#ConnectLife – der Podcast von A1
Spuren im Netz: Wie Unternehmen und private User:innen Kontrolle über ihre Daten behalten
Transkript

Joe Pichlmayr: Wir als Individuen haben überhaupt keine Chance, uns gegen diese Form von Datenmissbrauch zu wehren. Es sei denn, wir würden auf all diese Dienste verzichten. Das ist nicht im Sinne des Erfinders. Keiner von uns will quasi als digitaler Eremit – offline, abgetrennt von allen anderen Menschen – leben. Das soll es nicht sein.

Leo: Das Internet kann nicht vergessen, das ist richtig. Sobald etwas im Internet gelandet ist, ist es ganz leicht für jemand anders, das herunterzuladen und dann später irgendwo wieder hochzuladen.

Joe Pichlmayr: Für uns alle gilt eigentlich ja updaten, updaten, updaten und Sicherheit auch tatsächlich leben und nicht irgendwie, ja, von Fall zu Fall einmal darauf zu schauen und sie zu ignorieren; weil das ist etwas, was sich unterm Strich irgendwann rächen wird.

Martina Steidl: Mit jedem Posting, jeder Story, jeder Nachricht, mit jedem Klick hinterlassen wir Spuren im Netz. Manchmal bewusst und freiwillig, aber oft auch unbewusst und unbemerkt. Das spürt man, wenn man einmal einen Babynahrungs-Spot bis zum Ende angeschaut hat und ab dann plötzlich jeden Tag Werbung für Baby-Zubehör bekommt. Oder es als Unternehmen plötzlich mit Hackern zu tun bekommt, die wichtige Daten verschlüsseln und freipressen wollen. Was passiert mit meinen Daten? Wo landen sie? Wie kann ich als Privatperson und Unternehmen die Kontrolle über meine Profile auf Social Media und meine Daten behalten? Genau darüber spreche ich heute mit Joe Pichlmayr, CEO des Cybersecurity-Unternehmens IKARUS, und Leo, Cybersecurity Analyst bei A1. Ich bin Martina Steidl und freue mich auf eine spannende Folge.

Hallo, Joe, herzlich willkommen bei #ConnectLife – dem Podcast von A1.

Joe Pichlmayr: Hallo!

Martina Steidl: Joe, du bist ja der Experte in Sachen Computerviren und Cyberattacken. Ich möchte mit dir gerne über Cyberattacken auf Unternehmen, auf Firmen sprechen. Die richtig großen Angriffe zum Beispiel, wie im Vorjahr auf das IT-Unternehmen Kaseya – deshalb mussten ja in Schweden über 800 Supermärkte schließen, weil die Kassen nicht mehr funktioniert haben. Wie ist so was eigentlich möglich?

Joe Pichlmayr: Ja, so was ist genauso leicht möglich, wie ein Unternehmen, das mein Primär- oder mein Endziel ist, anzugreifen; das heißt, Softwarehersteller oder Cloudservice- und Cloud-Dienstanbieter sind ja genauso wie alle anderen Unternehmen rechtlich dazu verpflichtet, bessere Maßnahmen zu ergreifen. Aber letztlich heißt es nicht, dass die nicht angreifbar sind. Und für Angreifer macht es natürlich absolut Sinn, Unternehmen anzugreifen, bei denen sich die Angreifer direkt in die Supply Chain hacken können. Man spricht von einer sogenannten Supply Chain Attack, das heißt, ich hacke einen Lieferanten oder ich hacke einen Dienstebereitsteller und kann damit quasi die Liste meiner Opfer wirklich multiplizieren – wie wir das in den letzten Jahren gesehen haben, in denen es sehr erfolgreiche Angriffe gegen diverse Softwareanbieter gegeben hat und dann gleich mit einem Angriff die Tür zu vielen tausenden weiteren Unternehmen geöffnet wurde.

Martina Steidl: Da geht es ja meistens dann um Erpressung, um viel Geld. Du hast es erwähnt, ein möglichst großer Schaden. Warum gerade diese IT-Firma? Wie suchen sich Hacker ihr Ziel?

