#ConnectLife – der Podcast von A1
A1 Sommergespräche: Gehackt, erpresst, bestohlen – die 9 ¾ besten Tipps für mehr digitale Sicherheit
Transkript

00:00:01:05 - 00:00:45:03
Die Fire-and-Forget-Lösung, die gibt es nicht. Cybersicherheit ist eine Reise, auf der Sie sich mit dem Thema immer wieder beschäftigen müssen. Es ist nicht damit getan, dass Sie einmal Maßnahmen ergreifen, sich zurücklehnen und sagen, so, das war es. So wie sich die Märkte entwickelt haben, haben sich natürlich auch Dienstleister für diese Märkte entwickelt. Das heißt, ich kann mir Hacker mieten, um Angriffe durchführen zu lassen. Es braucht nämlich den Zugang, dass Sie die Leute, die Cybersicherheit in Ihrem Unternehmen ansteuern, tatsächlich sehr, sehr nahe an die Chefetagen heranführen und sie in alle Unternehmenstätigkeiten eingebunden werden, weil Sie nur mit einem gesamtheitlichen Ansatz oder gesamtheitlichen Zugang hier halbwegs sinnvolle Ergebnisse zusammenbringen.

00:00:46:15 - 00:01:26:19
Hackerattacken, Datenraub, Erpressung. Die Zahl der Cyberangriffe auf Private, Unternehmen, Verwaltungen oder Behörden ist in den vergangenen zwei Jahren regelrecht explodiert. Wie können wir uns vor Cybercrime besser schützen? Wo sind Unternehmen angreifbar? Worauf zielen einzelne Hacker oder ganze Gruppen überhaupt ab? Und wie reagiere ich richtig, wenn der Ernstfall eintrifft? Das alles und noch einiges mehr erfahrt ihr im A1 Sommergespräch von #ConnectLife – dem Podcast von A1. Mein heutiger Gast ist Joe Pichlmayr, CEO bei Ikarus Security Software. Ich bin Martina Steidl. Viel Spaß beim Zuhören.

00:01:28:05 - 00:01:32:20
Hallo, Joe! Lieber Joe, ich freue mich, dass du wieder Gast bist bei uns, bei #ConnectLife – dem Podcast von A1.

00:01:33:11 - 00:01:34:20
Sehr gerne. Danke für die Einladung.

00:01:35:09 - 00:02:08:22
Wir haben uns ja bereits in Folge 27 ein wenig über das Thema Cybersecurity mit dir unterhalten. Und wir wollen unseren Hörerinnen und Hörern noch mehr Tipps geben für mehr digitale Sicherheit. Sicher arbeiten, surfen, gamen, Daten speichern. Wie macht man das alles richtig? Eben all das und noch mehr wollen wir heute mit dir besprechen. Und zum Start: Was ist denn eigentlich jetzt das Um und Auf, sage ich mal, für den privaten User, die private Userin, um gegen einen Cyberangriff, einen Hackerangriff gewappnet zu sein?

00:02:09:18 - 00:03:55:15
Ja, das lässt sich leicht beantworten. Das Um und Auf ist die Fähigkeit, dass er die Daten, die er bei so einem Angriff verlieren kann, wieder rekonstruieren kann. Das heißt, dass ich mich als Privatanwender tatsächlich ernsthaft darum kümmere, dass meine Daten regelmäßig weggesichert werden. Ich kann einen GAU nicht verhindern, wenn ich tatsächlich Ziel eines Angriffs werde, unverschuldet, weil der Angreifer einfach wirklich gut ist oder weil es halt passiert. Und es passiert auch einfach, und dann ist es natürlich immer dumm, wenn man erst dann reagiert und überlegt, wie tu ich jetzt? Es ist immer schlauer, ein bisschen vorzubeugen. Und natürlich ist es ein bisschen aufwendiger, wenn man sich auch überlegt, was sind die wirklich wichtigen Daten für mich? Und wie stelle ich sicher, dass die auch außerhalb meiner Systeme, meines Netzwerks gesichert und

gelagert werden? Aber das zahlt sich aus. Da gibt es viele Möglichkeiten. Es ist gar nicht so kompliziert, ich muss es mir nur anschauen. Ich kann meine Daten in der Cloud speichern. Das ist ein sehr effizienter Weg. Das ist durchaus auch ein Weg, den man empfehlen kann. Es gibt sehr gute Angebote aus Österreich, die man auch, wenn man nicht möchte, dass seine Daten das Land verlassen, in Anspruch nehmen kann. Es ist sehr einfach, Daten etwa auf einen USB-Stick wegzukopieren. Es ist sehr einfach, Daten auf einen externen Datenträger, also auf eine externe Festplatte wegzukopieren. Es gibt auch viele Unternehmen, die Backup as a Service anbieten. Da muss man sich aber auch vertraut damit machen, welche Angebote gibt es dort, welche könnten für mich passen, und das in Anspruch nehmen. Und wir kennen viele Unternehmen, aber auch Private, die nicht nur ein Backup, sondern zwei, drei haben, einfach, um auf Nummer sicher zu gehen.

00:03:56:03 - 00:04:05:15
Jetzt sind schon viele Apps oder Programme vorinstalliert. Sind die hilfreich? Inwieweit sind sie das? Kann man die nutzen? Reicht das aus?

00:04:06:08 - 00:04:59:16
Die boardeigenen Mittel sind immer hilfreich. Grundsätzlich gilt beim Thema Security: 100 Prozent ist a) nicht realisierbar und erreichbar, und b) ist auch nicht wirtschaftlich. Das heißt, versuchen Sie einmal, mit den boardeigenen Mitteln die 80 Prozent zu erreichen, und das reicht im Regelfall aus. Ich stelle aber auch sicher, dass ich a) meine boardeigenen Mittel kenne, und b) auch sicherstelle, dass die boardeigenen Mittel genauso wie meine Betriebssysteme und die Programme, die ich nutze, auch immer aktualisiert werden. Und wenn ich einmal in der Lage bin, quasi mein System mit den boardeigenen Mitteln anzusteuern, dann bin ich eigentlich eh schon ganz gut unterwegs, weil dann habe ich mich schon mal ernsthafter damit auseinandergesetzt, welche Möglichkeiten bietet mir ein Betriebssystem, welche Möglichkeiten bieten mir meine Programme, bieten mir die Dienste, die ich nutze. Und das ist ganz sicher ein wichtiger Schritt in die digitale Reise, die jeder tun sollte.

00:04:59:23 - 00:05:01:21
Wie arbeiten da die größeren Unternehmen?

00:05:02:18 - 00:06:31:07
Die größeren Unternehmen gehen hier natürlich ein bisschen diversifizierter vor. Es ist natürlich klar, dass zwei Augen immer mehr sehen als eines, oder vier Augen mehr als zwei sehen. Das heißt, die setzen hier auf einen Mix aus verschiedenen Maßnahmen. Das kann man natürlich auch machen. Das ist immer die Frage – wie intensiv möchte ich mich damit beschäftigen, weil es letztlich dann doch auch ein Aufwand ist. Also die, wenn man so möchte, Fire-and-Forget-Lösungen, die gibt es nicht. Cybersicherheit ist eine Reise, auf der Sie sich mit dem Thema immer wieder beschäftigen müssen. Es ist nicht damit getan, dass Sie mal Maßnahmen ergreifen, sich zurücklehnen und sagen so, das wars. Das wird nie der Fall sein, weil mit jedem neuen Update, mit jedem neuen Programm, das Sie runterladen, mit jedem neuen System, das Sie in Betrieb nehmen, natürlich diese Arbeit wieder getan werden muss, auf der einen Seite. Dann, auf der anderen Seite, weil natürlich die Angreifer einem recht simplen Prinzip folgen, nämlich dem Weg des geringsten Widerstands – schauen wir mal, wo sind Systeme leicht angreifbar, weil sie nicht gewartet werden, weil sie alt sind, weil sie vielleicht gerade eine Sicherheitslücke bieten, weil der oder die Betreiber sich einfach nicht geschickt verhalten. Na, dann wird man dort zuschlagen, bevor man ein gut gesichertes System, einen Anwender, der sich richtig verhält, versucht, mit wesentlich höheren Aufwänden anzugreifen. Und was mir dabei einfach klar sein muss, ist, dass das Florianiprinzip, also um einiges besser zu sein als die Mehrheit der anderen, wirklich schon viel helfen kann.

00:06:32:11 - 00:06:38:11
Welche Rolle spielt denn jetzt, sag ich mal, das Passwort? Jeder steigt ein auf seinem PC, muss das Passwort eingeben.

