#ConnectLife – der Podcast von A1
Cybersecurity: alles über Hackerangriffe und wie ihr euch schützt
Transkript

Natascha Kantauer-Gansch: Es ist ganz wichtig, dass wir bei unerwarteten Nachrichten sehr, sehr vorsichtig sind und nicht klicken, auch wenn wir im Stress sind oder es eilig haben. Hier ist ganz wichtig, immer zu hinterfragen, bin ich mit dem Unternehmen eigentlich in Kontakt oder habe ich hier Kontakt gehabt? Also wirklich noch mal ganz gezielt darauf zu schauen, von welchem Unternehmen werden die Nachrichten versandt – und wie könnte mich das eigentlich betreffen?

Richard Malovic: Wir schützen auf der Netzebene. Und was am wichtigsten ist, wir fokussieren uns auf die Benutzerfreundlichkeit. Das heißt, wir machen alles, dass der Kunde geschützt wird, ohne dass etwas installiert oder eingestellt wird.

Martina Hammer: Mitten in der Nacht am Bahnhof ist es nicht so unsicher wie tagsüber im Internet. Hacker und Cyberangriffe machen Unternehmen, Behörden, ganzen Städten und natürlich auch uns normalen Usern immer mehr zu schaffen. Fast 36.000 Fälle sind im Vorjahr registriert worden, das zeigt der Cybercrime-Report des Innenministeriums. Zum Vergleich: 2010 waren es 4.000. Im Internet wird spioniert, es wird betrogen und erpresst. Viele Firmen in Österreich wappnen sich gegen die Gefahr aus dem Netz. Aber was können private User und UserInnen wie du und ich tun? Wie können wir uns vor Cyberattacken schützen? Das kläre ich mit meinen heutigen Gästen: Richard Malovic ist CEO und Founder von Whalebone, einem Cyber Security Provider und Mitglied am A1 Startup Campus. Und mit dabei ist heute auch A1 CCO Natascha Kantauer-Gansch. Ich bin Martina Hammer. Ihr hört #ConnectLife – den Podcast von A1, und jetzt geht's los!

Hallo Richard, fein, dass wir es geschafft haben. Herzlich willkommen bei #ConnectLife, unserem Podcast.

Richard Malovic: Hallo!

Martina Hammer: Richard, wir gehen gleich mitten rein ins Thema. Ich glaube, ziemlich jeder oder jede, die ein Smartphone besitzen, haben im Vorjahr vor Weihnachten eine Fake-SMS oder eine Fake-E-Mail von einem Paketzusteller bekommen. Was verbirgt sich denn hinter dieser Masche? Und was passiert im schlimmsten Fall, wenn ich auf diesen Link klicke oder zustimme?

Richard Malovic: Ja, alle haben wahrscheinlich solche Nachrichten in den letzten Tagen erhalten. Ich selber heute in der Früh. Also, was passiert da? Die Angreifer nutzen die Neugierde und Eile von uns allen aus. Und gehen dann weiter in die Attack. Immer wieder bist du neugierig, was für ein Paket du erhalten hast. Was steht da? Was habe ich vergessen? Was hat mein Mann bestellt? Und gehst in den meisten Fällen gleich auf die Website des Packet-Service. Aber das ist ja wahrscheinlich schon eine Fake-Website, und da geht alles schon los. Irgendwelche schadhafte Software wird runtergeladen oder du wirst deine Daten eingeben und im Worst Case werden deine Daten dann auch gestohlen. Nicht nur Name, Nachname, auch Adresse, Rufnummer, Bankomatkarte, und natürlich wird dann auch manchmal Geld gestohlen.

Martina Hammer: Durch dieses Annehmen oder Zustimmen installiere ich also eine schädliche Software. Was kann ich denn jetzt tun, wenn ich zugestimmt habe? Wenn ich diese Fake-App oder -Software installiert habe auf meinem Handy?