Joe Pichlmayr: Das ist ganz unterschiedlich. In den allermeisten Fällen ist es schlicht und einfach Zufall. Das heißt, Hacker scannen im Netz nach Schwachstellen. Hacker suchen nach der Verfügbarkeit bestimmter Dienste, wo sie Schwachstellen kennen. Das ist der allergängigste Weg. Hacker verschicken E-Mails, da wird man zum Kollateralschaden, ist man gar nicht das Primärziel, sondern wird quasi als Beifang in einem großen Fischzug, wenn man so möchte, mitgefangen. Anders schaut die Geschichte aus, wenn man selbst Primärziel ist. Primärziel wird man, weil man für den Angreifer etwa interessante Daten hat – oder Geld, wie jetzt bei den erfolgreichen Angriffen gegen die Spieleplattform, bei denen über 540 Millionen Äquivalent in Kryptowährungen gestohlen wurden. Aber auch, wenn es über meine Infrastrukturen möglich ist, ein viel lohnenderes oder lukrativeres oder sehr gut geschütztes Unternehmen anzugreifen – etwa, wenn ich Lieferant eines großen Unternehmens bin, das sehr gut geschützt ist, oder wenn mein Unternehmen eine besondere Vertrauensstellung beim eigentlichen Endziel genießt.

Martina Steidl: Kurz gesagt, Hacker suchen richtig nach Schwachstellen. Was sind denn diese Schwachstellen?

Joe Pichlmayr: Schwachstellen entstehen einfach beim Programmieren von Softwarelösungen. Je größer eine Softwarelösung, ein Softwarepaket ist, umso größer ist die Wahrscheinlichkeit, dass es da irgendwelche Schwachstellen gibt. Je mehr Dienste, je mehr Funktionalität so ein Programm oder so ein Dienst für uns bereitstellt, umso größer ist die Wahrscheinlichkeit, dass sich irgendwo eine kleine Lücke verbirgt, die ein Angreifer dann mit viel Geschick für sich nutzen kann. Oder: Manchmal ist es viel einfacher, als man denkt, mit einem einfachen Programmaufruf dann tatsächlich Zugriff auf das eigentliche Zielsystem zu erlangen, ohne dass man das großartig lang und breit oder wochenlang vorbereiten muss oder vielleicht User-Interaktion braucht … sondern dass man schlicht und einfach diese Schwachstelle oder diese Hintertür ausnutzen kann, um aus der Ferne mit sehr geringem Aufwand direkt auf das System zuzugreifen.

Martina Steidl: Wie viele Leute sind denn bei einem solchen Hackerangriff in dieser Größenordnung beteiligt? Und wie lange bereiten die sich auf so was vor? Auf so einen Angriff? Das passiert sicher nicht von heute auf morgen.

Joe Pichlmayr: Auch das ist immer vom jeweiligen Angriff abhängig. Wenn es ein zielgerichteter Angriff ist, wo es darum geht, etwa ein Unternehmen auszuspähen, dann wird man sich dafür viel Zeit nehmen, weil alles, was schnell und unter Druck passiert, meistens Spuren hinterlässt oder auffällt. Das heißt, wenn meine Intention ist, mich sehr, sehr lange in dem Unternehmen, das ich ausspionieren möchte oder das ich letztlich angreifen möchte, unentdeckt zu bewegen, quasi meine Position in dem Unternehmen auszubauen, dann kann das bis zu einem Jahr dauern. Wir haben auch schon Angriffe gesehen, wo der Angreifer schon wesentlich länger als ein Jahr im Netz präsent war. Da bewegt er sich natürlich sehr vorsichtig. Das Lateral Movement, so wird das bezeichnet, erstreckt sich wirklich über viele Wochen und Monate und der Angreifer bemüht sich wirklich sehr, hier nicht aufzufallen. Wenn es dem Angreifer darum geht, das Unternehmen direkt anzugreifen, etwa mit einer Ransom-Attacke, dann wird sich der Angreifer so lange still verhalten, bis er alle für seinen Angriff notwendigen Informationen hat. Das heißt, er wird versuchen, einmal alle Rechte in diesem Unternehmen, die er braucht, zu erschleichen oder zu erhacken. Er wird versuchen, herauszufinden, ob er das Backup unterbrechen kann oder wie er das Backup des Unternehmens auch mitverschlüsseln kann. Das heißt, er wird versuchen, ein Maximum an Schaden für das

