

Intro

Hallo und herzlich Willkommen zu einer neuen Folge Canon OnAIR. Let's Talk., dem B2B-Podcast der Canon Deutschland GmbH, moderiert von Heidi Kiser.

Heidi Kiser

Willkommen zu einer neuen Folge von Canon OnAIR. Let's Talk.. Wenn über IT-Sicherheit gesprochen wird, denken die meisten Menschen zunächst an Firewalls, E-Mail-Sicherheit, Cloud-Plattformen und den Schutz von Servern und Arbeitsplätzen. Doch moderne Unternehmens-IT besteht aus deutlich mehr Komponenten.

Viele davon sind vernetzt, verarbeiten Daten und kommunizieren mit anderen Systemen, erhalten aber oft nicht dieselbe Aufmerksamkeit wie klassische IT-Endpunkte. Genau darüber sprechen wir heute. Warum entstehen trotz hoher Investitionen in Cybersecurity immer noch Sicherheitslücken?

Welche Rolle spielen dabei sogenannte blinde Flecken in der IT-Landschaft und weshalb lohnt sich ein genauer Blick auf die Druck- und Dokumenteninfrastruktur? Darüber spreche ich heute mit zwei Experten. Herzlich willkommen Philipp Kalweit von Kalweit ITS und Julian Lucht, Solutions Business Consultant bei Canon. Bitte stellt euch doch erst einmal vor.

Julian Lucht

Ja, ich würde mal den Anfang machen. Also mein Name ist Julian Lucht. Ich bin Solutions Business Consultant bei Canon. Mittlerweile seit 14 Jahren bei Canon tätig und entsprechend die letzten vier Jahre als Solutions Business Consultant. Das heißt in der Beratung der Bestands- und auch potenziellen Neukunden. Und gerade mit dem Schwerpunkt Output Management, Lösungen in der Region Mitte, also alles rund um Frankfurt.

Philipp Kalweit

Hallo Heidi, schön, dass ich da sein darf. Ich bin Philipp Kalweit, ich bin einer der zwei Geschäftsführer bei der Kalweit DTS. Am Ende des Tages sind wir eine unabhängige Unternehmensberatung. Wir machen IT-Sicherheit für Mittelstandsunternehmen, für Konzerne.

Aber das Spannende an unserer Tätigkeit ist, dass wir die Angreifer Perspektive ganz stark berücksichtigen. Einfach aus dem Grund, dass wir die Angreifer sind. Wir versuchen die Infrastruktur unserer Kunden anzugreifen und Schwachstellen zu finden, bevor sie potenziell einen echten Angreifer finden kann.

Heidi Kiser

Ja, das klingt total spannend. Ja, Philipp, IT-Security gehört inzwischen bei fast jedem Unternehmen zu den Top-Themen. Trotzdem lesen wir beinahe täglich von Sicherheitsvorfällen, Datenlacks und erfolgreichen Cyberangriffen. Warum tun sich gerade viele mittelständische Unternehmen so schwer, ihre Sicherheitsstrategie wirklich ganzheitlich umzusetzen?

Philipp Kalweit

Ich glaube, das ist eine sehr vielfältige Frage. Was wir in den Beratungsgesprächen mit unseren Kunden feststellen, ist zum einen, dass die IT, denken wir mal an Anfang der 2000er zurück, auf jeden Fall noch relativ einfach geprägt. Weil ich habe ihn eingestellt, hat die IT gemacht, hat sich um die Firewall gekümmert, den Mail-Server verwaltet, vielleicht gab es noch eine Webseite. Mittlerweile ist das Thema viel komplexer geworden.

Das heißt zum einen, wir haben verschiedene Fachbereiche, verschiedene Fachthemen, wir haben das Thema Cloud, die Firewall sind ein eigenes Thema, wir haben Betriebssysteme. Dafür braucht es spezialisiertes Wissen. Das heißt, dieser allgemeine Generalist, der in der IT so ziemlich alles kann, der wird heutzutage viel, viel seltener.

Was da hinzukommt, ist natürlich, dass wir zunehmende Komplexität in dieser Digitalisierung haben. Das heißt, dass wir eigentlich auch schon gar nicht mehr so viel über die anderen Fachbereiche wissen. Also früher war das so, man konnte noch so ein bisschen erahnen, was macht der andere, was sind da für Themen relevant und vielleicht auch einschätzen, was kann man, was kann man nicht.

Heutzutage ist es glaube ich so, dass wir schon eine ganz starke Dynamik erleben. Vielleicht kommt heute ein neues Thema raus. Wir haben gerade viel mit Large Language Modellen, KI. Nächste Woche ist das Ganze wieder schon disruptiv, hat sich weiter verändert. Das heißt, vollständige Kontrolle solcher wirklich immens komplexen Systeme ist heutzutage kaum noch möglich.

Früher war es vielleicht die digitalisierte E-Mail. Heutzutage sind es viele verschiedene Einzelsysteme. Die liegen teilweise bei Cloud-Anbietern, sind Software-as-a-Service. Die werden von einer Dienstleistungsstrecke in die nächste gebracht. Und ich glaube, das sind Themen, die wir heutzutage in der Komplexität, gerade im Mittelstand, gar nicht mehr erfassen können.

Einen weiteren relativ wichtigen Treiber sehe ich einfach daran, dass es extrem wichtig ist, risikopasiert zu arbeiten. Wenn ich nicht alles beherrschen kann, weil ich ja nicht mehr alles selber betreibe, ist es glaube ich umso wichtiger, auch die Risiken einschätzen zu können. Und was wir häufig in der IT sehen, ist die sogenannte Schatten-IT.

Das heißt, es gibt Systeme, die sind nicht immer unbedingt erfasst. Das sind Systeme, die kennt man vielleicht gar nicht. Und was ich nicht kenne, naja, da muss man ganz klar sagen, das kann ich plund auch gar nicht schützen.

Heidi Kiser

Ja und es wird ja häufig gesagt, die Strategie ist da, an der Umsetzung hapert es. Was bedeutet das dann konkret, Julian?

Julian Lucht

Also wir sehen auch in den Kundengesprächen, dass das Sicherheitsbewusstsein der Kunden wirklich deutlich erhöht ist, auch deutlich gestiegen ist. Teilweise gibt es Budgets bei den Kunden, nur für das Thema Sicherheit, aber wir merken halt einfach auch, dass der Fokus noch einfach auf den klassischen Systemen liegt, also klassisch Server und Clients und dass andere Systeme dann doch eher als Büroausstattung wahrgenommen werden, unter anderem eben auch diese oder unsere Multifunktionssysteme.

Heidi Kiser

Es ist schon spannend. Viele sagen wahrscheinlich, das ist doch nur ein Drucker, aber es ist eben nicht nur der Drucker. Philipp, hast du den Satz auch regelmäßig in deinen Gesprächen?

Philipp Kalweit

Absolut. Also ich glaube, das Kernproblem ist, wenn wir uns einfach mal in so ein Geschäftsführer hineinversetzen, dann muss man natürlich priorisieren, was darf jetzt besonders viel Investitionen bekommen, was nicht. Und ich glaube, in der IT-Sicherheit ist es besonders schwierig, das zu rechtfertigen.

Weil Schutz bedeutet erstmal, es passiert nichts. Das ist, glaube ich, das, was wir alle hoffen. Und das macht es eben so schwer, das am Ende des Tages zu rechtfertigen.

Also Investitionen sind immer schwierig. Wenn wir uns aber auf die Angreiferseite ein bisschen fokussieren und schauen, wie sieht das aus, dann ist mir eigentlich als Angreifer ganz egal, ob ich jetzt einen Client, also ein Notebook, einen Laptop angreife, einen Server oder vielleicht auch den Drucker oder die Alarmanlage. Von daher ist es schon etwas, was wir in einer Organisation, die so einer klassischen Firma, schon als große Herausforderung sehen.