00:06:39:05 - 00:08:13:20
Das lässt sich leicht anhand eines Beispiels erklären. Ein Passwort ist nichts anderes als ein Schlüssel. Meistens ist es so, dass ich nicht nur einen Schlüssel, sondern viele Schlüssel habe, weil ich ja nicht nur einen Raum, sondern viele Räume öffnen will. Also, ich habe einen ganzen Schlüsselbund und die Schlüssel auf diesem Bund ermächtigen mich oder ermöglichen mir einfach, viele verschiedene Bereiche zu betreten. Wird mir einer dieser Schlüssel gestohlen oder verliere ich den Bund, dann merke ich das natürlich sofort. Und das ist der große Unterschied zum Passwort, das zwar die gleichen Funktionen erfüllt – aber ich merke nicht, wenn mein Passwort gestohlen wird. Das heißt, es ändert sich für mich nichts, aber ein Dieb dieser Passwörter oder ein Hacker kann mit diesen Passwörtern dann natürlich die gleichen Bereiche betreten, die ich auch betreten kann. Um das zu verhindern, hat sich der sogenannte zweite Faktor mittlerweile durchgesetzt. Die allermeisten von uns kennen es vom Onlinebanking, da ist es schon zwingend vorgeschrieben, das heißt, da gibt es dann einen TAN aufs Handy zum Beispiel, oder eine zusätzliche Absicherung über einen zweiten Weg. Und diesen zweiten Faktor kann ich jedem nur empfehlen, weil selbst wenn Sie sehr sorgfältig mit der Auswahl Ihrer Passwörter sind und hier wirklich Passwörter ändern und viele verschiedene Passwörter verwenden, können Sie trotzdem nicht verhindern, dass dieses Passwort dort gestohlen wird, wo es verwendet wird, nämlich bei Ihrem Diensteanbieter. Und Sie merken ja nicht, dass es gestohlen worden ist.

00:08:13:29 - 00:08:25:21
Und dieser TAN jetzt in dem Fall, das ist dann quasi diese Rückversicherung, da kriege ich Bescheid, hoppla, da will wer mit meinem Konto arbeiten, über mein Konto arbeiten, und kann mich quasi mit der Bank in Verbindung setzen. Die ist schon einmal alarmiert.

00:08:25:23 - 00:08:53:09
Genau. Das gilt aber auch für die meisten Dienste, die ich im Bereich Social Media verwenden kann. Also egal, ob ich jetzt vielleicht LinkedIn oder Crossing oder andere Plattformen verwende, sobald die – und das tun mittlerweile die allermeisten – die Möglichkeit einer Zwei-Faktor-Authentifizierung anbieten, dann nutzen Sie es. Ich weiß, es ist nicht so bequem wie auf einen Link zu klicken, bei dem das Passwort schon im Browser gespeichert ist. Aber es ist tatsächlich einfach der sichere Weg.

00:08:54:00 - 00:09:04:01
Jetzt kannst du uns dann auch etwas empfehlen, wenn wir uns zu viele Passwörter merken müssen. Vielleicht noch einen zweiten Weg, eine Bestätigung. Wo soll man die alle aufheben? Wo sind die wirklich sicher aufgehoben?

00:09:04:27 - 00:10:06:10
Früher hat man gesagt, schreib keine Passwörter auf. Ja, mittlerweile tendiere ich auch dazu – wenn man sicherstellen kann, dass dieser Zettel, auf dem diese Passwörter stehen, oder dieses Heft oder wo immer sie notiert werden, quasi tatsächlich nur von mir eingesehen werden kann, dass man es sich durchaus notieren kann. Was im Büro natürlich viel schwieriger ist, weil ich halt nicht sicherstellen kann, wer tatsächlich dann Zutritt zu meinem Arbeitsplatz hat, wenn ich nicht da bin. Aber zu Hause ist es durchaus eine Option. Was sehr einfach geworden ist, ist, dass die meisten Browser mittlerweile anbieten, dass sie ein Passwort für mich speichern. Das heißt, ich muss es mir gar nicht merken, ich muss nur die Webseite aufrufen und der Browser schlägt mir dann

automatisch vor, mit diesem Usernamen und Passwort mich anzumelden. Das ist auch superpraktisch. Hat nur einen Nachteil, nämlich: Wenn es einem Hacker gelingt, mein System erfolgreich zu übernehmen, dann kann er sich natürlich überall anmelden. Das Risiko muss man sehen, dessen muss man sich einfach gewiss sein.

00:10:07:19 - 00:10:08:26
Und man vergisst es wieder ganz leicht.

00:10:08:28 - 00:11:16:26
Und man vergisst es wieder ganz leicht. Und das muss einem auch klar sein, wenn man zum Beispiel einen Password-Safe verwendet. Es gibt die Möglichkeit, dass ich ein Programm auf mein Smartphone oder auf meinen Computer lade. Das sind sogenannte Password-Safes wie etwa KeePass, in denen ich alle meine Passwörter hinterlegen kann. Und das Einzige, was ich tue, wenn ich meinen Rechner starte, ist, dass ich diesen Password-Safe öffne und dort direkt auf einen Link klicke, der mich gleich mit der Website verbindet und mich dort anmeldet. Aber auch dieser Password-Safe hat genau das gleiche Problem: Wenn ein Hacker tatsächlich Zugriff auf meinen Rechner hat, dann liest er natürlich auch dieses Masterpasswort aus, mit dem ich mich dort anmelde, und kann dann in meinem Namen alle diese Dienste zur Anmeldung nutzen. Deswegen ist die Zwei-Faktor-Authentifizierung eigentlich unerlässlich. Das ist im Moment tatsächlich eine der wirkungsvollsten Methoden, und die kann ich jedem nur ans Herz legen und empfehlen, bis wir – und darauf bin ich schon sehr gespannt – auf eine passwortlose Zukunft oder passwortlose Dienste stoßen werden. Da bin ich gespannt, was uns erwartet.

00:11:17:24 - 00:11:25:13
FaceID, TouchID, sind das auch Sicherungssysteme, sage ich mal, die man nutzen kann oder soll?

00:11:25:28 - 00:12:55:22
Ein Fingerabdruck oder eine Gesichtserkennung sind natürlich Möglichkeiten, ein Plus an Sicherheit zu erzielen. Wenn von einem Programm quasi Gesichtserkennung eingefordert wird, dann kann man schon einen sehr hohen Sicherheitsgrad damit erreichen. Biometrische Merkmale haben nur einen Nachteil: Auch biometrische Merkmale werden letztlich in binäre Dateien umgewandelt. Wenn es einem Angreifer gelingt, diese binären Dateien zu stehlen, dann kann er de facto diese binären Dateien nutzen, um sich ähnlich wie mit meinem Passwort bei einem Authentifizierungsprozess anzumelden. Und ein Passwort kann ich ändern, mein Gesicht könnte ich jetzt theoretisch auch ändern, aber ich werde deswegen ganz sicher nicht zum Chirurgen gehen. Also, das muss man einfach im Hinterkopf haben. Das gilt es abzuwägen. In gesicherten Umfeldern, hochkritischen Umgebungen wird so etwas eingesetzt. Zu Hause kennen wir es mit dem Fingerabdruck am Smartphone oder eben vielleicht auch mit der Gesichtserkennung. Superpraktisch. Hat aber zum Beispiel den Nachteil, dass natürlich jeder, der mir mein Handy wegnehmen kann, weil er körperlich stärker ist, auch sehr einfach Zugriff auf mein Handy erlangt, indem er es mir einfach vors Gesicht hält. Also, das sind alles Dinge, die man abwägen muss und die ein Plus an Sicherheit bringen, aber letztlich wieder auf den Ratschlag hinauslaufen, einen zweiten Faktor einzuführen.

00:12:56:14 - 00:13:15:00
Was auch schon passiert ist oder immer wieder vorkommt – dass Mitarbeiter zum Beispiel ihre privaten Daten, seien es jetzt Fotos, ein Adressbuch, irgendwas in diese Richtung, E-Mail-Adressen auf dem Firmen-PC speichern, weil sie glauben, dort sind die Daten wirklich sicher. Korrekt?

00:13:15:15 - 00:14:06:20
Also sicher ist einmal nichts. Das muss man mal klar aussprechen. Es gibt keine hundertprozentige Sicherheit, auch nicht in Unternehmen, die einen sehr, sehr hohen Grad an Sicherheit erzielen. Es kann immer passieren. Ja, natürlich, grundsätzlich, wenn ich mich nicht gut auskenne, wenn ich mich nicht mit Sicherheit beschäftigen will, im Unternehmen aber ein sehr gutes Team habe, tolle Infrastrukturen habe, dann ist die Wahrscheinlichkeit, dass die Daten dort, wenn sie noch mitgesichert werden – dass dort Daten sicherer sind, sehr hoch. Ich würde das aber trotzdem dennoch nur nach Rücksprache mit dem jeweiligen Unternehmen tun, indem man den Chef fragt, und dieser die IT-Abteilung fragt. Und es gibt viele Unternehmen, die bieten das als Service für ihre Mitarbeiter auch an, dass sie eben in speziell gesicherten Bereichen, wo automatisch immer weggesichert wird, ihre privaten Daten ablegen dürfen.