Unternehmen zu erreichen, um eine möglichst gute Verhandlungsposition zu erzielen. Und dann gibt es natürlich welche, die sind völlig unbedarft, die machen das vielleicht sogar zum ersten Mal oder denen ist alles egal. Ja, die wüten dann halt wie der Elefant in der Porzellankiste, die fallen dann im Regelfall auch schneller auf. Und wenn es ihnen natürlich gelingt, ihren Verschlüsselungstrojaner zu starten, dann kann es trotzdem bedeuten, dass man auf einigen Geräten dann einfach mit verschlüsselten Inhalten konfrontiert ist. Und wenn man dann kein Backup hat, dann wird es natürlich schwierig. Eine andere Option ist, dass man gar nicht von einem Einzeltäter, der sich alles vorher selbst vorbereitet hat, angegriffen wird. Das passiert nämlich nur in den allerwenigsten Fällen. In den allermeisten Fällen nutzen Angreifer die Services Dritter, das heißt Ransom as a Service zum Beispiel. Ich kann mir alle Unterlagen oder alle Informationen und Infrastrukturen, die ich brauche, um ein Unternehmen erfolgreich anzugreifen, im Netz mieten. Das ist recht praktisch. Dazu muss ich weder programmieren können, noch muss ich eine Idee von Security haben, noch eine Idee vom Hacken haben. Ich kann mir das quasi bestellen. Klar, ich muss es bezahlen und muss schauen, dass ich dann mit meinem Eingriff quasi mein Investment, meinen Aufwand wieder reinkriege.

Martina Steidl: Du hast jetzt oft von dem Angreifer gesprochen. Ist das jetzt eher eine Einzelperson oder sind das dann doch größere Gruppen, die solche Attacken dann vorbereiten und auch durchführen?

Joe Pichlmayr: Auch hier ist es querbeet. Wir haben sehr wohl Profile, wo wir mit Einzeltätern zu tun haben, die dann auch als Einzeltäter ausgeforscht worden sind. Allerdings muss man davon ausgehen, dass Attacken, die wir als weiter qualifiziert oder fortgeschritten bezeichnen, immer von Teams ausgeführt werden. Das gilt für staatliche Akteure, die im Team arbeiten, genauso wie für Angriffe, die man dem Cybercrime-Umfeld zuordnen kann, bei denen schlicht und einfach mehrere Akteure zu Werke gehen. Was einfach damit zu tun hat, dass man Spezialisten aus unterschiedlichsten Bereichen zu so einem Angriff zusammenzieht, eine Gruppe formt, weil ein Einzelner dafür entweder zu lange brauchen würde oder diesen Eingriff gar nicht durchführen könnte.

Martina Steidl: Wie gehen dann solche Angriffe in der Regel aus, wenn es um diese großen Erpressungsgeschichten geht? Wie teuer wird das für das Unternehmen und vor allem, wie lange dauert es eigentlich, bis dann wieder alles geregelt abläuft?

Joe Pichlmayr: Ja, das ist das, was es eigentlich wirklich teuer macht, nämlich wie lange dauert es, bis es wirklich wieder geregelt abläuft. Und das wissen auch die Angreifer. Also, in den allermeisten Fällen ist es Unternehmen schon möglich, quasi wieder aus eigener Kraft auf die Beine zu kommen. Aber das dauert sehr, sehr lang und die Angreifer wissen, dass ihr stärkster Trumpf jener ist, dass der Betriebsausfall, die Betriebsunterbrechung – also die Zeit, in der das Unternehmen nicht produzieren kann oder nicht online sein kann oder kein Geld verdienen kann – das ist, was den eigentlichen Schaden verursacht. Die wissen ganz genau, dass im industriellen Umfeld, im Produktionsumfeld die Summen, die sie fordern, meistens bei einem Zehntel des tatsächlichen Betriebsstillstands und Ausfalls liegen. Und damit wird es schon sehr lukrativ für die Betroffenen, darüber nachzudenken, zu denken, wir kommen halt nicht darum herum, da jetzt die geforderte Summe zu zahlen. Dafür können wir wesentlich schneller wieder online gehen und wesentlich schneller wieder die Produktion aufnehmen. Was aber auch dann nicht heißt, dass die zur Tagesordnung übergehen können; die sind dann tatsächlich meistens damit beschäftigt, die Gesamtsystem-Integrität ihres Unternehmens, ihrer Infrastrukturen wiederherzustellen, und so was kann mehrere Monate bis zu einem Jahr oder länger dauern und ist so oder so sehr, sehr teuer. Was man auch nicht übersehen darf, ist, dass man nie ausschließen kann, dass der Angreifer, der wohl seine Erpressersumme oder seine geforderte Lösegeldsumme bekommen hat,

die Daten, die er gestohlen hat, nicht noch zusätzlich weiterverwertet. Das erleben wir immer wieder, dass auch Unternehmen, die bezahlt haben, dann letztlich auch darunter leiden, dass die Daten, die ihnen gestohlen wurden, im Darknet noch einmal verkauft wurden oder mehrfach verkauft wurden, einfach weil der Angreifer sagt, okay, let's make money – und der hat ja keinen persönlichen Bezug zu seinem Opfer, den stört das wenig, der spürt kein Leiden, der spürt keinen Schmerz, der spürt keine Überstunden, der macht einfach nur Geld.