Aber diese Trennung und diese Spezifika, die haben wir als Angreifer eigentlich nicht. Für uns ist jedes System ein potenzieller Eintrittstor, um in das System zu kommen und im Rahmen von der Tool Movement Bewegung immer tiefer ins System einzudringen. Ganz egal, ob es die Alarmanlage, der Drucker oder das Notebook ist.

Heidi Kiser

Das heißt, es geht gar nicht so sehr um das fehlende Sicherheitsbewusstsein, sondern um die konsequente Einbindung aller relevanten Geräte in die Strategie, wenn ich euch beide richtig verstehe.

Philipp Kalweit

Absolut. Es ist ja nicht nur am Ende des Tages einfach ein Drucker, sondern am Ende des Tages ist es wirklich ein Computersystem, mit dem ich genauso viel anstellen kann, potenziell wie mit dem klassischen Notebook. Und das ist, glaube ich, die Gefahr, die wir häufig ein bisschen unterschätzen.

Heidi Kiser

Ja, Julian Canon verwendet ja in der aktuellen Security-Kampagne oft den Begriff Hidden Endpoints. Was genau versteht man denn darunter?

Julian Lucht

Ja, also Hidden Endpoints verstehen wir als Systeme, die entweder gar nicht beobachtet werden oder eben die Beobachtungen oder die nicht diese Beachtung bekommen, die sie bekommen sollten. Philipp hat es ja gerade erwähnt, die Multifunktionssysteme sind heutzutage weit mehr als einfach nur ein System, was einfach nur druckt. Es sind vollwertige Netzwerksgeräte, die eben entsprechend deutlich mehr Aufgaben haben und sind teilweise mit Active Directories verbunden, mit Mail-Servern, mit DNS-Servern, Netzwerkfreigaben etc. pp. Also mit vielen, vielen Netzwerksystemen innerhalb der Kundenumgebung. Und dementsprechend sollten diese Systeme auch so behandelt werden, wie Server oder Clients eben auch die Beachtung bekommen.

Heidi Kiser

Philipp, hast du da ähnliche Erfahrungen?

Philipp Kalweit

Ja, in jedem Fall. Also was wir uns immer ganz häufig ansehen ist, in der Regel, was hat das System eigentlich für Zugriffe? Welche Daten werden verarbeitet? Mit welchen Systemen kommuniziert es? Wer ist dafür verantwortlich? Und gerade bei den Druckern sehen wir, die wichtigsten Sachen werden in der Regel immer ausgedruckt. Ich brauche sie dann vor Ort und da fängt es eigentlich schon an. Ich glaube, Drucker sind in dieser Sicherheitsbetrachtung in der Regel gar nicht so stark im Kernfokus. Und das ist so ein Problem, das wir ehrlicherweise auch bei vielen anderen Unternehmen sehen.

Wenn wir uns anschauen, wie wird ein Unternehmen von solchen Cyberkriminellen eigentlich angegriffen, dann gibt es natürlich die ganz gezielten Angriffe, die wir vielleicht auch kennen aus der Tagesschau, wenn mal wieder ein großes DAX-Unternehmen angegriffen wird. Die viel, viel größere Anzahlunternehmen, die eigentlich angegriffen werden, ist der Mittelstand. 99 Prozent aller umsatzsteuerpflichtigen Unternehmen sind in Deutschland Mittelstand und das Bundeskriminalamt sagt, dass bis zu 600 Angriffe pro Tag auf jedes einzelne dieser Unternehmen stattfindet.

Die logische Konsequenz ist eigentlich ganz klar, die meisten dieser Angriffe sind eben nicht gezielt, sondern finden relativ automatisiert statt. Man kann das ein bisschen vergleichen wie mit so einem Taschendieb. Das ist eine organisierte Gruppe und die versucht in der Regel ein Szenario durchzuführen.

Das ist ganz klar, der Griff in die Hosentasche, um das Portemonnaie vielleicht das Telefon zu entwenden. Und da kann man ganz gut daran ableiten, sie brauchen eigentlich einen großen Raum. Er muss wuselig sein, es muss eine Menschenmenge sein, die dicht an dicht ist und es muss laut und viel Ablenkung muss da sein.

Auf einem Konzert, vielleicht sind wir auf einem Festival, bei einem Stadtfest oder ähnlichem. Und das machen in der Regel Angreifer gezielt im Internet auch. Sie suchen sich eine bestimmte Schwachstelle aus und versuchen sie eben gezielt zu finden.

Das heißt, sie sind auf ein oder zwei bekannte Schwachstellen spezialisiert. Es gibt automatisierte Scanner, mit denen ich das Internet filtern kann. Und wenn ich mal ein Unternehmen finde, das vielleicht potenziell diese Schwachstelle hat, sei es durch ein Findes-Sicherheits-Update oder durch eine bekannte Schwachstelle, die noch nicht mit einem Patch gefixt wurde, sind das durchaus Dinge, die dann das Augenmerk des Angreifers auf einen ziehen.

Und dann werden in der Regel versucht, vollautomatisierte Angriffe zu fahren. Das ist das Verheerende dabei. Dass das einfach eine Masse ist, die man heutzutage gerade im Mittelstand gar nicht mehr so richtig unter den Griff bekommt.

Heidi Kiser

Die Zahl, die du genannt hast, 600 Angriffe täglich, ist natürlich auch enorm. Philipp, hast du ein Beispiel aus der Praxis?

Philipp Kalweit

Ja, auf jeden Fall. Woran ich mich ganz häufig erinnere, das ist jetzt kein spezielles Fallbeispiel. Aber wenn wir uns häufig auch mit dem Thema der ISO 27001, also so Informationsmanagementsysteme befassen, dann ist es ganz häufig so, dass wir versuchen, den Schutzbedarf festzustellen und das heißt ganz konkret, dass wir jedes einzelne Asset versuchen zu identifizieren.

Das kann ein Notebook sein, das kann Docker sein, das kann aber auch der Server sein und was wir in der Regel tun, ist relativ plump zu denken. Das heißt, wenn ich jetzt ein Unternehmen hätte und ein Geschäftsführer frage, was brauche ich denn, um das Unternehmen zu sichern, dann würde der wahrscheinlich sagen, wir haben eine Firewall, wir haben Phishing-Filter, wir haben Antivirenschutz auf unseren Geräten. Was wir machen, ist relativ plumm. Wir schauen uns an, was gibt es überhaupt für Devices, welche Risiken könnten damit einhergehen und versuchen dann technisch oder organisatorische Maßnahmen zu ergreifen, um das Risiko auf einem angemessenen Niveau zu reduzieren. Das heißt nicht, dass wir hundertprozentige Sicherheit herstellen. Das heißt erstmal nur, dass wir einige Risiken akzeptieren, weil sie einfach zu gering sind in der Eintrittswahrscheinlichkeit und vielleicht in der Schadensführung nicht relevant genug, dass man sagt, da lohnt sich die Investition. Was wir aber ganz häufig feststellen ist, dass dieser Schritt schon besonders schwer ist, auch wenn er sehr basic ist, einfach aus dem Grund, dass viele Unternehmen gar nicht wissen: Was betreibe ich eigentlich? Worauf haben sie Zugriff? In welcher Version liegt sie vor? Es gibt ja glaube ich eine Universität, die York University, die hatte glaube ich genau das mal versucht. Die hatten gesagt, wir haben so 10.000 Systeme am Ende und sie waren sehr penibel, sind 25.000 entstanden. Das heißt mehr als das Doppelte und da kann man schon ganz klar sagen, wenn ich als Angreifer eine einzelne Verwundbarkeit finde, mit der ich in ein System komme, dann reicht mir das schon aus. Wenn ich als Unternehmer so jegliche Risiken präventiv minimieren muss, dann sind zehn bekannte und 25 tatsächlich tausende Systeme immer im Netzwerk schon eine unglaublich große Gefahr. Da bringt das beste Virenschutzkonzept nichts, da bringt die beste Firewall nichts. Wenn da Systeme sind, die offensichtlich nicht im Radar sind, können sie auch nicht geschützt werden. Und das ist in der Regel ein Problem, mit dem wir relativ früh auch uns begegnen. Das stellen wir eigentlich in so ziemlich jedem Mittelstandsunternehmen fest.