00:14:07:11 - 00:14:21:04
Bleiben wir vielleicht bei dem Beispiel eines kleineren Unternehmens. Was ist denn für diese an Grundwissen ganz wichtig? Was rätst du da? Sollen die auch in diese Richtung „Schutz vor Cyberattacken" geschult werden? Was gehört da zum Grundwissen dazu?

00:14:22:22 - 00:14:55:19
Also die Antwort ist ganz klar Ja, das wäre vergleichbar mit „Okay, du kriegst ein Auto und darfst am Verkehr teilnehmen". Da würde auch jeder sagen, ja, aber sicher nicht ohne dass du mal verstanden hast, wie das Auto funktioniert, und sicher nicht ohne dass du verstanden hast, wie die Regeln, wie die Straßenverkehrsordnung zu befolgen ist und wie die lautet. Ja, deswegen müssen wir alle einen Führerschein machen. Und genau das Gleiche gilt eigentlich auch für meine Mitarbeiter oder für Mitarbeiter grundsätzlich oder für alle Menschen, die quasi die Dienste und Möglichkeiten, die das Netz bietet, nutzen wollen.

00:14:55:21 - 00:16:21:29
Das heißt, eigentlich sollte ich schon in der Lage sein, ein bisschen Überblick darüber zu haben, was sind so die Basics, die ich wissen muss, und was ist so ein Verhalten, mit dem ich relativ sicher bin. Nur auf den Bauch zu achten und Augen zu und durch, das machen sehr viele Menschen. Das geht in vielen, vielen Fällen auch gut, aber in manchen Fällen eben auch nicht gut. Und dann ist der Impact schon groß. Das heißt, Mitarbeiter zu schulen bzw. als Mitarbeiter auch selbst Interesse daran zu haben, über die Systeme, mit denen man arbeitet, zu lernen – das kann nur ein Gewinn sein. Die Transformationskonsequenz der Digitalisierung zwingt uns ohnehin, lebenslang mitzulernen; wenn ich mich dem verschließe, werde ich einen sehr hohen Preis dafür zahlen. Entweder wird der Arbeitgeber irgendwann sagen, Freund, wenn du das nicht kannst, kann ich nichts mehr mit dir anfangen. Ich kann viele Dienste, viele Programme in Zukunft vielleicht einfach nicht mehr nutzen. Da biege ich ganz sicher auf die Verliererstraße ein. Also, ich sollte dem Thema gegenüber schon aufgeschlossen sein und versuchen, einfach die Basics mitzulernen. Ich muss ja nicht ein IT-Studium machen, aber ich sollte in Grundzügen schon wissen: Wie funktioniert mein System? Was braucht es, damit es sicher, halbwegs sicher funktioniert? Und vor allem, wie muss ich mich im Idealfall verhalten, damit es nicht schiefgeht? Und das mache ich beim Autofahren ja auch, ohne dass ich vielleicht so gut wie ein Verstappen oder anderer Topfahrer in der Formel 1 fahren kann. Ist ja nicht notwendig.

00:16:22:21 - 00:16:38:13
Bleiben wir vielleicht gleich bei dem richtigen Verhalten im Falle einer Cyberattacke. Oder zum Beispiel, sage ich nur, man kommt drauf, ich komm nicht mehr in mein System, das ist irgendwie verschlüsselt. Was wäre da jetzt die richtige Reaktion? Was macht man als ersten Schritt einmal?

00:16:39:20 - 00:19:38:26
Ja, wenn ich draufkomme, dass auf meinem System etwas verschlüsselt ist. Das wird meistens dadurch passieren, dass eine Nachricht auf meinem Bildschirm auftaucht, dass es so ist. Da sitz ich eigentlich schon in der Tinte, weil da ist es dem Angreifer schon gelungen, sich erfolgreich in meinem System einzunisten. Und wahrscheinlich hat er sich schon mehrere Wochen, Monate im Worst Case, darin herumgetrieben und einfach einmal schlaugemacht. Warum macht der Angreifer das? Weil er wissen will, was kann er denn potenziell von diesem Opfer erpressen. Er schaut sich an, okay, was gibt es da an Daten, die von Interesse sein könnten. Sei es, um sie weiterzuverkaufen. Sei es einfach, um Druck auf mich ausüben zu können. Vielleicht wird er irgendwann auch danach trachten, herauszufinden, wie schaut meine liquide Situation aus? Was kann er verlangen? Ich muss davon ausgehen, dass der schon länger da ist. Das Allerwichtigste in so einer Situation ist, einfach nicht vorschnell zu handeln und dem mal zu schreiben, ohne dass ich meine Optionen tatsächlich alle kenne. Wenn ich ein Mitarbeiter eines Unternehmens bin, dann werde ich mal umgehend meinen Administrator, meinen Support, meinen Vorgesetzten verständigen. Ich werde immer wieder gefragt, macht es Sinn, wenn ich meinen Computer abstecke? Ja, es ändert natürlich nichts mehr dran, dass mein Computer verschlüsselt ist. Aber ja. Also gerade für Unternehmens-PCs, aber auch für zu Hause kann man die Empfehlung sehr wohl aussprechen, den Computer mal vom Netz zu trennen. Muss mir nur klar sein, dass ich damit halt auch nicht mehr kommunizieren kann, nämlich auch nicht mehr mit dem Angreifer, aber mittlerweile kann es eh jeder über Smartphones oder andere Dinge tun. Das heißt, bevor Sie irgendwelche Gegenmaßnahmen ergreifen, schauen Sie sich mal an, welche Optionen haben Sie denn? Versuchen Sie mal zu verstehen: Was ist passiert? Das ist eigentlich eh vergleichbar mit der Schulung, die viele auch durchlaufen, wenn es brennt. Also, ich schaue mir einfach einmal an, okay, wo brennts? Was brennt? Wer ist betroffen? Es sind genau die gleichen Fragen, die Sie sich in so einem Angriffsfall auch stellen sollten. Wenn Sie die Möglichkeit haben, dass quasi die IT-Abteilung das Thema übernimmt, wunderbar. Wenn Sie privat davon betroffen sind, dann holen Sie sich ganz schnell Hilfe. Sie gehen auch nicht alleine auf Einbrecherjagd oder versuchen auch nicht selber zu löschen, wenn das Haus schon in Vollbrand steht. Das heißt, wenn Sie es nicht können, verschlimmern Sie die Situation nur. Also holen Sie sich die Leute, die Ihnen sagen können, was Sie tun sollen. Im Fall einer Ransomware-Attacke ist es ganz klar, kommunizieren Sie einmal nicht, bevor Sie nicht genau wissen, ob Sie in der Lage sind, Backups wiederherzustellen, also: Können Sie Ihre Daten sichern? Haben Sie andere Optionen oder sind Sie tatsächlich darauf angewiesen, dass Sie den Schlüssel wiederkriegen? Bevor Sie das nicht sicher sagen können, kommunizieren Sie nicht mit dem Angreifer, der hat eh Geduld. Nur ab dem Zeitpunkt, ab dem Sie angefangen haben zu kommunizieren, versucht er permanent, sie unter Druck zu setzen, und wird dann sehr ungeduldig deswegen.

00:19:40:00 - 00:19:48:12
Also, ich sage jetzt mal, wenn man wirklich Mitarbeiter in einem größeren Unternehmen ist, IT-Abteilung verständigen, Hände weg und wirklich die Fachleute auch dazulassen.

00:19:49:13 - 00:20:06:15
Genau, also informieren Sie einmal alle Kollegen rundum. Die meisten, viele von uns arbeiten in Großraumbüros, aber der allererste Schritt ist definitiv natürlich, die Experten im Haus zu informieren. Wenn die das nicht ohnehin schon wissen. Und die werden sich dann darum kümmern, die wissen im Regelfall, wie damit umzugehen ist.

00:20:07:15 - 00:20:17:13

Nun ein anderes Beispiel, mein Facebook-Account wurde gehackt. Ich merke, dass alle angeschrieben werden rundherum oder kriege fragwürdige Mails zurück, was verschickst du da? Was mache ich in dem Fall?