Martina Steidl: Was mache ich jetzt, wenn mir das passiert? Wenn ich die Nachricht bekomme, zum Beispiel, dass meine Daten verschlüsselt sind. Ich komme in kein System mehr rein. Was tun? Wo soll ich mich melden?

Joe Pichlmayr: Wenn ich nicht selber über das Wissen und über die Fähigkeiten verfüge, mit so einer Situation umzugehen, und das tun leider die allerwenigsten von uns, dann muss ich mal jemand holen, der mir helfen kann. Wenn ich hier versuche, auf eigene Faust und Gutdünken oder auf Bauchgefühl basierend Gegenmaßnahmen zu ergreifen, dann ist die Wahrscheinlichkeit, dass ich den Schaden viel schlimmer mache, sehr hoch. Wenn ich mit meinem Auto liegen bleibe und eine Panne habe, dann mache ich auch nicht mehr den Motorraum vorn auf und schaue nach, sondern ich rufe die, die wissen, wie es geht, nämlich den ÖAMTC oder den ARBÖ, also ich hole die Profis. Und genau das Gleiche gilt in so einem Fall. Wenn mir das an einem Wochenende passiert und ich die IT-Abteilung in meinem Unternehmen nicht erreiche, dann muss ich schauen, dass ich irgendeinen Kollegen, irgendeinen Chef erwische, weil das auch für das Unternehmen superkritisch ist. Je schneller hier alle, die betroffen sind, informiert sind, umso besser ist es. Und dann gilt es, einen kühlen Kopf zu bewahren und dann mal zu analysieren: Wer ist denn betroffen? In welchem Ausmaß sind wir betroffen? Welche Optionen haben wir? Und bevor Sie das nicht wissen, nehmen Sie auch keinen Kontakt zu dem Erpresser auf, weil die allermeisten Erpresser ihre Angriffe über Infrastrukturen von Dritten fahren. Und für die läuft der Zeiger ab dem Zeitpunkt, ab dem sie das erste Mal quasi mit dem Opfer Kontakt aufnehmen können. Und da gilt die Antwort des Opfers. Das heißt, solange das Opfer nicht antwortet, so lange tickt die Uhr nicht, so lange muss der Angreifer auch nicht dafür zahlen. Aber ab dem Zeitpunkt, wo Sie antworten, hat er Kosten und deswegen macht er Druck. Auch weil er weiß, am Anfang ist die Verzweiflung am größten. Da ist die Chance, dass Sie einknicken und bereit sind zu zahlen, am höchsten. Und je länger die Zeit voranschreitet, umso mehr Optionen haben Sie und umso geringer wird die Wahrscheinlichkeit, dass er zu seinem Geld kommt. Also, wenn Sie mit ihm Kontakt aufnehmen, dann sollten Sie Ihre Optionen schon kennen.

Martina Steidl: Wie können sich Firmen jetzt am besten schützen? Eine betroffene Firma wird sicher was unternehmen, dass das vielleicht nicht wieder vorkommt. Aber was ist jetzt so ein absolutes Must-have als Unternehmen?

Joe Pichlmayr: Das muss man differenzierter betrachten, weil die Möglichkeiten, die etwa ein großes Unternehmen mit ausreichend Ressourcen und vielen sehr gut geschulten Mitarbeitern und Prozessen und sehr guter Infrastruktur ergreifen kann, sind natürlich andere als die, die die meisten mittelständischen oder kleinen Unternehmen ergreifen können. Die Großen wissen sich im Regelfall zu helfen. Manchmal brauchen sie den Anschub, dass es einmal wehtut, aber dann finden sie im Regelfall schon zu einer Lösung, wo man sagen kann, ja, da erreichen sie schon ein sehr gutes Maß an Sicherheit. Zum einen, weil es das Gesetz vorschreibt, zum anderen, weil sie es natürlich aus Eigeninteresse machen. Bei den mittelständischen und kleinen Unternehmen ist es schon viel schwieriger, da auf ein Leistungsäquivalent zu kommen, das sich große Unternehmen leisten können. Das ist die Schwierigkeit, weil auch kleinere und mittlere Unternehmen mit den gleichen Attacken konfrontiert sind. Und da macht es durchaus Sinn – wenn man