Richard Malovic: Also, zuerst: Du musst nicht einmal zustimmen. Ja, vielleicht hast du gar nicht bemerkt, dass du etwas falsch gemacht hast. Du hast einfach die Lieferzeit verändert. Eine Bestätigungs-SMS ist dann gekommen und du glaubst also, alles ist in

Ordnung, aber deine Daten sind schon weg. Aber zurück zu deiner Frage: Wenn ich schon weiß oder falls ich weiß, dass ich eigentlich etwas Schadhaftes installiert habe, dann muss ich schnell in den Flugmodus gehen, das WLAN ausschalten und ruhig meine Daten irgendwohin anders kopieren. Wenn ich die nicht verlieren will. Das heißt, Daten-Backup alleine oder mit einer Hilfe. Aber was wichtig ist, offline [speichern].

Martina Hammer: Wie werde ich jetzt diesen Trojaner wieder los? Kann ich? Muss ich mein Smartphone entsorgen? Kann ich es nicht mehr benutzen oder kann ich es wieder benutzen?

Richard Malovic: Also, auf jeden Fall muss ich es nicht entsorgen. Wichtig ist, dass es für eine bestimmte Zeit offline bleibt und dann eigentlich in die Factory-Settings geht. Das heißt, erst Daten-Backup und dann Factory-Settings – und dann kann man es wieder verwenden.

Martina Hammer: Wie kann mir denn da mein Mobilfunkanbieter helfen, muss ich den auch informieren?

Richard Malovic: Also, ich glaube, jeder Funkanbieter wird sich freuen, wenn du ihn informierst, weil natürlich die Daten oder die Attacke … die Informationen über die Attacke werden gesammelt, und dann kann man sich verbessern auf Netzbetreiberseite. Aber für dich selbst … Nein, ich glaube, es ist schon genug, wenn du dein Handy mal wieder installierst.

Martina Hammer: Wie gehen jetzt diese Cyberkriminellen bei diesem Angriff auf private User vor? Wer entscheidet, eine SMS geht jetzt an diese Nummer? Warum? Warum werde gerade ich das Opfer?

Richard Malovic: Ja, es gibt natürlich mehrere Gründe, warum gerade du das Opfer bist. Nummer eins – ja, es kann Zufall sein. Nummer zwei, du bist eigentlich ein Produkt von jemandem, der schon eine Database vorbereitet und diese mehreren Kunden verkauft hat. Und diese Database kann dann wieder zufällig zusammengebastelt sein. Oder die Database weiß schon, dass du eine bestimmte Schwäche in deinem Handy oder in deinem Rechner hast. Das heißt, du kannst im Web diese Kontakte kaufen oder diese Database kaufen, mit einer bestimmten Beschreibung. Zum Beispiel diese Liste von, ich weiß nicht, zig Kunden oder zig Rufnummern oder zig E-Mail-Adressen, die eine bestimmte Schwäche haben. Und dann können natürlich die Angreifer ziemlich gezielt wirken.

Martina Hammer: Diese Angreifer, noch einmal zurück zu ihnen. Wo sitzen denn diese Kriminellen? Wer ist das? Kommt man denen überhaupt auf die Spur?

Richard Malovic: Ja, also, die sitzen überall. Leider. Es wäre jetzt schwierig, zu sagen, dass sie aus einem bestimmten Land oder einer Region kommen. Das ist eigentlich überall. Aber natürlich, fast jeder Angriff ist irgendwie verfolgbar. Aber die Kapazität der Polizei oder von irgendjemandem, der sich damit beschäftigen möchte, ist begrenzt. Das Problem ist, dass man eigentlich die Ressourcen nur für die größten Tiere hat. Das ist eine eigene Wirtschaft. Du kannst eigentlich verschiedene Attacken „as a Service" bestellen, also Ransomware as a Service, Spam as a Service usw. Ja, die haben sogar Free Trial. Das heißt, du kannst zum Beispiel, ich weiß nicht, 1.000 E-Mails als Free Trial haben, oder einen Monat DDoS oder so was. Das ist ja wirklich eine klassische Industrie geworden.

Martina Hammer: Sprechen wir jetzt vielleicht auch darüber, ganz wichtig, wie ich mich denn schon im Vorfeld vor solchen Cyberangriffen schützen kann. Du bist ja ein Mann vom Fach, CEO, Gründer von Whalebone, einem Cyber Security Provider. Was macht ihr denn genau?