00:20:18:03 - 00:21:24:16
Ja, so ein Fall ist im Prinzip leicht, da muss ich keine Experten beiziehen. Da muss ich nur schauen, ob ich noch in der Lage bin, mich selbst auf meinen Facebook-Account einzuwählen. Es kann ja auch sein, dass der Angreifer das Passwort für mich ändert. Dann wird es mühsamer. Dann muss ich quasi den Beweis gegenüber Facebook erbringen, dass ich der eigentliche Inhaber dieses Accounts bin. Wenn das nicht passiert, reicht es, wenn ich mich mit meinem Facebook-Account verbinde und das Passwort ändere. Sobald ich das getan habe, werde ich natürlich versuchen, auf meinem Account selbst zu schreiben, dass ich gehackt worden bin und dass in meinem Namen vielleicht Links verschickt worden sind, mit Materialien, die ich nie verschicken würde oder die vielleicht dann sogar weiterführend auf andere Viren, Malicious Links führen. Da geht es dann einfach darum, wirklich eben Leute zu informieren. Die meisten sind dann eh skeptisch. Wenn von mir plötzlich irgendein Link verschickt wird oder vielleicht irgendeine Nachricht mit einem Thema verschickt wird, die ich sonst nie verschicken würde, da erlebt man ... Meistens kommt man dann eh so drauf, dass man eben von Freunden und Bekannten angerufen wird, hey, was hast du da gerade verschickt?

00:21:25:15 - 00:21:28:03
Hilft in dem Fall wirklich ein besseres Passwort?

00:21:28:21 - 00:22:11:26
Nein, in dem Fall hilft kein besseres Passwort, weil man muss sich immer fragen: Wie kommt denn der Angreifer zu dem Passwort? Ja, klar, wenn ich als Passwort nur 123 verwendet habe, ja, logisch. Dann kann es sein, dass er es einfach nur erraten hat. Solche Dinge passieren meistens, indem Passwörter wo gestohlen werden. Es kursieren ja Millionen Datensätze, das kann jeder für sich selbst rausfinden, ob schon Passwörter von ihm gestohlen worden sind. Da gibt es sehr spannende Seiten, wo man es probieren kann. Also, das hat nicht zwangsläufig damit zu tun. Ja, klar, wenn ich Susi1, Auto5 verwende, also ein Passwort, das einfach nicht sicher ist, das jedermann vielleicht auch einfach erraten kann – klar, dann setze ich mich da schon einem sehr hohen Risiko aus.

00:22:12:08 - 00:22:28:04
Aber was ist jetzt das Ziel, sag ich mal, von jemandem, der ein Profil bei Social Media hacken will? Das höre ich ja oft aus dem privaten Umfeld. Ich habe nichts zu verstecken, da kann jeder reinschauen. Ich hab da keine Geheimnisse drauf. Was ist das Ziel einer solchen Attacke?

00:22:28:18 - 00:24:46:05
Die Frage kann man leicht beantworten. Wobei, da würde ich vorher mit einem weitläufigen Irrtum aufräumen, nämlich, ja, bei mir gibt es nichts zu holen oder ich habe nichts zu verbergen. Wir sind als Anwender, selbst wenn Sie sagen, ich bin ein 0815-Anwender, ein superspannender Businesscase für einen Angreifer. Ein Angreifer kann immens viel von dem, was wir im Netz tun, von dem, was wir an Daten auf unseren Systemen haben, zu Geld machen. Was mein Verhalten anlangt, was die Daten anlangt, die ich auf meinen Systemen habe, meine Infrastruktur selbst kann er zu Geld machen, wenn es ihm gelingt, meinen PC, meine Webcam, meine, keine Ahnung, Steuerung vom Rasenmäher zu kontrollieren und diese dann dafür verwenden kann, Dritte anzugreifen oder das als Service Dritten zugänglich zu machen. Und das passiert, und dann verdient er damit Geld. Das heißt, mir muss klar sein, dass auch wenn Dinge für mich scheinbar keinen Wert haben, es immer jemand gibt, für den diese Dinge einen Wert haben. Das

heißt, ich werde vom Angreifer jetzt nicht als Idiot betrachtet, der sieht das völlig wertfrei. Wir sind schlicht und einfach ein Geschäftsmodell für ihn. Und wenn wir es ihm ermöglichen, dass er mit seinen Angriffen, mit seinen Zielen durchdringt, dann wird er uns bewirtschaften. Ganz einfach. Das nimmt er nicht persönlich. Das ist auch eine Möglichkeit, die er ergreift. Und nachdem er das mit vielen Tausenden überall auf der Welt machen kann, verdient er recht gut Geld damit. Warum macht man so was? Weil der Angreifer auch das Vertrauensverhältnis, das ich quasi in einer Gruppe genieße, ausnutzen kann. Ja, ganz extrem. Warum sollte er ein Kind angreifen und versuchen, die Identität dieses Kindes zu klauen? Na ja, weil das Kind halt eine Mama oder einen Papa hat, die vielleicht in einem Unternehmen arbeiten, das sein eigentliches Ziel ist. Und wenn es ihm gelingt, eine Nachricht als Tochter an den Papa zu schicken, dann ist die Wahrscheinlichkeit, dass der Papa sich das anschaut, einfach groß. Weil es ja von der Tochter kommt. Und das sind alles Dinge, die Angreifer im Kopf haben, aber Anwender im Regelfall nicht.

00:24:46:07 - 00:24:49:19
Ja stimmt, das muss einem erst einmal bewusst sein, dass man eben über andere Wege …

00:24:49:27 - 00:25:00:21
Genau. Das heißt, auch wenn ich kein Primärziel bin, mein unmittelbares Umfeld ist immer eine Art Sprungbrett zu einem Primärziel, und das macht mich zum Ziel.

00:25:01:25 - 00:25:21:23
Ich habe mir die Zahlen vom Bundeskriminalamt ein bisschen angeschaut. 46.000 Cybercrime-Anzeigen waren es im Vorjahr. Deutlich mehr als in den Jahren zuvor. Also ein Rekord, leider ein negativer. Mit welchen Attacken haben wir da jetzt eigentlich zu kämpfen? Was häuft sich denn da in letzter Zeit?

00:25:22:23 - 00:27:31:18
Na ja, das ist eigentlich leicht zu beantworten. Nachdem wir immer mehr Bereiche unseres Lebens digitalisieren, erhöhen wir damit automatisch die Angriffsfläche. Und die spektakulärsten Fälle sind natürlich jene, wo ich gehackt werde, wo meine Systeme verschlüsselt werden, wo ich zahlen muss, wo ich erpresst werde. Das ist nämlich etwas, wo man jedem nur empfehlen kann, bitte zeigt das an, auch wenn ich jetzt nicht erwarten darf, dass quasi die Staatsgewalt einrauscht mit den IT-Spezialisten und das Problem für mich löst. Das wird im Regelfall nicht passieren. Das sind die spektakulären Fälle. Wir haben aber auch Fälle, die wesentlich unspektakulärer sind, aber trotzdem einen Schaden bedeuten. Das betrifft vor allem Frauen – dass ich gestalkt werde, dass ich immer verfolgt werde, dass ich vielleicht auch gemobbt werde, das betrifft sowohl Erwachsene als auch Kinder – Kinder natürlich auch sehr stark. Und das ist auch etwas, wo man wirklich nicht zur Tagesordnung übergehen soll, weil ich oft die Reaktion erlebe, na ja, mein Gott, der wird das schon aushalten, wenn ein paar über ihn lästern. Nein, es ist leider nicht so. Wenn es früher am Schulhof passiert ist, dann habe ich wenigstens eine Ruhe gehabt, wenn ich heimgegangen bin oder weggegangen bin; im digitalen Raum verfolgt mich das, und im Worst Case 24/7, und das hat ganz massiv Impact. Das sind Dinge, die man nicht auf die leichte Schulter nehmen sollte. Diebstahl von Daten natürlich, wenn es Unternehmen sind, wo Forschungsergebnisse betroffen sind, oder andere sensitive Daten … genauso eher Phishing Mails – so was brauche ich nicht anzeigen, so was rauscht wahrscheinlich zu hunderten in meine Mailbox. Vielleicht nicht jeden Tag, aber im Lauf der Zeit. Da tut sich einfach eine Vielzahl an Fällen auf, wo Betroffene, die das merken und dann auch einen Schaden erlitten haben, dann einfach zur Anzeige schreiten. Und nachdem der Cybercrime-Markt ja unendlich schnell wächst, zehnmal schneller als der Cybersecurity-Markt – und der wächst schon enorm schnell –

und sehr, sehr viel Geld zu verdienen ist, gibt es unterschiedlichste Einschätzungen. Für 2021 sind etwa 2,5 Billionen Dollar genannt worden. Kann man sich ausrechnen, dass das nicht einfach vorbeigehen und wieder aufhören wird, sondern ein Phänomen bleiben wird, das uns eine längere Zeit verfolgt.

00:27:31:28 - 00:27:40:10
Worum geht es den Angreifern, wenn sie ein Unternehmen, wenn sie Behörden hacken, Verwaltungen hacken? Was ist da das primäre Ziel?