nicht wirklich selbst Ressourcen aufbringen kann, um sich um dieses Thema zu kümmern –, hier seinen Provider, seinen Dienstleister zu beauftragen – A1 bietet hier wirklich umfangreiche Lösungen an – und diese in Anspruch zu nehmen, weil diesen hohen Spezialisierungsgrad in all diesen Bereichen, in denen es Maßnahmen braucht, den kann man als KMU oder als mittelständisches Unternehmen im Regelfall weder finanzieren noch aufbringen. Also, da macht es wirklich Sinn, mit seinen Partnerunternehmen zu sprechen und diese Aufgabe dann gemeinsam mit einem Dienstleister zu erfüllen.

Martina Steidl: Was lädt den Hacker geradezu ein? Gibt es für dich Situationen, wo du von einem Unternehmen gebeten wirst, was für die Cybersecurity zu tun, und du denkst dir, um Gottes Willen, ein Wunder, dass noch nichts passiert ist?

Joe Pichlmayr: Ja, was natürlich sehr einfach und schnell geändert werden kann, das ist, dass man seine Systeme aktuell hält. Für jeden von uns ist es ganz normal, dass er mit seinem Auto einmal im Jahr zur Überprüfung fährt. Da denkt niemand darüber nach, obwohl es der Gesetzgeber sogar vorschreibt. Da wissen wir alle, warum wir das brauchen. Weil wir nicht in ein Auto steigen wollen, dem wir nicht vertrauen können, weil vielleicht die Bremsen nicht funktionieren. Das Gleiche gilt auch für unsere Infrastrukturen, gleich ob das auf unseren Handys, Tablets, Smartphones, auf unseren PCs oder Servern ist. Wenn ich mich nicht darum kümmere, dass die immer up to date sind, dass dort immer die aktuellsten Versionen laufen, wenn ich mich nicht darum kümmere, wer darf denn auf welche Daten zugreifen … Es ist ja auch so: Zu Hause regle ich ja auch, wer bei mir reindarf und wer bei mir nicht reindarf. Das sind so grundlegende Dinge, wo wir sehr schnell sehen, okay, das ist jetzt wirklich die offene Tür, die jeden Hacker quasi einlädt. Wenn das nicht klar geregelt ist oder wenn alte Systeme, veraltete Systeme im Einsatz sind und wenn es keine klaren Benutzerrichtlinien gibt, wer wie auf welche Daten zugreifen darf.

Martina Steidl: Also die Aufforderung zum Update nicht immer ignorieren oder auf später verschieben, sondern wirklich updaten.

Joe Pichlmayr: Das ist das Um und Auf. Das ist für IT-Unternehmen eigentlich schon verpflichtend. Da gibt es wirklich keine Ausreden mehr. Das ist für Unternehmen im produzierenden Bereich oder im Bereich von Mess- und Regeltechnik, Steuerungstechnik, im industriellen Umfeld natürlich schon viel, viel schwieriger, weil deren Anlagen ja nicht so einfach upgedatet werden können wie vielleicht etwa unser PC oder unser Smartphone. Dort braucht es dann andere Maßnahmen, etwa, dass man die Netze sehr klug segmentiert, dass man andere Richtlinien und Maßnahmen ergreift. Aber für uns alle gilt eigentlich ja updaten, updaten, updaten und Sicherheit auch tatsächlich leben und nicht irgendwie, ja, von Fall zu Fall einmal darauf zu schauen und sie zu ignorieren. Weil das ist etwas, was sich unterm Strich irgendwann rächen wird.

Martina Steidl: Da sind wir dann auch schon beim Stichwort für die letzte Frage: Datenmissbrauch. Daten sind das neue Gold, das hört man jetzt immer öfter. Das Sammeln von Daten. Ja, wie können sich denn Privatpersonen vor Datenmissbrauch schützen?

