produktion. Aber so im Durchschnitt, was wir dort sehen, ist das Alter dort eher bei 15 Jahren. So schätze ich es eher ein, was der Durchschnitt ist, was auf das Alter bezogen an OT-Systemen in der Produktion aufzufinden ist.

Katja Lübcke [00:25:26] Kann sich jemand automatisch sicher fühlen, wenn die alten Geräte einfach komplett gegen neue Geräte ausgetauscht werden?

Timo Bunghardt [00:25:32] Also ich denke, dass der Sicherheitsgedanke in den neueren Systemen schon in der Entwicklung mehr Einzug erhalten hat. Also es ist auf jeden Fall ein wichtigeres Thema geworden. Aber ich denke auch bei neueren Produkten gilt es immer zu beachten: In welchem Rahmen werden die in meiner Anlage eingebunden? Gibt es vielleicht irgendwelche Wechselwirkungen? Zum Beispiel, dass ich durch mein neues Gerät vielleicht einen Zugang nach Außen ermögliche und dann auf einmal Geräte in meiner Anlage im Internet hängen, die ich so eigentlich gar nicht vorgesehen hatte. Also da kann man nicht pauschal sagen, dass da die Sicherheit immer höher ist. Der Gedanke ist da, aber man muss sich auch immer individuell über die Architektur Gedanken machen.

Florian Schleinkofer [00:26:11] Und ich muss auch immer wieder betrachten, dass ich zwar ein neues, super sicheres Gerät haben kann. Wenn ich aber dann einen physischen Zugang zu dem Gerät noch mit ermögliche und Besucher zum Beispiel sehr leicht an die Anlage mit rankommen und hier etwas über den USB-Port mit anstecken können und dann sehr viele Sicherheitsmechanismen aushebeln, die in einem Gerät eingebaut sind, dann bringt auch ein neues tolles Gerät an der Stelle nichts. Ich muss das gesamtheitlich betrachten. Eben vom physischen Zugang: Wie sind die Geräte eingestellt, wie betreue ich sie auch im Nachhinein? Das betreiben wir mit unseren Ansätzen und wir sehen das Thema IT-/OT-Sicherheit an der Stelle nur gesamtheitlich.

Katja Lübcke [00:26:50] Wie geht es weiter? Was erwartet ihr in den nächsten Monaten oder auch Jahren bezüglich der Nachfrage zu so etwas wie Whitelisting oder anderen Lösungsansätzen? Was erwartet ihr aber vielleicht auch in Sachen technischer Entwicklung? Habt ihr da Hoffnungen? Seht ihr Dinge, die vielleicht kommen könnten?

Florian Schleinkofer [00:27:05] Ich sehe da große Weiterentwicklung. Solange die Digitalisierung vorangeht – das Thema ist ja auch ein Megatrend - wird auch die Cyber-Security mit vorangehen. Die Digitalisierung wird nur funktionieren, wenn sie an der Stelle auch sicher ist. Ansonsten werden viele Unternehmen sich der Digitalisierung verweigern. Somit ist dort Cyber-Security ein sehr, sehr großer Punkt und die Entwicklung, auch technischer Natur, wird dort immer weitergehen. Und auch die Hackergruppen werden dort noch aufrüsten. Auf der anderen Seite werden natürlich die Hersteller von Anlagen immer mehr mit aufrüsten, damit man hier immer einen kleinen Schritt voraus ist und ich die Anlagen sicher betreiben kann.

Katja Lübcke [00:27:42] Ja, vielen Dank fürs Mitmachen. Wir haben jetzt ganz viel zu Cyber-Security für OT erfahren. Also auch noch mal eine super Ergänzung zu dem, was wir schon in unserem IT-Security-Podcast aufgenommen haben. Danke, dass ihr dabei wart.

Florian Schleinkofer [00:27:56] Danke auch an die Zuhörer. Vielen Dank, dass Sie zugehört haben. Vielleicht hört oder sieht man sich auch mal neben dem Podcast, um über Cyber-Security zu sprechen. Vielen Dank von meiner Seite.

Timo Bunghardt [00:28:06] Danke auch von meiner Seite, Katja, für die Einladung zum Podcast und für die Möglichkeit, hier über so ein relevantes Thema zu sprechen. Wir hoffen einfach, dass es in der Zukunft immer mehr Awareness dafür gibt, dass man sich vielleicht auch mal vor dem Vorfall über Cyber-Security mehr Gedanken macht. Also bevor im Nachhinein immer mit dem Schaden im Rücken etwas passieren muss.

Katja Lübcke [00:28:24] Ja, wir seitens Podcast wären natürlich auch bereit, dass mal ein Kunde mit uns spricht zu dem Thema Security. Wir können aber natürlich auch verstehen, dass das nicht das Lieblingsthema ist, über das man sich unterhalten möchte, wenn man da leider schon ein Problem hatte. Wie auch immer, weiterführende Infos finden Sie wie immer in unserer Service Digithek. Ich freue mich, wenn Sie auch das nächste Mal wieder zuhören, wenn es heißt: Einblick. Zweiblick. Weitblick. Digitale Services im Gespräch.

Erfahren Sie mehr und melden Sie sich jetzt an: www.siemens.de/service-digithek