Heidi Kiser

Aber dein Beispiel zeigt ja auch ganz klar, es ist gar nicht so sehr ein Technologieproblem, sondern hat tatsächlich auch was mit Transparenz zu tun.

Philipp Kalweit

Absolut. Also ganz klar muss man sagen, es geht hier nicht nur darum, dass wir Dinge erkennen, sondern es geht am Ende natürlich auch so ein bisschen um diesen Zielkonflikt, dass wir in der IT versuchen, eine gewisse Verfügbarkeit herzustellen, eine gewisse Usability. Und da gehört es natürlich auch dazu, zu priorisieren. Und eines ist immer ein ganz großes Problem, dass wir gar nicht wissen, wie gefährlich ist eigentlich so ein System, was ist damit potenziell möglich.

Und dadurch eigentlich schon immer sagt, Mensch, wenn wir nicht alles beherrschen können, fokussieren wir uns aufs Wesentliche. Und das weist der Angreifer und nutzt es in der Regel aus, und zwar genau dort, wo wir eben nicht so häufig hinschauen.

Julian Lucht

Genau aus dem Grund nutzen wir eben auch den Begriff Hidden Endpoint. Da hast du ja eben auch erwähnt, Philipp, es gibt eben Suchmaschinen, die darauf spezialisiert sind, das Internet zu scannen nach Geräten, nach IoT-Geräten, nach Servern, Routern oder eben auch Multifunktionssystemen. Und genau das machen wir uns eben auch zunutze.

Wir tun das tatsächlich auch. Als Beispiel nutzen wir da Shodan. Wir greifen auf die Informationen, die Shodan uns gibt, zurück, um eben entsprechend Canonsysteme zu finden, die eventuell frei im Internet verfügbar sind für jedermann.

Versuchen dementsprechend dann die Kunden, die zu diesen Geräten gehören, auch zu ermitteln und auf diese Gefahr hinzuweisen, die da momentan herrscht, die dann im seltensten Fall absichtlich ist. Es war häufig einfach ein System, was nicht beachtet wurde oder eben, wie wir schon gesagt haben, der Begriff Hidden Endpoint, was eben nicht die Beachtung bekommen hat, die es bekommen sollte. Und häufig können wir auch gemeinsam mit dem Kunden entsprechende Maßnahmen vornehmen, sei es Netzwerkanpassungen oder eben auch Gerätehärtung.

Ja, beispielsweise hilft es natürlich auch, die Geräte einfach an ein SIEM-System anzubinden, also ein Security Information und Event Management System, um einfach auch die Sichtbarkeit im Kundennetzwerk und für den Kunden eben auch zu ermöglichen.

Heidi Kiser

Eine Aussage in der Sicherheitskampagne ist ja auch, ihr SIEM sieht alles außer die Geräte, die niemand eingebunden hat. Das ist ja genau das, was ihr gerade auch dargestellt habt.

Philipp Kalweit

Absolut. Ich glaube, die Kernfrage ist einfach nicht, ob das Gerät gefährlich ist, was sich in der Regel die meisten sofort ganz reflexartig stellen würden, sondern die Frage ist eigentlich, habe ich es

überhaupt auf dem Radar? Denn am Ende kann man wirklich nur da schützen, was man auch kennt. Und daher finde ich die Aussage nicht nur passend, sondern ehrlicherweise auch sehr realitätsnah.

Heidi Kiser

Ja, jetzt habt ihr schon ein Praxisbeispiel genannt. Jetzt ist die Frage, welche Muster begegnen euch denn so regelmäßig in der Praxis?

Philipp Kalweit

Erst letzte Woche habe ich mit einer Frau gesprochen, die ein Autohaus betreibt. Das ist ein Autohaus, eine Unternehmensgruppe, die hat mehrere Autohäuser und die hatten vor einigen Jahren, 2022, einen wirklich sehr, sehr krassen Fall. Da ist wirklich etwas passiert, was dieses Unternehmen komplett aus der Bahn geworfen hat.

Und wenn man mich jetzt so fragen würde, Philipp, warum ist jetzt gerade dieses Fallbeispiel so interessant? Weil es einfach nochmal ganz klar zeigt, am Ende des Tages ist es jedes Unternehmen, das da getroffen werden kann. Die haben 100 Jahre existiert und mussten dann tatsächlich Insolvenz anmelden. Da hat eine Mitarbeiterin ganz bitterlich geweint, weil sie sagte, Entschuldigung Frau Bauer, ich bin wahrscheinlich dafür verantwortlich, ich habe auf diese Mail gekriegt, es tut mir leid.

Und die Kernkonsequenz ist, sie haben jetzt neu gegründet und da sie diese Autos in der Regel über Kredite finanzieren, ist es tatsächlich so, dass die Bank ihnen jetzt deutlich schlechtere Kredite gibt. Einfach aus dem Grund, dass sie eben eine relativ kurze Finanzhistorie haben, neues Unternehmen, 100 Jahre Existenz, liegt immer vor einer Bank besser als wenn das jetzt drei Monate existiert. Und mir ist da ein Satz noch in Erinnerung geblieben, den werde ich bis heute nicht vergessen. Sie hat nämlich gesagt, das Schlimmste war eigentlich nicht der Angriff selbst, das Schlimmste war unseren Kunden zu erklären, dass jetzt gar nichts mehr funktioniert.

Die hat gesagt, haben Sie sich schon mal überlegt, was denn passiert, wenn man so ein Autohaus angegriffen wäre? Dann habe ich gesagt, weiß ich nicht, also die Autos stehen dann noch auf dem Parkplatz, so, das kriegt man hin. Da hat sie gesagt, ja das Schlimmste ist einfach, wenn die Leute zum Beispiel in den Winterreifen wieder wollen, die lagern wir für die.

Da habe ich gesagt, ja die sind da auch im Lager, also die sind da jetzt nicht verschlüsselt. Dann sagte er mir, ja kann man, also was soll ein Kunde sagen, wie sieht denn da aus? Dann sagt er, der ist schwarz und rund, mit vier Stück habe ich, also da kommt sie auch nicht mit weiter.

Also sie hatten die banalsten Alltagsprobleme, die konnten die Reifen nicht ausgeben, die wussten nicht mehr, wer hat welches Auto gekauft, sie hat mir erzählt. Da hat eine Frau über eine Bank ihr Auto finanziert und drei Jahre lang dann nicht gezahlt, weil sie hatten ja dann keinen Zugriff auf das Konto. Die konnten diese Zahlung nicht einsehen, haben ihr das Auto natürlich wissentlich gegeben.

Und sie hat dann am Ende behauptet, Mensch, also habe ich jetzt nicht gesehen, dass die Rate nicht von meinem Konto abging. Und das Autohaus konnte das gar nicht feststellen, hat da viel zu spät reagiert. Warum?