Joe Pichlmayr: Das sind die Schattenseiten meines Jobs, dass ich immer die schlechten Nachrichten überbringen muss. Wir als Individuen haben überhaupt keine Chance, uns gegen diese Form von Datenmissbrauch zu wehren. Es sei denn, wir würden auf all diese Dienste verzichten. Das ist natürlich nicht im Sinne des Erfinders. Keiner von uns will quasi als digitaler Eremit – offline, abgetrennt von allen anderen Menschen – leben, das soll es nicht sein. Die Schwierigkeit liegt darin, dass es immer herausfordernder, immer komplexer wird selbst für Menschen, die sehr vorsichtig sind, für Menschen, die viel Wert

auf ihre Privatsphäre legen, nachvollziehen zu können, wo sie denn Daten verlieren, wenn man es so bezeichnen möchte, oder wo sie den Daten abliefern. Das fängt ja bei unseren Smartphones an, wo selbst Forscher an Universitäten nicht genau sagen können, was denn unser Smartphone ohne unser Wissen an den Betreiber oder an den Hersteller kommuniziert. Da kann man nur mutmaßen und vermuten. Mit jedem Dienst, den wir nutzen, mit jeder App, die wir installieren, stimmen wir im Regelfall auch zu, dass unsere Daten verwendet werden können. Uns muss bewusst sein, dass wir das Produkt sind. Alles, was gratis ist, bezahlen wir mit unseren Daten. Und das verdrängen wir gern, weil es halt angenehm ist, dass wir wirklich viele tolle Services, tolle Apps, tolle Produkte nutzen können, ohne dass wir dafür zahlen müssen oder indem wir nur sehr wenig dafür zahlen. Das ist etwas, was im Bewusstsein der meisten Menschen nicht verankert ist. Und selbst wenn es verankert ist, dann ist der Mensch schlicht und einfach damit überfordert, zu verstehen, welche Möglichkeiten diverse Diensteanbieter haben, um an Datenpunkte zu kommen. Und das ist sicher ein großes Problem, nicht nur für uns als Einzelne, sondern auch für uns als Gesellschaft. Nämlich dass der Basisdeal des Netzes – du gibst mir deine Daten – dazu führt, dass die allermeisten Apps und allermeisten Dienste darauf optimiert sind, sehr, sehr viele Datenpunkte von ihren Nutzern, von ihren Anwendern zu bekommen. Und wir sprechen von sehr, sehr vielen Datenbanken, von wirklich Millionen Datenpunkten. Und wenn man diese Datenpunkte miteinander vermischen kann, man Algorithmen damit füttern kann, wenn man sogenannte Predictive Maintenance, also vorhersehende Algorithmen, wie es so schön heißt, damit füttern kann, dann ist es den unterschiedlichsten Anbietern sehr rasch möglich, auch sehr fragmentierte Bilder von uns zu vervollständigen. Wenn ich in Schulen gehe, mich Kinder fragen, wo muss ich aufpassen oder warum weiß denn Google alles über mich? Ich bin doch vorsichtig und erzähle Google gar nicht alles über mich. Dann erzähle ich meine Geschichte und sag, wenn du einen Freund besuchst, der gerade ein Puzzle baut, das noch gar nicht fertig ist, dann reichen dir die wenigen Puzzlesteine, die du siehst, um schon zu erkennen, um welches Bild es sich handelt. Und genauso ist es bei Google und all den anderen Großen. Ihnen reichen im Regelfall nur wenige Puzzlesteine, um sich ein komplettes Bild von dir machen zu können, weil sie den Rest einfach durch Vergleiche und vorhersehende Berechnungen quasi ausrechnen können. Und das macht uns eigentlich, ja, gläsern ist, glaube ich, schon intransparent, das macht uns mehr als gläsern.

Martina Steidl: Kannst du nachts gut schlafen, wenn du online was bestellt hast?

Joe Pichlmayr: Absolut. Warum kann ich gut schlafen, wenn ich online was bestellt habe? Weil ich ein Mindestmaß an Vorsicht walten lasse. Weil ich meine Systeme up to date halte. Weil ich das tue, was dem Stand der Technik entspricht. Und sollte ich hier quasi Opfer eines Eingriffs werden, bin ich wirklich sehr zuversichtlich, dass mir dann vom jeweiligen Dienstebetreiber der Schaden sehr schnell wieder ersetzt wird, sei das beim Onlinebanking, sei das, wenn ich auf einer Onlineplattform bestelle, da schlafe ich wirklich entspannt.