00:27:41:05 - 00:29:08:24
Das hängt immer von der Intention des Angreifers ab. Wenn der Angreifer an Daten und Informationen gelangen will, dann natürlich, weil er die Daten und Informationen haben will. Wenn der Angreifer Geld verdienen will, indem er das Unternehmen erpresst, dann natürlich eine Erpressung. Und eine Erpressung muss nicht immer darin liegen, dass man alle Systeme verschlüsselt und sagt, wenn ihr es wiederhaben wollt, dann zahlt, sondern es kann auch sein, dass man sagt, okay, wir haben sensible Daten von euch, zahlt oder wir veröffentlichen sie. Wir greifen eure PCs gar nicht an, oder wir haben vielleicht sensible Daten speziell über dich, und wenn du nicht willst, dass wir sie veröffentlichen, dann zahle. Oder, wenn du nicht möchtest, dass wir deine Systeme lahmlegen, dann zahle. Oder „Distributed Denial of Service"-Attacken, indem wir einfach deine Systeme überlasten und du nicht mehr Geld verdienen kannst, weil deine Webshops nicht mehr funktionieren oder weil du vielleicht nicht mehr produzieren kannst. Dann bist du natürlich vom Umstand des Betriebsausfalls oder des Produktionsausfalls betroffen, und dann musst du überlegen: Bin ich in der Lage, mich zu wehren und zu schützen oder habe ich keine Option mehr? Muss ich zahlen? Das heißt, da gibt es einen – so wie es einen sehr arbeitsteiligen und hoch spezialisierten Cybercrime-Markt gibt, gibt es eben auch da sehr, sehr viele Möglichkeiten, Geld zu verdienen. Und da sind die Menschen sehr kreativ und fantasievoll, und da sind wir mit den unmöglichsten Dingen konfrontiert.

00:29:09:11 - 00:29:15:18
Lösegeld wird in solchen Fällen meist verlangt. Soll man das zahlen, damit man weiterarbeiten kann?

00:29:15:23 - 00:29:20:15
Natürlich ist das Primärziel einmal, nicht zu zahlen. Das ist … das ist natürlich.

00:29:20:21 - 00:29:21:18
Aber kann man dem entgehen?

00:29:22:04 - 00:31:01:01
Das hängt immer davon ab. Wenn man sich gut vorbereitet hat und wenn man in der Lage ist, quasi den Machs-wieder-gut-Knopf zu drücken, jetzt sehr vereinfacht gesagt, dann wird der Angriff ins Leere führen und der Angreifer hat sich umsonst bemüht. Ich habe zwar den Aufwand, meine Daten wiederherzustellen und mir dann anzuschauen, wie sie denn überhaupt reinkommen. Aber ja, ich kann sein Geschäftsmodell quasi zerstören. In anderen Bereichen ist es schon viel, viel schwieriger. Nämlich dann, wenn ich zum Beispiel ein produzierender Betrieb bin und ich vielleicht sogar in der Lage bin, meine Systeme selbst wiederherzustellen, aber die Zeit, die ich brauche, um meine Systemintegrität wiederherzustellen, um wieder sicher produzieren zu können, beträgt mehrere Wochen oder vielleicht sogar mehrere Monate – versus der Summe, die der Angreifer fordert. Und gerade im produzierenden Umfeld sehen wir das oft, dass die Angreifer sehr wohl wissen und eine Idee davon haben, was ein Tag Stillstand kostet. Wie lange es dauert, bis die Betroffenen quasi wieder selbst auf die Beine kommen. Und da trifft man sich dann irgendwo in der Mitte. Und dann ist es natürlich ein legitimes

Mittel, auch wenn es nicht leicht ist, zu sagen: Nein, auf keinen Fall, wir zahlen nicht, weil wir unterstützen damit nur die Cyberkriminellen. Das gilt es halt immer abzuwägen. Das ist auch im Urteil des Unternehmers, ja, dem war halt sein Betriebsergebnis wieder wichtiger als der Kampf gegen Cyberkriminalität – ja, aber was sollte zum Beispiel ein Spital tun, wenn es dem passiert, oder ein Arzt tun, oder jemand, der über wirklich kritische Daten verfügt? Also da über jemanden zu urteilen, das würde ich mir nicht anmaßen und auch niemandem empfehlen. Es ist immer eine Entscheidung, die jeder für sich persönlich treffen muss, und die ist schon schwer genug.

00:31:01:21 - 00:31:24:06
Jetzt hast du gemeint, dieser Cybercrime-Markt, der wächst überdurchschnittlich schnell. Cyberkriminalität ist ja ein richtig professionelles Geschäft geworden. Wie kann man sich das vorstellen? Es gibt da Profis, für die ist das Hacken ein Geschäftsmodell, aber ich muss ja gar nicht selber Hacker sein, wenn ich sage, mir geht es jetzt darum, dieses Unternehmen zu schädigen. Ich kann das ja quasi in Auftrag geben, oder?

00:31:24:17 - 00:32:40:24
Genau. Das heißt, der Markt entwickelt sich quasi wirklich in lupenreiner Form, wenn man möchte, nämlich über Angebot und Nachfrage. Dort gibt es keine Standards und Normen, dort gibt es keine Regulative, da gibt es keine Gesetze, da kann de facto jeder machen, was er will. Und das, was funktioniert, das wächst, und zwar rasant, und wird sofort kopiert und verändert und modifiziert, und deswegen explodiert es auch, weil Menschen dann recht schnell draufkommen, ah, in dem Segment kann ich Geld verdienen. Manche Segmente explodieren so erfolgreich, dass dann fast alle davon wissen, so wie eben Erpressungs-Trojaner; andere sind verdeckter oder da weiß man vielleicht weniger darüber, aber sie funktionieren auch. So wie sich aber die Märkte entwickelt haben, haben sich natürlich auch Dienstleister für diese Märkte entwickelt. Das heißt, ich kann mir Hacker mieten, um Angriffe durchführen zu lassen. Ich kann mir Infrastrukturen mieten, um selbst irgendwo anzugreifen, wenn ich über dieses Know-how nicht verfüge. Ich kann mir Trojaner kaufen, ich kann mir Fake-Webshop-Infrastrukturen mieten. Also ich kann, wenn ich die kriminelle Energie aufbringe, ohne großes technisches Grundverständnis hier andere angreifen und schädigen und mit krimineller Intention Geld verdienen.

00:32:41:14 - 00:32:55:12
Diese Täter, die scheinen sich wirklich sehr schnell anzupassen, sind auch technisch hochentwickelt. Schaffen es jetzt Unternehmen wie deine hier eigentlich mitzukommen, mitzuhalten oder vielleicht sogar einen Schritt voraus zu sein?

00:32:55:25 - 00:33:42:13
Also, der Schritt voraus ist etwas, das man seitens der Sicherheitsindustrie natürlich gern über Marketing und Werbung kommuniziert. Aber die silberne Kugel, wenn man so will, die die Lösung für alle ist, die gibt es nicht. Einen Schritt voraus kann niemand sein. Man kann quasi immer nur versuchen, auf Augenhöhe zu bleiben und natürlich präventiv ein paar Maßnahmen zu ergreifen. Aber das ist letztlich immer eine Frage der Zeit bzw. des Aufwands, den Angreifer betreiben, um tatsächlich erfolgreich mich oder mein Unternehmen anzugreifen. Es ist nicht so, dass jeder Angreifer superintelligent ist. Der Cybercrime-Markt repräsentiert Anteile unserer Gesellschaft und da gibt es Menschen, die sehr geschickt sind und die sehr schlau sind; und dann gibt es Menschen, die sich dann vielleicht einfach ungeschickter anstellen.

00:33:42:15 - 00:33:43:00
Die es mal probieren.