Naja, am Ende des Tages war es ein Chip in der Alarmanlage, so zumindest laut Verbauer. Und das ist wirklich so eines der klassischen Fälle, wo man sieht, da wird irgendwas installiert, da kommt ein Servicetechniker, kauft so eine Alarmanlage meistens einmal im Leben, bis sie dann mal wieder kaputt ist. Und dass gerade ausgerechnet das am Ende des Tages dafür zuständig ist, dass ein ganzes Unternehmen um seine Existenz bangen muss, das hätte die Frau Bauer sich auch nicht gedacht.

Also die hätte gesagt, Mensch, im Zweifelses-Notephook, wir klicken nicht mehr auf so viele E-Mails, die komisch aussehen, aber das ist ausgerechnet die Alarmanlage. Damit hätte sie im Leben nicht gerechnet.

Heidi Kiser

Das ist schon ein eindrucksvolles Beispiel. Aber es zeigt auch ganz klar, man investiert in so eine Alarmanlage, die läuft und irgendwie verschwindet sie dann aus dem Bewusstsein. So frei nach dem Motto, das läuft, das habe ich nicht mehr auf dem Schirm, dass das eventuell auch sicherheitsrelevant sein könnte.

Philipp Kalweit

Absolut. Also am Ende des Tages geht das ja mit vielen Geräten so. Das kann die Firewall sein, das Druckersystem, die Überwachungskamera oder auch vielleicht ein Rechner, den man einfach nicht so häufig verwendet.

Die Grundsatzfrage, die ich mir immer stellen würde, ist so ein bisschen, welche Netze sind, welche Systeme sind denn eigentlich mit dem Unternehmenswertzwerg verbunden? Welche davon sind eigentlich wirklich geschäftskritisch? Welche brauche ich? Und wer trägt am Ende die Verantwortung für die Absicherung?

Ist es jetzt bei einer Alarmanlage wirklich der Herr, der es installiert? Sind wir als Betreiber dafür verantwortlich, das Autohaus selbst? Ja, und wie werden scheinbar nebensächliche Systeme eigentlich bewertet?

Also am Ende des Tages ist es so, dass Unternehmen sich schon ganz häufig auf die Fahne schreiben, wenn ich sehe, das Produkt, das ich im Einsatz habe, hat gerade Sicherheitsrisiken, kümmere ich mich darum. Ich sehe das aber häufig eben nicht bei gleichwertigen Systemen wie einer Alarmanlage, einem Drucker oder auch hin und wieder mal banalen Themen wie das Smart Device, das man vielleicht hat, die Türklingel im Mittelstandsbüro, das an der Außenklingel ist und mit der App verbunden ist. All das sind Fragestellungen, wo ich verstehe, dass Unternehmen diese klassischen IT-Systeme häufig nochmal gesondert und intensiver bewerten als gleichrangige und vielleicht genauso geschäftskritische.

Zumindest Systeme wie jetzt eben Alarmanlagen, Drucker und Co., die vielleicht genau die gleichen Berechtigungen im Netzwerk haben wie das Computersystem.

Heidi Kiser

Jetzt begegnen dir in deiner Arbeit bestimmt ganz viele spannende Beispiele. Hast du vielleicht noch ein anderes Beispiel für uns, wo so Muster auch erkennbar werden, die dir immer wieder begegnen?

Philipp Kalweit

Also ein Fall, den ich immer richtig spannend finde, ist ein Fall, den wir auch hier wieder nicht betreut haben, aber von dem ich auch aus den Medien erfahren habe, das ist der Firm Arup. Das ist ein Ingenieurbüro, die sind international tätig. Ich glaube, die sind in über 20 Ländern tätig, die machen riesige Umsätze. Also das ist ein riesiger internationaler Konzern.

Ich glaube, Hauptsitz ist in Großbritannien, in London. Und da hat sich irgendwann mal der CFO aus London bei einem Hongkonger Kollegen gemeldet und gesagt, wir müssen jetzt eine Videokonferenz machen, es ist ein dringlicher Fall. Sie müssen 25 Millionen US-Dollar überweisen.

Und es war ein Videocall, da gab es ein Audio zu, man hat das Gesicht gesehen, die Mitarbeiter haben das überwiesen. Und am Ende des Tages muss man ganz klar sagen, das war ein Deepfake. Also diese Videoinhalte des CFOs, die waren tatsächlich KI generiert, auch der Ton.

Das war kein echter Kollege, das war nicht der echte Chef. Am Ende des Tages ist der Fall nicht aufgefliegen, weil die Überweisung getätigt wurde, sondern weil sich jemand aus dem Hongkonger Büro gemeldet hat in Großbritannien und gesagt hatte, Mensch, das war jetzt eine ganz knappe Situation, wir mussten den Betrag ja dringend überweisen, das wäre ein absoluter Notfall, konnten wir die Gefahr für unser Unternehmen abwenden? Und da sagte der CFO, wer sind sie eigentlich und worum geht es hier eigentlich? Das zeigt ganz gut, auch große Konzerne, die über Kostenstellen verfügen, über Freigabeprozesse für Überweisung, sind auf gezielte Angriffe häufig nicht spezialisiert.

Dann ist klar, ganz oben ist die Frage eigentlich, wer kümmert sich darum, wenn neue Angriffstechnologien wie KI jetzt mittlerweile in Unternehmen Anklang finden und ausprobiert werden, auch diese Methoden festzustellen, die in die Sicherheitsmaßnahmen zu implementieren. Wer ist dafür zuständig, wenn solche Freigabeprozesse passieren und wer trägt dafür die Verantwortung? Natürlich, es gibt für die Freigabe solcher Zahlungen Verantwortlichkeiten, Sicherheitsmechanismen, auch in der IT-Sicherheit, aber gerade Angreifer spezialisieren sich auf das, was wir häufig gar nicht im Blick haben.

Also auch hier wieder, dass das Unternehmen nicht darauf spezialisiert ist, dass solche Autorisierungsmechanismen vielleicht umgangen werden können, wenn es sich um Notfälle handelt, wenn wir durch andere Indikatoren wie sichtbares Bild oder auch den Ton absolutes Vertrauen haben und der Mensch auch da bereit ist zu sagen, es gibt zwar Regeln, das ist eigentlich nicht erlaubt, aber ich kenne die Person, ich sehe sie gerade und ich habe ein absolutes Vertrauen, dass wir in Notfallsituationen auch mal gezielt lösungsorientiert handeln müssen. vielleicht nicht unbedingt so, wie es die Unternehmensvorschrift sagt. Ich glaube, das ist die absolute Gefahr, wenn Sachen passieren, die wir so nicht kennen oder am Ende des Tages, die wir vielleicht gar nicht berücksichtigt haben.

Heidi Kiser

Aber es zeigt erstens, wie die Entwicklung auch voranschreitet, was für Möglichkeiten es mittlerweile auch gibt. Und es zeigt natürlich auch die Herausforderungen, die man da organisatorisch auch als Unternehmen mit solchen Fällen hat.

Philipp Kalweit

Das ist es meistens auch. Also was man ganz klar sagen muss, die Verantwortlichkeit für Cyberrisiken muss über die IT ganz klar hinausgehen. Und auch diese Sicherheitsmaßnahmen, die auch eingeführt werden, müssen am Ende sicherstellen, dass diese Geschäftsmodresse eben auch aktuellen Bedrohungslagen Schritt halten und neuen Technologien.