Martina Steidl: Da sind wir jetzt auch schon viel entspannter, nach diesen Abschlussworten von dir, Joe. Vielen, vielen Dank für das interessante Gespräch. Danke schön.

Joe Pichlmayr: Sehr, sehr gern.

Martina Steidl: Ist ein Profil auf Social Media wirklich so einfach zu hacken? Wie viel von unseren Daten sollen wir preisgeben? Einmal im Netz, immer im Netz? Sind unsere Spuren im Internet wirklich unauslöschbar? Das wird uns jetzt mein nächster Gast, Cybersecurity Analyst bei A1 Leo, beantworten.

Hallo, Leo, willkommen bei unserem Podcast von A1, bei #ConnectLife.

Leo: Hallo! Schön, dass ich da sein darf.

Martina Steidl: Leo, du bist Cybersecurity Analyst bei A1. Was machst du genau? Bist du von Beruf Hacker?

Leo: Was wir in der Cybersecurity machen, ist, wir jagen Hacker beziehungsweise wir versuchen, Hacker aus dem Unternehmen fernzuhalten. Und wie macht man das am besten? Na ja, indem man weiß, wie man hackt oder wie ein Hacker vorgehen würde. Und mit dem Wissen kann man halt gegen die Bösewichte vorgehen.

Martina Steidl: Wir reden ja heute über die Spuren im Netz und du bist ja auch ein Profi, was Daten im Netz betrifft. Du hast hoffentlich oder du hast bestimmt eine Antwort auf meine nächste Frage: Wenn ich im Netz etwas gesucht habe, einen Suchbegriff eingegeben habe, ob das jetzt Schuhe sind, ein Tennisschläger oder eine Couch, warum bekomme ich dann überall sofort Werbung oder Infos zu meinem Suchbegriff angezeigt? Wie funktioniert das? Woher wissen das die Unternehmen, die dann alle reagieren?

Leo: Also, die Position eines Suchmaschinenanbieters ist total gut, weil er kann ganz viele Sachen über dich lernen, nämlich alles, was du gesucht hast. Das sind die Dinge, die dich interessieren. Und wenn man jetzt ein Anbieter ist von irgendetwas, das man verkaufen möchte, dann geht man hin zu einem Suchmaschinenanbieter und bezahlt den für die Informationen. Die sind nämlich tatsächlich das, was so viel wert ist. Die Informationen, sagt man ja, sind das neue Gold oder neue Öl oder was auch sonst immer.

Martina Steidl: Die meisten, die persönlichen Daten, die geben wir ja vollkommen freiwillig preis in den sozialen Netzwerken. Schauen wir uns vielleicht bitte Social Media ein bisschen genauer an, Instagram, Facebook, Twitter, TikTok und so weiter. Was passiert hier mit unseren Daten, mit den Bildern, die wir posten? Mit Likes?

Leo: Ganz genau dasselbe Spiel. Es sind nur andere Spieler da drinnen. Die konkurrieren miteinander, Suchmaschinen und verschiedene Social Media. Aber wenn wir etwas liken, dann heißt das, hey, das ist eine Sache, die mich interessiert. Oder wenn ich in irgendeiner Gruppe zu irgendetwas poste, oder irgendetwas mit irgendwelchen Tags, Hashtags oder so, dann kann, wer auch immer diesen Service betreibt, ganz, ganz viel über mich lernen und entsprechende Werbung schalten.

Martina Steidl: Nehmen wir jetzt an, ich finde Fotos oder Videos von mir im Netz, die ich nicht selbst dort postiert habe. Wie schaffe ich es, sie wieder zu löschen? Geht das überhaupt? Oder ist das so? Einmal im Netz, immer im Netz?

Leo: Das ist tatsächlich ganz schwierig. Und grundsätzlich ist es genau so: Wenn es einmal im Netz ist, ist es immer im Netz. Jedenfalls dann, wenn es ganz besonders wertvoll ist oder interessant ist für die Allgemeinheit, sage ich jetzt mal. Man hat mir mal gesagt, das Internet kann nicht vergessen. Das ist richtig, weil sobald etwas im Internet gelandet ist, ist es ganz leicht für jemand anders, das runterzuladen und dann später irgendwo wieder hochzuladen. Und wenn sich so etwas weit genug verbreitet hat, ist es einfach unmöglich, sämtliche Kopien davon zu finden. Wenn es aber so ist, dass jemand einzelnes irgendwo Bilder gepostet hat und das irgendeine Art moderiertes Forum ist, wie zum Beispiel ein soziales Netzwerk, dann – ich bin jetzt kein Rechtsexperte, aber meines Wissens ist der Anbieter verpflichtet, die Sachen runterzunehmen, wenn man so einen

Take-down Request, so heißt das, macht. Aber das heißt nicht, dass der, der das ursprünglich aufgestellt hat, das nicht mehr auf seinem eigenen Computer irgendwo hat und das später wieder wohin tun könnte. Das ist wirklich ganz schwierig.