00:33:43:02 - 00:36:55:00
Oder die es mal probieren und die vielleicht dabei selber Opfer werden. Das ist immer die Frage. Wow, jetzt bin ich im Darknet gewesen und habe mir das einmal angeschaut oder habe da vielleicht selber was probiert. Da kann ich jedem nur empfehlen, die Finger davon zu lassen, weil du bist schneller Opfer, als du schauen kannst, wenn du nicht weißt, was du tust. Also, das heißt, wir haben da einfach unterschiedliche Spezialisierungsgrade, wir haben da unterschiedlich schlaue Modelle. Wir haben Angriffsmodelle, auf die man sehr einfach reagieren kann. Wir haben welche, auf die man … gegen die man sich nur sehr, sehr schwer wehren kann. Wir haben ja unterschiedliche Akteure, gerade wenn ich etwa ein Unternehmen bin, das sehr sensitive Daten oder kritische Daten hat, oder eine neue Behörde bin, dann bin ich vielleicht im Fokus von staatlichen Angreifern oder von hochprofessionellen Wirtschaftskriminellen, die wirklich versuchen, hier Informationen zu stehlen, ohne vielleicht mir unmittelbar zu schaden. Also etwas, das wir kaum bewerten können, wo aber sehr, sehr viel Geld drinnen liegt, ist, wenn Angreifer einfach nur still in Unternehmen mitlauschen und einfach die Informationen, die so am Tag gesammelt werden, dann für sich nutzen können. Also wenn ich vor dem Kapitalmarkt weiß, dass ein Merger oder ein Verkauf ansteht oder eine Gewinnwarnung ansteht, dann kann ich das sehr einfach zu Geld machen, mit dem angenehmen Nebeneffekt, dass es quasi schon gewaschen ist, das Geld, und ich mir nicht am Ende den Kopf darüber zerbrechen muss, wie kriege ich es jetzt sauber auf mein Konto, ohne dass ich hintennach Wickel kriege. Das ist schon hochspezialisiert. Menschen, die sich vielleicht überlegen, na ja, das mit den Kryptowährungen, das klingt interessant, das probier ich jetzt auch einmal, und eher unbedarft an die Sache rangehen – na ja, die kann ich auch sehr einfach überlisten oder sehr einfach ausrauben, weil er sich mal schlaumachen muss, was gibt es denn da? Ja, und dann vielleicht sogar über bekannte Plattformen sein eigenes Portfolio anlegt und dann seine Kryptowährungen vielleicht in irgendein Wallet lokal auf seinem PC ablegt, statt auf irgendeinem externen Datenträger. Und beim Wallet ist es so, dass das nur mit einem Passwort gesichert ist. Und wenn ich dieses Passwort verloren habe, dann kann der Angreifer dieses Geld einfach mitnehmen, und dann ist es weg. Und dann sind wir auch wieder dort: Kann ich mich als Anwender geschickt verhalten, muss der Angreifer schlauer sein. Verhalte ich mich als Anwender unbedarft, ist es auch für den Angreifer leichter. Wie tun wir uns dabei? Indem wir uns a) eigentlich sehr nischig fokussieren. Wenn man über Cybersicherheit spricht, deckt das eigentlich schon einen immens großen Bereich ab. Ja, also gerade als Anbieter von Sicherheitslösungen gibt es mittlerweile gar keine … Selbst die weltgrößten Konzerne können Cybersicherheit in der Gesamtheit nicht mehr mit ihrem Portfolio oder ihrer Dienstleistung abbilden. Das ist völlig unmöglich, weil einfach Cybersicherheit als Querschnittsthema einfach überall mit drinsteckt. Man sucht sich die Nische, in der man sich spezialisiert, und versucht halt einfach mit sehr guten Leuten am Ball zu bleiben bzw. danach zu trachten, so wie wir das machen, also sehr ähnlich den langen Weg zu gehen, junge Talente sehr früh abzuholen und sie in ihren Fähigkeiten und Neigungen zu fordern, zu fördern und zu unterstützen. Und dann kann man natürlich auf Topleute zugreifen, und die braucht es auch.

00:36:57:02 - 00:37:16:05
Eine Aufgabe von dir oder deinem Unternehmen ist es ja auch, Schwachstellen aufzudecken in den Systemen. Wo hakt es denn noch bei Unternehmen? Was sind denn so Schwachstellen, wo du sagst, das könnte man wirklich ganz leicht ausbessern? Und egal, ob es jetzt große oder kleine Unternehmen sind, ich glaube, es sind alle davon betroffen.

00:37:16:22 - 00:39:11:19
Ja, da muss man sich mal vor Augen halten, dass Schwachstellen in Unternehmen ja quasi vielseitig sind. Das hat ja nicht nur mit der Infrastruktur, die dieses Unternehmen

betreibt, zu tun, sondern auch mit den Mitarbeitern in dem Unternehmen, mit dem Verhalten des Unternehmens, mit den Produkten des Unternehmens. Das muss man ja gesamtheitlich sehen. Und viele Unternehmen oder gute Unternehmen betrachten es ja schon gesamtheitlich und wissen, dass quasi eine technisch-organisatorische Maßnahme, wie ein bestimmtes Sicherheitssystem zu installieren, eigentlich der letzte Schritt ist. Der erste Schritt ist einfach mal, sich zu überlegen: Wo bin ich denn überhaupt angreifbar? Was sind denn die wirklich kritischen Unternehmensbereiche, die ich schützen muss? Kann ich das aufteilen? Das heißt, kann ich das segmentieren und quasi auf Inseln aufteilen, die ich im Krisenfall über Wasser halten kann? Also da gibt es viele, viele, viele, viele Zugänge dazu. Das macht es sehr schwierig für Unternehmen, mit einer Strategie das alles abzubilden – weil es nicht etwas ist, wo man sagen kann, ja, okay, da haben wir mal großartig Hirnschmalz investiert und das haben wir umgesetzt. Hakerl, erledigt. Nein, das ist etwas, was sich ja tagtäglich ändert, weil die Systeme, die wir nutzen, sich auch tagtäglich ändern auf der einen Seite; auf der anderen Seite wir tagtäglich neue Systeme in unsere Netzwerke einbringen, neue Apps installieren, gerade im Bereich Netzwerksegmente, wo es jetzt nicht mehr um klassische IT, wie wir sie kennen – nämlich um die PCs auf unseren Schreibtischen und die Server in unseren Serverräumen – geht, sondern Stichwort Smart Home, Smart Grid. Denken Sie es weiter durch, da tut sich eine solche Vielzahl an weiteren möglichen Angriffsflächen auf, die man halt in seine Sicherheitsüberlegungen alle mit einfließen lassen muss. Und das ist etwas, was permanent wächst, das, auch wenn man es optimieren kann, letztlich eine nie endende Geschichte ist. Und dessen muss man sich bewusst sein.

00:39:11:24 - 00:39:32:00
Ja. Also, das heißt, darüber haben wir eingangs auch gesprochen, up-to-date bleiben. Vor drei Jahren ein Antivirusprogramm installiert zu haben wird nicht mehr reichen. Du kennst sicher auch Unternehmen, die gehackt wurden, die geschädigt wurden. Was erzählen dir denn da so die Verantwortlichen? Wie geht es ihnen damit? Und was würden sie heute anders machen?

00:39:33:00 - 00:41:36:20
Das ist ganz, ganz unterschiedlich. Das ist wirklich überraschend, dass es Unternehmen gibt, die aus diesen negativen Erfahrungen lernen und wirklich strukturiert daran arbeiten, dass solche Fehler oder solche Angriffe in Zukunft minimiert oder vermeidbar sind. Und andere, die quasi achselzuckend zur Tagesordnung übergehen und sagen, passiert, ja. Und viele, viele Mischformen mittendrin. Okay, dann erhöht man halt den Security-Etat der IT, aber Primärfokus vom Topmanagement ist es trotzdem nicht. Das verstehe ich bis zu einem gewissen Grad auch, weil die natürlich strategisch getrieben sind, von Eigentümerinteressen getrieben sind, von Mitbewerbern, Märkten getrieben sind. Aber so wie viele, nämlich auch vom Top Executive Management, zumindest von der Awareness her schon verstanden haben, uhh, Cybersecurity ist vielleicht doch ein Chefthema, müssen viele von dieser Awareness erst ins Handeln kommen. Es gibt schon einige, die das tun, solche, die schon betroffen waren. Solche, die noch nicht so – zumindest nicht so medienwirksam – betroffen waren. Aber da gibt es trotzdem noch sehr viele, sehr, sehr viele Möglichkeiten, sei es auf Behördenseite oder bei Unternehmen. Das eine, eben das Bewusstsein, mmm, könnte sein, dass da jetzt doch das Cybercrime-Risiko immer höher wird, hin zum tatsächlich Tun. Und tatsächlich tun heißt eben nicht eine isolierte Maßnahme, nämlich na ja, okay, gib mir da mal ein paar Tausender für irgendein Sicherheitssystem frei. Das können Sie sich sparen. Es braucht ganz andere Zugänge. Es braucht nämlich den Zugang, dass Sie die Leute, die Cybersicherheit in Ihrem Unternehmen ansteuern, tatsächlich sehr, sehr nahe an die Chefetagen heranführen und diese in alle Unternehmenstätigkeiten eingebunden werden, weil Sie nur mit einem gesamtheitlichen Ansatz oder gesamtheitlichen Zugang hier halbwegs sinnvolle Ergebnisse zusammenbringen. Alles, was da quasi in dislozierter

Kleinarbeit erbracht werden muss, ist natürlich besser als nix, aber ist unterm Strich viel zu wenig.

00:41:37:01 - 00:41:44:20
Trifft es eigentlich kleinere Unternehmen mehr als größere? Wer steht da mehr im Visier der Angreifer?