Und damit ist natürlich ganz klar, dass kritische Prozesse wie Zahlungen, Lieferantenänderungen oder auch vertrauliche Kommunikation regelmäßig auf neue Angriffsmethoden geprüft werden müssen. Also es reicht nicht zu sagen, wir schaffen das jetzt an. Es gibt einen Prozess, der das eben freigibt, sondern es muss auch immer wieder stetig validiert werden, hat der möglicherweise auch Bestand gegenüber neuen Angriffen.

Spreche ich mit Mittelstandsunternehmen und deren Geschäftsführern heißt es häufig, wir sind im Bereich der Prävention, Detektion und im Bereich der Reaktion auf Cyberangriffe gewappnet. Die Frage ist allerdings immer auch auf neue, wie sieht es mit den KI-Risiken aus? Dieses Jahr gab es Fälle, letztes Jahr gab es Fälle, das Thema hatten sie noch nicht berücksichtigt.

Und da wiegt man sich auch immer so ein bisschen in Gefahr, wenn man nur die Sachen schützt, die man kennt und auch immer wieder validiert, funktionieren die noch. Verliert man manchmal den Blick fürs Wesentliche, reicht es eigentlich noch aus? Habe ich Dinge vielleicht vergessen? Denn Betriebsblindheit ist ein unglaubliches, wichtiges Instrument.

Der Förster sieht den Wald von lauter Bäumen manchmal nicht mehr. Von daher ist auch immer wieder die Frage, ist alles so, wie es ist, auch wirklich richtig? Habe ich alles berücksichtigt? Gibt es was, was ich vergessen habe?

Und die Checkliste raus zu uns zu sagen, wir haben da einen Plan und den immer wieder durchzugehen, schützt einen leider nicht vor genau solchen Szenarien. Da ist ein bisschen frischer Wind, der Blick von außen immer mal wieder ganz relevant.

Heidi Kiser

Jetzt haben wir über Unternehmen gesprochen und da Praxisfälle kennengelernt, aber sicherlich spielt auch kritische Infrastruktur oder öffentliche Einrichtungen eine Rolle. Hast du da auch ein Praxisbeispiel, das du uns schildern könntest?

Philipp Kalweit

Absolut. Also was wir persönlich ganz häufig erleben ist, dass wir solche Prozesse wie jetzt bei der Arup auch häufig ganz gut umgehen können, indem wir auch Vertrauen schaffen. Häufig ist es so, dass wir uns auch Social Media anschauen, gibt es da eine Klimaanlage im Büro, dann sehen wir da ein Logo, schreiben dort einen Brief hin und sagen, Mensch, wir haben da einen Wartungstermin.

In der Regel passiert immer Folgendes, die Dame am Empfang sagt, den Brief haben wir bekommen, aber wir haben eigentlich keinen Vertrag mit Ihnen. Also ich kann Sie hier jetzt nicht reinlassen. Der Satz zu sagen, Mensch wissen Sie, vor 15 Jahren hatte ich noch 10 Minuten für so eine Wartung, jetzt sind es 5.

Ich kann Ihnen nicht sagen, was da schiefgelaufen ist. Das hat irgendwer aus Polen aus unserem Callcenter verschickt. Ich kann Ihnen nur sagen, Sie stehen auf meiner Liste.

Ich muss Sie abarbeiten. Sie müssen jetzt einmal bestätigen, dass ich hier nicht rein darf. Ich müssen Sie einmal kurz unterschreiben.

Dann gibt es eine 60 Euro Anfahrsgebühr. Und dann machen Sie einen neuen Termin aus. Aber ich bin jetzt drei Wochen im Urlaub.

Da müssen wir dann schauen, wann es klappt. Da muss ich Sie irgendwo zwischenquetschen. Und dann sieht die Frau sich meistens in einer Situation am Empfang, wo sie sagt, Also da kann ich jetzt quasi gar nicht anders reagieren.

Ich möchte nicht verantwortlich sein, dass das jetzt nicht geklappt hat. Ich lasse den Herrn rein. Und das sehen wir in anderen Situationen auch ganz häufig.

Also ein Fall, den ich aus den Medien auch kenne, ist dieser Alaska-Gipfel. Das war ein relativ wichtiges Thema. Ich glaube, da hat sich Donald Trump mit Vladimir Putin 2025 getroffen.

Und in einem Hotel hat man dann tatsächlich in so einem Drucker, in dem Hotel Drucker Unterlagen gefunden, die für dieses wichtige Gespräch als Vorbereitung dienten. Und auch da wieder muss man sagen, da ist die Person wieder kreativ geworden. Ich habe meistens meinen eigenen Drucker nicht dabei.

hey, sitze irgendwo im Ausland, wir brauchen physische Notizen. Und dann ist natürlich klar, dass ich die Infrastruktur vor Ort nutze. In dem Fall war es nur leider so, die Dokumente lagen dann noch drin.

Es war ein wichtiges Meeting, hat man nicht geschafft, es abzuholen. Vielleicht hat man den Ausdruck vergessen. Und so war am Ende des Tages für jedermann verfügbar.

Und das kann man eigentlich auch ganz gut auf Unternehmen übertragen. Also jeden Tag versuchen wir vertrauliche Dokumente über unseren SharePoint zu schmeißen. Wir schicken E-Mails hin und her und hin und wieder scannen wir auch mal Dokumente ein, von Behörden, die wichtig sind, wichtige Verträge, wir haben Ablagen, wir nutzen Drucker, wir scannen Dinge ein.

Und am Ende des Tages ist die Frage eigentlich gar nicht, wie können wir noch besser werden, sondern wie können wir Dinge, die wir eigentlich täglich übersehen, tatsächlich auch mal absichern und das als möglichen Eintrittstor auch möglicherweise verhindern. Denn Dokumentenprozesse, die nicht sicher sind, helfen eben am Ende des Tages auch nicht, wenn ein Angreifer reinkommen will, ob die Firewall geschützt ist oder der Ausdruck im Drucker liegt. ich nehme immer das verwundbarste Glied der Kette und wenn es der Drucker ist, dann ist das am Ende ein Entrypoint, den ich auch wirklich sehr gerne nutze.

Heidi Kiser

Absolut.

Julian Lucht

Ja, also es ist wirklich ein gutes Beispiel, was du gemacht hast mit dem Alaska Summit. Das hatte ich auch gelesen in den Nachrichten und ich habe mich doch auch schwer gewundert, weil eigentlich heutzutage doch Output-Management-Lösungen eigentlich sehr verbreitet sind und solche Vorfälle dementsprechend gar nicht mehr passieren müssten eigentlich. Also wer sich damit noch nicht beschäftigt hat, kann ich wirklich nur sehr empfehlen, spätestens jetzt zu tun. Also solche Vorfälle müssen eigentlich nicht mehr passieren. Es ist sehr einfach handhabbar, dass Druckaufträge entsprechend erst ausgelöst werden und ausgegeben werden, wenn der User vor dem Gerät steht und dementsprechend den Druckauftrag dann auch entgegennimmt und mitnimmt und nicht liegen lassen kann. Also da muss schon sehr viel dann passieren, damit man dann noch abgelenkt wird, um die Druckaufträge zu vergessen. Da gibt es wirklich ganz einfache Methoden, wie man sich dann authentifizieren kann am System, sei es per Karte, Smartphone oder zumindest mal über einen PIN, um zumindest mal datenschutzrelevante Aufträge auch abzusichern, so wie es jetzt in dem Fallbeispiel auch war. Und selbst auch für Gäste, wie jetzt in dem Beispiel auch, auch dafür gibt es entsprechende Lösungen.

Also auch das kann kein Grund sein, weshalb so ein Vorfall passieren könnte.