Martina Steidl: Was rätst du jetzt generell? Wie sollte man denn mit seinen Daten im Internet umgehen? Was ist unbedenklich oder wo wird es gefährlich?

Leo: Grundsätzlich nicht hergeben, weil das geht ja niemanden was an, diese Informationen sind für andere Leute wertvoll und die gehören aber eigentlich mir. Wenn es nicht unbedingt notwendig ist, würde ich mich nicht – und tue ich auch nicht – irgendwo registrieren, weil ich gebe halt echt nur Unternehmen Informationen, die für sie wertvoll sind und mir nichts bringen. Das heißt, wenn man sich mal schnell registriert, um irgendeinen Service zu bekommen – es gibt E-Mail-Anbieter, die einem eine E-Mail-Adresse geben, die nur kurz gilt, mit der man sich dann registrieren kann.

Martina Steidl: Wie kann man sich denn sonst noch schützen, sei es jetzt als Privatperson oder auch als Unternehmen, um nicht gehackt zu werden?

Leo: Das ist schwierig. Man muss halt wirklich auf seine Sachen aufpassen. Mal als erstes von wegen, hey, ihr benutzt sicher sichere Passwörter. Sichere Passwörter sind in erster Linie lang. Das mit den ganzen Sonderzeichen und so weiter, das ist nicht so wichtig, sie müssen nur lang sein. Das kann man sich ganz einfach mathematisch ausrechnen. Und es ist zu empfehlen, nicht für unterschiedliche Dienste dieselben Passwörter zu verwenden. Das ist wirklich gefährlich, weil sobald ein Dienst gehackt wird und dort dann die Passwörter zum Vorschein kommen, könnte man ja dieselben Passwörter für andere Dienste verwenden, die jemand auch noch verwendet. Und wenn es dann wirklich jemand auf einen abgesehen hat – das nennt man Social Engineering, wenn man versucht, doch irgendwie nett zu fragen und so, hey, ich brauch mal schnell ein Telefon, um irgendwen anzurufen, und halt davor außer Atem daherkommt, um sehr überzeugend zu wirken. Fast jeder Mensch stimmt dem zu. Das ist wirklich eine Wissenschaft.

Martina Steidl: Was bedeutet Social Engineering für Unternehmen, für Firmen?

Leo: Na ja, eine Firma zu hacken wäre doch viel leichter von innen, weil wenn man schon mal in dem Gebäude drinnen ist, findet man sicher irgendwo irgendeine Internetbuchse, wo man was anstecken kann, oder einen Computer, der nicht gesperrt ist, und das heißt, man müsste mal reinkommen. Und es funktioniert am besten einfach so, indem man sich eine schöne Geschichte ausdenkt, wieso man denn ganz dringend da reinmuss. Weil man von irgendeiner Firma ist, weil man ihnen etwas liefern muss oder sonst was. Geht zum Empfang. Fragt dort ganz lieb, ob man aus diesem und jenem Grund denn reindarf. Und dann hat man sich am besten eine gute Geschichte ausgedacht, und das funktioniert auch sehr gut, wenn man Leute unter Druck setzt. Hey, das muss jetzt passieren, da muss jetzt eine Entscheidung fallen, das ist wichtig. Dann kommt man überraschend oft rein. Ich habe sehr viele Geschichten gehört und gelesen.

Martina Steidl: Dann sage ich vielen, vielen Dank, Leo, für das interessante Gespräch und all dein Insiderwissen.

Leo: Danke, dass ich da sein durfte.

Martina Steidl: Die Spuren zu #ConnectLife – dem Podcast von A1, die findet ihr übrigens auf allen gängigen Podcast-Plattformen. Falls Ihr Feedback, Fragen oder Wünsche habt, schreibt an podcast@a1.at. Ich sag Danke fürs Zuhören und freu mich auf das nächste Mal. Bis dann!