00:41:44:26 - 00:43:35:03
Es trifft in Summe natürlich viel mehr kleinere Unternehmen, a) weil es mehr gibt und b) weil immer nur die Großen in den Medien stehen. Wenn irgendein KMU an der tschechischen Grenze oben davon betroffen ist, dann hat das natürlich nicht den Werbewert oder dieses Medieninteresse, wie wenn es ein internationaler Konzern ist, eine Behörde oder eine Länderorganisation ist. Ja, klar, natürlich sind KMU viel, viel mehr davon betroffen. Und KMU tun sich ja auch viel, viel schwerer als große Unternehmen und Organisationen, die eigene Fachkräfte haben, die eigene Abteilungen dafür haben, die eigene Pläne und Strategien haben, wie man Sicherheit in diesen Unternehmen realisiert. Das ist für KMU definitiv schwerer. Das heißt aber nicht, dass KMU jetzt die Flinte ins Korn werfen müssen. Die KMU profitieren wirklich davon, dass sie wesentlich kleinere Organisationseinheiten haben und damit überschaubarer sind. Und damit ist es auch, unter Anführungszeichen, vielleicht sogar einfacher, mal ableiten zu können, okay, was brauche ich denn, wie muss denn meine Sicherheitsstrategie ausschauen? Da kann man eigentlich schon mit sehr wenigen Maßnahmen sehr viel erreichen, und man ist schon ganz gut dabei, wenn man versucht, diese 80 Prozent zu erreichen. Und die erreicht man relativ schnell, und da kann man noch was draufpacken, indem man schlicht und einfach mal schaut, okay, was leisten denn meine Diensteanbieter, die ich sowieso brauche. Was leistet mein Internet Service Provider zusätzlich an Sicherheitsdiensten? Und wenn ich die in Anspruch nehmen kann, dann muss ich mich a) gar nicht darum kümmern, weil das machen die Spezialisten dort, und b) die können es sicher besser als ich und, nachdem es quasi ein Shared Service ist, wesentlich günstiger als ich. Und das sind Dinge, wo man eigentlich mit sehr einfachen Maßnahmen schon sehr viel erreichen kann.

00:43:35:28 - 00:44:03:09
Die Pandemie kann man ja, glaube ich, als Brandbeschleuniger für Cybercrime bezeichnen. Stichwort Homeoffice – das wollte ich noch ansprechen als mögliche Schwachstelle. Wie ist das, wenn man zu Hause arbeitet, aber trotzdem zu Firmendaten Zugang hat bzw. den Zugang bekommt, selber aber vielleicht in einem eher ungesicherten Netzwerk unterwegs ist – nutzen das die Hacker auch aus, um so über verschiedene Wege zum eigentlichen Angriffsziel zu kommen?

00:44:03:22 - 00:45:37:14
Ja, natürlich! Weil es für einen Hacker natürlich viel einfacher ist, quasi den PC von der Jeti Tant daheim zu knacken, als vielleicht die Firmen-Firewall der Nationalbank oder der Telekom, weil das ist schon wesentlich schwieriger. Das ist natürlich etwas, was das Ganze beschleunigt hat, und etwas, das uns als Heimanwender in unserem Homeoffice ganz klar zu Zielen macht, weil wir mit unseren Infrastrukturen halt auch Zugriff in unseren Unternehmen haben. Nachdem wir die PCs zu Hause aber meist für viele Dinge nutzen, nämlich nicht nur zum Arbeiten, ist die Chance, dass Sie dort quasi erfolgreich angegriffen werden, schon sehr hoch. Vielleicht sogar noch, wenn der PC von mehreren Personen im Haushalt genutzt wird, und, und... Dessen muss man sich einfach bewusst sein, dass solche Arbeits-PCs, die eigentlich für einen Unternehmenseinsatz aufgesetzt, entwickelt worden sind, halt dann vielleicht nicht unbedingt die Spiele- und Surf- und Ach-was-gibt-es-im-Internet-zu-entdecken-PCs sein sollten, weil ich dort natürlich auch das Risiko habe, mir etwas einzutreten, was ich nicht möchte. Dieses Verhalten muss ich

natürlich auch mitbringen, also diese Awareness, dieses Bewusstsein dafür. Und immer mehr Unternehmen versuchen auch, dieses Bewusstsein von Mitarbeitern zu schulen, sei es eben gegen Phishing-Attacken, sei es gegen das Klicken von Anhängen in E-Mails, sei es gegen Telefonanrufe, mit denen versucht wird, Passwörter zu stehlen. Also, da hat man schon erkannt, dass man gegensteuern muss.

00:45:38:06 - 00:45:46:09
In Sachen Hilfe und Unterstützung bei einem Cyberangriff – vielleicht noch mal konkret, wie kann mir mein Netzbetreiber oder mein Serveranbieter helfen?

00:45:47:01 - 00:46:43:00
Eigentlich sehr, sehr gut, weil er ja derjenige ist, der mir den Zugang ins Internet überhaupt ermöglicht. Und damit hat er auch die Chance und die Möglichkeit, sehr erfolgreich Angriffe abzuwehren. Und die allermeisten Unternehmen machen es. Vor allem die Telekom Austria ist da sehr, sehr früh mit sehr guten Lösungen am Markt gewesen. Ich kann mich erinnern, im Jahr 2000, 2000 war das schon, hat man die ersten Mailfilter bei der Telekom implementiert. Da war man wirklich weit, weit voraus, und das hat sich ganz toll entwickelt. Wenn man sich das Portfolio anschaut, das von der A1 Telekom mittlerweile angeboten wird, wo ich als Unternehmen eigentlich nur mehr ein Hakerl machen muss oder mir den Experten aus der Telekom ins Haus holen kann und er mir sagt, welche Dienste und Services es gibt – da hat man es Unternehmen eigentlich schon sehr einfach gemacht. Da muss man als Unternehmen eigentlich nur mehr sagen, ja, okay, ich schaue mir das an.

00:46:43:09 - 00:47:11:09
Jetzt sind wir wirklich, glaube ich, schon viel schlauer geworden in Sachen Schutz vor Cyberkriminalität, vor Cyberangriffen. Du hast vorhin erzählt, ihr seid immer auf der Suche nach Topleuten, um auch in dieser Branche da mitzukommen, mit dieser Entwicklung mitzuhalten bzw. vorauszuarbeiten. Wie schaut es denn da jetzt eigentlich mit Ausbildungsmöglichkeiten für Cybersecurity-Experten aus? Das ist ja ein neues Berufsfeld, welches das Ganze eigentlich mit sich gebracht hat, oder?

00:47:11:20 - 00:47:18:21
Schlecht. Das muss man leider so sagen, wie es ist, und ich kann es auch recht einfach belegen.

00:47:20:00 - 00:47:22:21
Informatikstudium reicht mal nicht, oder?

00:47:24:19 - 00:50:24:24
Also, ein Informatikstudium geht natürlich einmal in die richtige Richtung. Alles, was in den Bereich des Aufbaus von Medienkompetenz, von digitaler Kompetenz geht, geht schon in die richtige Richtung, weil man Sicherheit nicht als quasi isolierte Disziplin betrachten darf, sondern es gesamtheitlich sehen muss. Ich muss ja, wenn ich mich mit Sicherheit beschäftige, eben auch wissen, okay, welchen Risiken sind meine Kollegen und Mitarbeiter ausgesetzt und wie kann ich sie dazu bringen, diesen Risiken quasi aus dem Weg zu gehen oder sie zu vermeiden. Also, das hat ja jetzt nur wenig mit dem Informatikstudium zu tun. Wenn man tatsächlich, wenn man so will, Sicherheitsexperten ausbilden möchte, dann fangen wir eigentlich erst sehr spät an. Sehr spät heißt, bis auf wenige Ausnahmen – es gibt da eine Handvoll HTLs, wo das wirklich schon sehr, sehr gut gemacht wird. Die HTL in Kaindorf zum Beispiel, in der Steiermark, der Rennweg, Sankt Pölten. Da gibt es wirklich schon sehr, sehr gute Ansätze. TGM in Wien, ich hab jetzt sicher etliche vergessen, aber es gibt glücklicherweise schon ein paar. Aber es ist trotzdem so, dass, wenn man so will, eine professionelle Security-Ausbildung eigentlich

erst auf Universitätslevel anfängt. Wenn man es dann mit dem Spitzensport vergleicht und überlegt, wir fangen an, unsere Spitzensportler erst mit 19, 20 zu fördern – dann ist der Zug abgefahren. Da müsste man viel, viel früher anfangen und viel, viel früher heißt eigentlich ab dem Zeitpunkt, ab dem wir unseren Kindern die Möglichkeit geben, an diesem Netz, an diesem Internet teilzuhaben. Und das passiert meistens schon im Volksschulalter, wenn Mamis ihren Kindern Rechenzentrums-Äquivalente, nämlich Smartphones, in die Hand drücken. Durchaus mit der guten Absicht, ja, mein Kind soll mit dieser Technologie aufwachsen. Das ist ja eh gut, das will ja jede Mama und jeder Papa, dass das Kind da im Zuge der Chancengleichheit sich mit diesen Themen beschäftigt. Was die allermeisten Eltern aber nicht wissen, ist, welchen Risiken sie ihre Kinder dabei aussetzen. Und da muss man nachschärfen, und ich betrachte das als super Chance für Eltern, hier gemeinsam mit ihren Kindern zu lernen und zu erfahren, was gibt es da? Worauf muss man aufpassen? Und das fängt bei Nutzungszeiten an, bei konsumierten Inhalten, wie lange spiele ich, was spiele ich, welche Risiken bieten Messenger-Dienste wie TikTok oder Snapchat? Ist mein Kind dem Risiko ausgesetzt, dass sich vielleicht Erwachsene meinem Kind annähern, was ich so nie erlauben würde? Das sind alles Dinge, die man wissen sollte. Und das sind durchaus auch Dinge, die man für sich selbst dann einmal verwenden kann, wenn man da ein bisschen Sicherheit hat und wenn man ein bisschen Verständnis hat. Wenn man da ein bisschen Verständnis entwickelt hat, dann hat man selbst mehr Sicherheit, dann traut man sich vielleicht auch mehr zu, dann kann man Situationen besser einschätzen, dann wird Sicherheit auch spannender, weil Sicherheit ist wie alles im Leben, wenn man sich damit beschäftigt und mal ein bisschen was erfährt darüber und weiß, ja, dann ist es gar nicht mehr so ein spanisches Dorf, und dann ist vieles ja in sich schlüssig und logisch erklärbar, und dann macht es auch richtig Spaß.