Philipp Kalweit

Absolut. Ich glaube, da geht ja für Drucksysteme das Gleiche wie für andere Systeme. Welche Informationen sind eigentlich sensibel? Es gibt eine Dokumentenklassifizierung. Ich Druckfreigabe, wie du schon sagst. Ich kann pin-geschützten Druck nutzen. Am Ende des Tages sind es für uns einfach viele Eintrittsmöglichkeiten. Wo entstehen, wo liegen diese Informationen?

Bei einem Drucker sind sie eigentlich immer gebündelt. Ich kann sie ganz gut nutzen. Wer darf in der Regel darauf zugreifen? Also das sind so Themen, womit ich mich als Angreifer eigentlich immer ganz gerne beschäftige. Denn auch so ein Drucker hat sowohl die Geschäftsführung Zugriff als auch der Systemadministrator und die Dame am Empfang. Wenn ich es drauf anlege, ist das eigentlich ein wirklich schöner Entrypoint. Es kann einfach sein, dass ich mir physisch den Ausdruck aus der Auslage nehme oder den Loka einfach technisch versuche anzugreifen.

Denn er muss ja aus jedem System heraus erreichbar sein. Und das ist am Ende des Tages ein schöner Entrypoint für uns, um auch sowohl technisch als auch analog in solche Unternehmen hereinzukommen.

Heidi Kiser

Ja, wenn ich das jetzt zusammenfasse, was ihr gesagt habt, dann geht es eben nicht mehr nur um Sicherheit, sondern es geht tatsächlich um Widerstandsfähigkeit und Resilienz.

Philipp Kalweit

Absolut. Ich glaube, Resilienz ist so ein bisschen das Kernthema. Wenn wir uns zurück überlegen, wie kommen eigentlich Angriffe ins Unternehmen, sind das meistens von Automatisierten.

Das heißt, diese Gruppen sind ja auf ein oder zwei Angriffe spezialisiert. Und das kann man eigentlich ganz gut mit so einem Effekt oder mit einem Spruch oder mit so einem kleinen Gimmick ganz gut gleichsetzen. Ich sage immer Milch, Milch, Milch. Was trinkt die Kuh? Die meisten würden jetzt Wasser sagen.

Das ist auch richtig, aber es gibt natürlich auch den Hang dazu zu sagen Milch. Einfach weil ich Milch, Milch, Milch so häufig wiederholt habe. Und das sagt eigentlich ganz gut, wie der Mensch eigentlich so tickt.

Ich kann so ein bisschen prognostizieren, was er sagen wird, was vielleicht nicht. Und da gibt es ganz viele spannende Effekte, die man nutzen kann. Der Mensch ist gerne hilfsbereit, der ist nicht so konfliktfreudig. Das sind alles Themen, die Angreifer gezielt nutzen, um eine Situation herzustellen, wo wir eben auch solche Mechanismen zurückgreifen, wo ich dann am Ende auch wirklich weiß, da wird die Person so handeln.

Wenn wir am Ende des Tages aber auch über direkte Cyber-Angriffe sprechen, die digital funktionieren und nicht immer so physisch oder über Social Engineering, dann ist so ein ganz großes Problem Ransom. Also Angreifer verschlüsseln häufig einfach sofort, nicht sofort die Systeme, sondern sind eben unbemerkt für längere Zeit im Netzwerk. Also meine Statistik, die ist ein bisschen veraltet, sagt bis zu 42 Tage, in der Daten exfiltrieren kann, also sich herunterladen kann, da kann dann eben eine Erpressung vornehmen.

Das Kernthema ist quasi, dass man bei Ransomware-Angriffen denkt, Mensch, wenn die Systeme verschlüsselt sind, habe ich ja Backups. Aber es fängt eben viel früher an, dass die Unternehmen eben eigentlich das Problem haben, dass der Angreifer eine viel höhere Verweildauer hat. Und die Statistik, meine ich, ist ein bisschen veraltet, sagt bis zu 42 Tage, wo der Angreifer eben Daten entwenden kann, exfiltrieren kann und damit möglicherweise auch eine Erpressung vornimmt.

Das heißt, wenn eben keine Lösegeldforderung gezahlt wird, um diese Daten wiederzubekommen, dann landen sie manchmal im Internet. Und da sind Backups, wie gesagt, einfach nicht automatisch die Rettung, sondern es ist auch so ein bisschen die Frage, sind die vollständig, sind sie aktuell, können wir eine Wiederherstellung stattfinden lassen? Wie lange dauert so eine Wiederherstellung? Und naja, die eigentliche Krise beginnt quasi erst nach dem Angriff und nicht mit dem Angriff, denn die Frage ist eigentlich so ein bisschen, wie weit ist der Angreifer reingekommen? Wie weit ist er vorgedrungen? Was hat er alles entwendet? Und da fangen auch wieder diese Kompromisse an.

Also die IT selbst hat eben nicht in der Regel das Interesse, so schnell wie möglich den Wiederanlauf zu starten. Was wir in der Praxis ganz häufig sehen, ist, dass sie quasi versuchen mit eigener Sicherheitssoftware diese Malware, diese Schadsoftware zu erkennen und selber zu bereinigen und dann feststellen, Mensch, das System ist ja deutlich stärker infiziert als wir dachten. Das ist ein relativ großer Fall. Das sollten wir vielleicht doch mal sauber aufarbeiten, um zu schauen, sind vielleicht wichtige Daten entwendet worden.

So wie der Angreifer vielleicht über eine Lösegeldforderung behauptet. Und wenn das passiert, kommen wir als Forensiker und stellen dann fest, forensische Beweise sind durch diese Bereinigung manchmal schon verschwunden. Das heißt, ich habe gar keine Möglichkeit mehr festzustellen, sind da überhaupt Daten entwendet worden, ist das alles nur ein Bluff? Das sehen wir auch ganz häufig bei anderen Herausforderungen.

Also häufig ist es so, dass wenn wir eine Forensik durchführen wollen, es ist ein Notebook von einem Mitarbeiter, das sich zum Beispiel die Frage stellt, dürfen wir überhaupt Forensik betreiben, wenn das privat in gewissen Anteilen genutzt werden dürfte, das dienstliche Gerät. Da kann es zumindest nach meinem Kenntnisstand sein, dass der Mitarbeiter das verweigern kann. Und das sind dann zum Beispiel Dinge, wo man sagt, naja, also wenn er dafür zuständig ist und das vielleicht auch der Grund war, warum wir jetzt infiziert sind, weil er da Privatgas gesurft hat, dann wäre die erste Reaktion eigentlich Schadensbegrenzung. Ich gebe keinen Zugriff darauf. Das zeigt ganz gut, Unternehmen müssen sich schon vorab darüber Gedanken machen. Wie kann ich Systeme schützen? Was passiert

bei einem Angriff? Welche Dinge muss ich vielleicht präventiv machen, weil sie später als Reaktion gar nicht mehr nützlich sind?

Und da fängt es eigentlich bei solchen kleinen Fragestellungen an. Resilienz beginnt nicht mit den Kernfragen, welche Systeme müssen geschützt werden, sondern was passiert nach einem Angriff, was passiert vor einem Angriff. Wir gehen heutzutage nämlich nicht mehr davon aus, dass wir Systeme hundertprozentig schützen können, sondern wie wichtig ist eigentlich die Frage, was passiert, wenn es dann doch ausnahmsweise mal passiert, zum Beispiel, weil Systeme angegriffen werden, die gar nicht in unserer Verwaltung liegen, Software as a Service, Drittanbieterlösung, Cloud-Systeme etc., wie wir dann damit quasi umgehen.

Wie weit kommt der Angreifer rein, wie weit eben nicht. Was für Maßnahmen treffen wir, dass er vielleicht, wie bei einem physischen Einbruch ins Haus, nicht nur durch die Balkontür reinkommt und dann im Wohnzimmer ist und ins Schlafzimmer kann, sondern wir auch mal ein paar Zimmer abschließen, dass er vielleicht dann nur noch ins Gäste-WC darf und vielleicht dann doch nicht mehr ins Schlafzimmer. Das sind Fragestellungen, die heutzutage aus meiner Sicht besonders relevant sind.

Informationssicherheit ist nämlich auch eine Führungssache, nicht eine reine IT-Geschichte. Das heißt, Geschäftsführer müssen am Ende eben gar nicht verstehen, welche dieser Systeme müssen geschützt werden, aber die Risikosteuerung eben auch verantworten. Das heißt, sie legieren, selbst entscheiden. Denn IT, wie wir eben gerade festgestellt haben, heißt nicht immer Informationssicherheit. Das eine ist der Betrieb, das andere ist Kontrolle, Risikobewertung. Das ist so ein natürlicher Interessenskonflikt, von daher ist auch hier eine Trennung notwendig. Ich würde empfehlen, Cyberrisiken sind immer Unternehmensrisiken und gehören damit in die Unternehmenssteuerung und nicht ausschließlich nur in die IT. Und damit ist die Frage nicht, muss jeder Geschäftsführer jede Technologie verstehen? Muss er sich um sondern nein, er muss die Risiken wirksam steuern, unabhängig bewerten und auch eben angemessen handeln.

Und das gilt eben auch für Systeme, die er vielleicht gar nicht auf dem Schirm hat oder die gar nicht in seinem Verantwortungsbereich liegen.

Heidi Kiser

Jetzt sprechen wir heute über IT-Sicherheit. Julian, viele Menschen verbinden, Canon ja erstmal mit Druckern und Multifunktionssystemen. Welche Rolle spielt denn Canon bei Sicherheitsfragestellungen?

Julian Lucht

Also für uns ist erstmal natürlich wichtig herauszufinden, was den Kunden aktuell beschäftigt. Welche Systeme hat der Kunde im Einsatz, welche Prozesse und natürlich auch welche Risiken dann da entsprechend hinterstecken, weil es ganz klar, es gibt nicht den einen Kunden und es gibt auch nicht die eine Lösung. Das muss immer individuell betrachtet werden, von Kunde zu Kunde, weil einfach jeder Kunde individuelle Anforderungen und Vorgaben hat, die er entsprechend erfüllen muss.

Heidi Kiser

Und welche Rolle spielt in dem Zusammenhang auch das IT-Kompetenzcenter von Canon in Dresden?

Julian Lucht

Also wir haben da einen großen Vorteil durch das ITCC, also das IT-Kompetenzcenter. Das ist quasi unser internes IT-Systemhaus für Kunden. Über das ITCC können wir entsprechend unser Kernportfolio noch erweitern, indem wir eben entsprechend nicht nur Systeme und unsere Software anbieten, sondern auch beispielsweise die Hardware für unsere Softwarekomponenten bereitstellen können.

Also als Beispiel mal Server, um das ein Beispiel zu nennen. Wir können über das ITCC eben auch Endpoint Security oder Firewalls anbieten. Also alles, was über die reine Gerätesicherheit hinausgeht, um das Netzwerk des Kunden abzusichern.

Aber natürlich bieten wir darüber auch Beratungsleistungen, Implementierungsleistungen oder generelle Operational Services an. Ein bisschen tatsächlich sogar auch zu Pentest selber, die wir über das ITCC entsprechend abbilden können, um Kunden wirklich ganzheitlich betreuen zu können. Vielleicht ist einigen der Begriff Managed Print Service in dem Bezug auch bekannt.

Also darüber können wir wirklich Kunden dann ganzheitlich abbilden.

Heidi Kiser

Das heißt, es beginnt ganz oft bei einem Drucker oder Multifunktionssystem und endet aber bei einer viel größeren Fragestellung.

Julian Lucht

Ja, es geht eigentlich nie nur um den Drucker oder das Multifunktionssystem. Es geht darum, dem Kunden eine effiziente und sichere Arbeitsumgebung zu schaffen.

Heidi Kiser

Einfach der ganzheitliche Ansatz. Ja, das möchte ich sagen. Philipp, was ist dein wichtigster Rat an Unternehmen, wenn es um IT-Sicherheit geht?

Philipp Kalweit

Jön, du hast ja auch schon einige Themen benannt. Und man muss ja ganz klar sagen, ich glaube, gerade auch Mittelstandsunternehmen sind ja gar nicht mal so stark in der Lage, sich in jedem Themenfeld auch wirklich auszukennen und für jeden auch einen internen Experten zu haben. Und das Problem, das ich da einfach sehe, ist, wir können diese Situation gar nicht richtig beherrschen.

Also ich glaube, alle Maßnahmen, die wir treffen können, sind sinnvoll, aber sie müssen auch richtig eingesetzt werden. Und wie wir wissen, ich glaube, Unternehmen investieren gerne in die Dinge, die sie kennen, die sie auch verstehen und die sie auch absichern können. Und das eben so ein bisschen die Grundsatzfrage gar nicht, wie muss ich besser werden, sondern was habe ich übersehen?

Und das fängt natürlich ganz klar, wie ich schon am Anfang sagte, mit einer klassischen Inventarisierung. Jetzt habe ich das Wort. Genau, aller Assets statt.

Also, dass man quasi nicht von vornherein sagt, wir brauchen Phishing-Schutz, wir brauchen irgendwie Endpoint-Protection wie XDR und eine SIEM. Ach Mensch, das können wir uns ja gar

nicht leisten. Alle Experten sagen, wir brauchen das, sondern wirklich zu schauen, welche Systeme habe ich eigentlich in Einsatz und welche Risiken haben die.

Das kann natürlich mit dem Notebook starten. Wer nutzt dieses Notebook? Ich muss nicht jedes Notebook aufzählen, aber ich kann sie ja klassifizieren.

Es gibt Notebooks für die Geschäftsführung, die haben andere Berechtigungen wie in der Buchhaltung und bei der Dame am Empfang. Und das ist ja zum Beispiel etwas, wo ich ganz klar ableiten kann, mit welchen Daten hat sie zu tun, in welchem Netzwerk ist sie angebunden, auf welche Systeme hat sie Zugriff. Das sind die Themen, die leicht sind.

Spannender wird es aber eben bei den Fragen, mit denen wir uns nicht so gut auskennen. zum Beispiel eine Alarmanlage oder einem Drucker. Und auch dort ist es eben nicht wichtig zu sagen, wir müssen das Risiko beherrschen. Es fängt schon allein damit an zu überlegen, kann ich damit eigentlich etwas tun? Sind dort auch hier wieder Berechtigungen drin? Was kann dieses System eigentlich im Netzwerk tatsächlich tun?

Und dann die Frage zu stellen, können wir das intern absichern? Wollen wir das intern absichern und wenn nein, nehmen wir das Risiko in Kauf? Zum Beispiel, weil wir sagen, es ist jetzt kein so extrem großes Risiko oder die Absicherung ist unwirtschaftlich.

Oder, das ist ja auch durchaus ein valider Gedanke, wir sagen, das System hat so viele Zugriffsrechte, so viele Vernetzungen, das ist quasi fast schon wie mit einem Rechner aus einer anderen Schutzkategorie gleichzustellen. Wenn wir das nicht selber absichern können, müssen wir vielleicht Experten hinzuholen, die das punktuell tun. Und da fängt richtige IT-Sicherheit an. Nicht zu sagen, wir müssen für alles den besten Standard haben, sondern angemessen zu gucken, ist eine Alarmanlage jetzt wirklich ans Internet angebunden?