00:50:25:09 - 00:50:45:02
Aber wo fischst du zum Beispiel nach Talenten? Wo schaut ihr euch da um? Oder wie stoßt ihr auf jemanden, wo du sagst, oh, hoppla, den könnte man vielleicht noch in die richtigen Bahnen lenken, nämlich zu unserem Nutzen bzw. zum Nutzen für Unternehmen, um sie vor Cyberangriffen zu schützen. Wo, ja, wo stößt man auf solche Leute?

00:50:45:14 - 00:52:32:22
Ja, indem wir Wettbewerbe für Cybersicherheitstalente anbieten. Die Austria Cyber Security Challenge ist mit Sicherheit der bekannteste. Die European Cyber Security Challenge ist eine europäische Erfolgsgeschichte – heuer im siebten Jahr übrigens das Finale Mitte September in Wien. Wir erreichen dort in der Qualifikation schon über 17.000 junge Burschen, überwiegend leider noch viel weniger Mädchen. Dieser Anteil bei Mädchen liegt schwankend, aber nicht über 5 Prozent. Da haben wir wirklich noch einiges Verbesserungspotenzial. Das heißt, dort findet man dann schon sehr rasch junge Menschen, die hohe Affinität zum Thema Sicherheit haben, weil sie in der Lage sind, solche Wettbewerbe zu spielen, die wollen es wirklich, weil die sind alle ein Produkt ihrer intrinsischen Motivation, weil die Schulen, wo sie das lernen können, die gibt es so nicht. Es gibt keine Schulen, wo du jetzt lernst, wie du Unternehmen hackst, das bringen sich die Leute alles selber bei. Das ist ein Punkt, wo wir viele gute Leute finden. Ein anderer Punkt ist natürlich der, dass wir viele Forschungskooperationen mit Universitäten eingegangen sind, aber auch, dass wir schon lange am Markt sind. Und gerade bei jungen Menschen, die mit dem Thema Malware-Analyse, Incident Response, wie wehre ich Hacker ab, wie kann ich selber quasi Unternehmen hacken, bekannt sind und die sagen, dort kann ich ausschließlich das machen oder auf einem sehr hohen Niveau ein Level machen – man kann nicht nur selber viel lernen, sondern auch wirklich coole Sachen –, die kommen dann zu uns, und das ist natürlich eine Schwierigkeit und eine Herausforderung, die andere Unternehmen in der Form dann vielleicht nicht so haben,

weil sie halt in anderen Bereichen sehr erfolgreich und attraktiv sind und diesen Sicherheitsexperten aber trotzdem brauchen.

00:52:34:17 - 00:53:12:17
Vielleicht noch ein Thema zum Abschluss: Cybercrime, darüber haben wir jetzt viel gesprochen. Cyberwar, ein Cyberkrieg, ist ein anderer Begriff. Da geht es dann wirklich um Angriffe auf Infrastrukturen, auf Länder, auf Stromnetze, auf Gesundheitssysteme. Und auch das erleben wir tatsächlich schon. Wo stehen wir da oder wie weit kann dieser Cyberwar eskalieren? Wie wahrscheinlich sind denn wirklich digitale Angriffe jetzt auch außerhalb von Kriegsgebieten, derzeit Ukraine, zum Beispiel in Europa? Ist Österreich für so einen Angriff gerüstet?

00:53:13:04 - 00:54:00:02
Hmm. Also Cyberwar ist ja quasi nur eine Klammer für eine Vielzahl von Aktivitäten, die staatliche Akteure oder Personen im Auftrag von staatlichen Akteuren durchführen. Man kann von einer kalten Phase sprechen, die ohnehin schon längst stattfindet. Also, wenn man so will, ein kalter Cyberkrieg, den gibt es, seitdem wir Informationssysteme betreiben. Seitdem Staaten anfangen, entsprechende Kapazitäten aufzubauen, wo wir jetzt, wenn man so will, in einer Reconnaissance-Phase sind, sprich, wo Staaten einfach einmal das Netz kartografieren und schauen, okay, wer macht dort was, wer hängt dann an wem dran? Versuchen, Zugänge in Unternehmen aufzubauen, das heißt, schlicht und einfach Kontrolle über die digitalen Infrastrukturen ganzer Länder zu erlangen.

00:54:00:10 - 00:55:31:09
Das passiert laufend. Ja, das macht der Angreifer ja nicht als, keine Ahnung, vorbereitende Angriffe des Staates X, sondern das ist halt irgendein Angriff. Und ja, dann hat der Forensiker oder der Sicherheitsspezialist vor Ort die Schwierigkeit, herauszufinden, wer steckt hinter dem Angriff, und meistens wirds halt Hakerl drunter, und dann wars halt ein Cyberkrimineller. Da nutzen staatliche Akteure schon sehr geschickt dieses Grundrauschen, das Cybercrime mit sich bringt. Eine heiße Phase erleben wir derzeit ganz sicher im Bereich der Ukraine, auch Litauen ist aktuell davon betroffen, weil es eben den Korridor Kaliningrad gesperrt hat, wo tatsächlich Angreifer, Behördenvertreter, Banken, kritische Infrastrukturen angreifen und deren Services zum Erliegen bringen, mit all den Konsequenzen, die das dann für die jeweilige Gesellschaft dort hat. Das ist sicher ein Aspekt, der uns in Zukunft noch sehr, sehr stark beschäftigen wird. Alleine der Umstand, dass sich die großen Staaten oder fast alle Staaten der Welt nun darauf einigen haben können, irgendeine Art Konvention, eine Art Regelwerk für Cyberwar zu entwickeln, zeigt schon, wie erfolgversprechend dieses neue Schlachtfeld, wenn man das so in dieser neuen Dimension sehen will, von vielen Staaten gesehen wird. Und es ist einfach auszurechnen und einfach zu erklären: Je abhängiger wir in all diesen Infrastrukturen werden, umso größer ist der Impact eines erfolgreichen Angriffs. Und damit wird es in Zukunft ganz sicher bestimmender Faktor für uns alle werden.

00:55:31:11 - 00:55:34:16
Und da sollte man wirklich darauf vorbereitet sein.

00:55:34:18 - 00:55:38:19
Auch das ist etwas, wo man definitiv vorbereitet sein muss.

00:55:39:05 - 00:55:39:20
Sind wir auch darauf vorbereitet?

00:55:40:28 - 00:56:06:10

Mit Sicherheit noch nicht ausreichend genug. Da haben wir wirklich noch viele, viele Kilometer vor uns, und da wird auch diskutiert darüber. Da gibt es schon die eine oder andere Maßnahme, da gibt es schon ein Bewusstsein. Aber in dem Ausmaß, in dem es nötig wäre, definitiv nicht. Da sind wir wirklich noch sehr, sehr tiefenentspannt. Die Insel der Seligen wird schon nicht so wild werden.

00:56:06:19 - 00:56:08:29
Vielen Dank für all die Infos, Joe. – Sehr gern.

00:56:09:06 - 00:56:16:11
Alles Gute weiterhin für die Zukunft. – Vielen Dank. – Und ich gehe jetzt gleich updaten. Alles, was geht.

00:56:19:02 - 00:56:44:26
Daten also immer sichern. Updates nicht ignorieren. Ruhig ein bisschen misstrauisch sein und doppelt nachfragen und auch ohne Scheu auf Profis in Sachen Schutz vor Cybercrime zugreifen. Zusammengefasst wohl die wichtigsten Tipps, die wir von Joe Pichlmayr gehört haben, um bei einem Cyberangriff gewappnet zu sein und richtig zu reagieren. Ich hoffe, es war für euch genauso spannend wie für mich selbst. Danke fürs Zuhören und bis zum nächsten Mal!