Muss die genauso geschützt werden wie ein klassisches Notebook, das einen hohen Schutzbedarf hat? Oder ist das ein abgetrenntes System ohne Schnittstellen, ohne Internetverbindungen? Dann sprechen nicht.

Und wenn ich das sauber durchführe, dann am Ende ist IT-Sicherheit auch bezahlbar und gerade auch für den Mittelstand sinnvoll umsetzbar. Denn schützen können wir uns nicht vor allem. Die Frage ist vor allem eher, kennen wir das?

Wollen wir da Maßnahmen haben? Und es kann auch durchaus sein, dass wir vielleicht mal an dem Fall sind, dass wir sagen, hey, das ist ein Asset, das ist nicht so wichtig. Am Ende gab es genau deswegen Angriff.

Aber wir wussten zumindest, hey, das haben wir bewertet und jetzt müssen wir es vielleicht nochmal anders angehen und die Einordnung nochmal korrigieren. Weil da fängt IT-Sicherheit nämlich an, auch wieder und wieder zu hinterfragen, ist das, was wir gerade machen, auch richtig? Und nicht immer nur die Frage zu stellen, wie werden wir besser?

Heidi Kiser

Ja, Julian, und dein Schlusswort?

Julian Lucht

Ja, also wir haben es ja eben besprochen, wir sehen einen klaren Trend. Unternehmen investieren definitiv immer mehr in Sicherheit. Die Frage ist noch manchmal, ob wirklich alle relevanten Endpunkte betrachtet werden.

Philipp, du hast es eben auch erwähnt, gerade die Multifunktionssysteme sind halt häufig auch stark vernetzt im Netzwerk. Das muss tatsächlich nicht mehr sein heutzutage. Also es gibt auch Lösungen, Cloud-Lösungen beispielsweise, die es den Kunden ermöglichen, nach wie vor ganz normal das Deauthentifizierung, das Drucken, das Scannen und alles, was man so kennt, zu ermöglichen und bereitzustellen, ohne dass das Gerät wirklich einen großartigen Netzwerkzugriff hat auf internen Ressourcen.

Also es reicht heutzutage vollkommen aus, dem System einfach nur einen Internetzugriff zu geben und gar keinen netzwerkseitigen oder LAN-Zugriff zu gewähren. Dementsprechend kann man dadurch schon einige Risiken, die wir eben schon besprochen haben, deutlich minimieren, wenn nicht sogar komplett verhindern. Und für die Kunden, die sich da gerne selbst zu informieren möchten, haben wir natürlich auf unseren Webseiten entsprechende Informationen bereitgestellt.

Aber auch auf unseren Handbuchseiten haben wir Sicherheitsleitfäden oder auch beispielsweise eine Schritt-für-Schritt-Anleitung, um eine SIEM-Anbindung vorzunehmen. Und für die Kunden, die sich entsprechend direkt mit uns austauschen möchten, beraten werden möchten, können wir natürlich auch sehr gerne in Kontakt treten, um entsprechend unserer Security-Lösungen bereitzustellen. Also dementsprechend kann ich nur die Empfehlung aussprechen, auf uns zuzugehen, damit wir sie entsprechend dann dahingehend beraten können.

Heidi Kiser

Danke. Wenn ich jetzt die drei zentralen Punkte aus dem Gespräch mit euch beiden mitnehmen würde, würde ich sagen, Sichtbarkeit beziehungsweise Transparenz ist ein ganz wesentlicher Faktor, weil man nur schützen kann, was man auch kennt, was einem auch bewusst ist. Resilienz, eben Sicherheit bedeutet eben nicht nur Krisen oder Datenlecks oder so zu verhindern, sondern eben auch im Ernstfall handlungsfähig zu bleiben.

Philipp, mir ist auch ein Satz von dir ganz stark in Erinnerung aus einem Gespräch, wo du sagst, wir können gar nicht die Frage stellen, werden wir angegriffen, weil das wird im Zweifelsfall sowieso passieren, sondern wie gut sind wir darauf vorbereitet und wie handlungsfähig bleiben wir auch. Also Resilienz ist ein ganz zentraler Faktor und dann auch Verantwortung. Also es geht eben nicht nur darum, das IT-Team ins Zentrum zu rücken, sondern IT-Sicherheit ist zu einer richtigen Managementaufgabe geworden.

Und vielleicht der wichtigste Punkt auch in Bezug auf Canon ist, Drucker sind heute nicht einfach mehr Drucker. Die sind angeschlossen, sie sind Teil der digitalen Infrastruktur und damit Teil auch einer ganzheitlichen Sicherheitsstrategie. Das ist vielleicht auch ein Punkt, den viele sich bewusst machen müssen noch.

Ja, bevor ich euch jetzt entlasse oder verabschiede, kommen wir noch zu unserem traditionellen Fragenhagel. Das heißt, ihr bekommt von mir zwei Begriffspaare immer vorgegeben und entscheidet euch möglichst spontan aus dem Bauch heraus für einen von beiden, der am besten zu euch passt. Seid ihr bereit?

Ja. Dann starten wir. Kaffee oder Tee?

Philipp Kalweit

Tee.

Julian Lucht

Ja, Tee.

Heidi Kiser

Berge oder Meer?

Julian Lucht

Meer.

Philipp Kalweit

Meer

Heidi Kiser

Buch oder Podcast

Julian Lucht

Buch

Philipp Kalweit

Podcast

Heidi Kiser

Teams-Meeting oder persönlicher Austausch?

Julian Lucht / Philipp Kalweit

Persönlicher Austausch.

Heidi Kiser

Schnelle Entscheidung oder gründliche Analyse?

Philipp Kalweit

Beides.

Julian Lucht

Kommt drauf an.

Heidi Kiser

Passwort oder Face ID?

Julian Lucht

Face ID

Philipp Kalweit

Ja.

Heidi Kiser

Transparenz oder Perfektion?

Philipp Kalweit

Transparenz

Julian Lucht

Transparenz, ja.

Heidi Kiser

Angriff verhindern oder Krise meistern?

Julian Lucht

Verhindern

Philipp Kalweit

Verhindern.

Heidi Kiser

Ja, dann sind wir jetzt auch schon wieder am Ende unseres Fragenhagels. Vielen Dank Philipp und Julian, dass ihr heute da wart und vielen Dank für die spannenden Einblicke.

Julian Lucht

Ja, vielen Dank, dass wir hier sein durften.

Philipp Kalweit

Heidi, vielen Dank für die Einladung.

Heidi Kiser

Und an unsere Zuhörerinnen und Zuhörer, wenn sie das Thema weiter vertiefen möchten, haben wir in den kommenden Wochen gleich mehrere Gelegenheiten. Nämlich am 24. September veranstalten wir ein Webinar rund um aktuelle Trends und Herausforderungen im Bereich IT-Sicherheit.

Außerdem sind wir mit Canon auf der Smart Country Convention in Berlin vom 13. bis 15. Oktober und würden uns natürlich auch da freuen, Sie persönlich kennenzulernen.

Und wir sind auch auf der it-sa in Nürnberg vom 27. bis 29. Oktober und informieren über aktuelle Lösungen und Sicherheitskonzepte.

Vielen Dank fürs Zuhören und bis zur nächsten Folge des Canon OnAIR Podcast. Auf Wiederhören.

Outro

Das war Canon OnAIR. Let's Talk. Weitere Informationen finden Sie auch immer in den Shownotes oder unter [Canon.de/business](https://www.canon.de/business). Freuen Sie sich schon jetzt auf die neuen Folgen von Canon OnAIR. Let's Talk.