Richard Malovic: Wir schützen auf der Netzebene. Und was am wichtigsten ist, wir fokussieren uns auf die Benutzerfreundlichkeit. Das heißt, wir machen alles, dass der Kunde geschützt wird, ohne dass etwas installiert oder eingestellt wird, weil damit wird die Adoption viel höher. Mehr Leute verwenden dann Security und werden auch geschützt, also ungefähr zehnmal mehr, als wenn sie etwas installieren müssen. Also, wir schützen auf der Netzebene, ohne dass etwas installiert wird.

Martina Hammer: Also, ihr schützt auf der Netzebene. Das heißt, verbunden zu sein schützt.

Richard Malovic: Genau. Also eigentlich, wenn man sich die Angriffe und die Bedrohungen vorstellen möchte: Alles braucht Konnektivität und alles läuft durch die Konnektivität. Wir arbeiten mit dem Netzbetreiber zusammen und stellen dort sicher, dass die verdächtigen Anfragen innerhalb der Konnektivität gecheckt werden und gegebenenfalls auch gestoppt werden. Und wir bauen dann ein Produkt daraus. In Österreich ist das A1 Net Protect, und wir können die meisten Attacken schon präventiv stoppen, bevor sie das Gerät erreichen können.

Martina Hammer: Sind dann alle meine Geräte, die mit dem Internet verbunden sind, durch Whalebone geschützt?

Richard Malovic: Genau, alle Geräte. Und das ist besonders wichtig, wenn du dir jetzt dein Zuhause vorstellst und denkst, okay, was alles ist schon verbunden? Und in der Zukunft wird natürlich auch dein Auto komplett verbunden, komplett online sein. Alles „connected means protected", aber: Connected bedeutet auch Gefahr.

Martina Hammer: Wie bist du eigentlich auf den Bereich Cybersecurity gekommen? Was fasziniert dich denn daran?

Richard Malovic: Also, mich fasziniert das Impact, was wir machen können. Dank der Zusammenarbeit mit den Netzbetreibern können wir eigentlich Millionen – und langfristig wollen wir eigentlich eine Milliarde Kunden schützen. Und das ist für mich das Interessanteste. Und warum ich und Cybersecurity? Dank meiner Freundschaft mit dem Mitbegründer von Whalebone, der ein Fachmann in Cybersecurity ist. Und der ist einfach gekommen und hat gesagt, hey, du hast ja Erfahrung mit internationalem Vertrieb und Geschäftsaufbau, komm, machen wir es zusammen.

Martina Hammer: Die Liste der Cybercrime-Delikte ist ja relativ lang. Spyware, Phishing – ich glaube, das sind geläufige Begriffe. Botnet, Ransomware gibt es da auch noch. Was tritt denn am häufigsten auf bei privaten Usern?

Richard Malovic: Also, relativ überraschend, die meisten Attacken fangen mit einer URL oder mit einer Domain an, auf die geklickt wird. Also, einfach gesagt, in der Fachsprache heißt es Phishing. Die meisten Attacken fangen mit Phishing an, und dann geht's weiter.

Martina Hammer: Das heißt, da kommt dann, sei es eine SMS oder eine E-Mail, „Bitte bestätigen Sie Ihre Informationen von der Bank", das kennt man ja schon mittlerweile.

Richard Malovic: Genau so was in die Richtung. Aber solche Verknüpfungen oder solche Links kann es eigentlich überall geben, auf einer Website, in einer Werbung, fast überall. Und dann, wenn ich mal klicke, dann steigen die weiteren Begriffe, die du eigentlich gesagt hast, ein. Dann kommt eine Software, die runtergeladen wird, und das kann dann vielleicht eine Ransomware-Software werden, oder eine andere.

Martina Hammer: Okay, du bist mit Whalebone ja auch am A1 Startup Campus vertreten. Wie lange denn schon? Und welche Vorteile haben sich da ergeben?

Richard Malovic: Es werden bald fünf Jahre, und wir sind sehr froh, dass wir diesen Schritt gemacht haben, weil A1 hat uns wesentlich dabei geholfen, dass unser Produkt skalierbar wird. Also, historisch haben wir mit kleineren Netzbetreibern gearbeitet, und die Zusammenarbeit mit A1 und die gemeinsame Entwicklung hat uns geholfen, dass wir wirklich ein World-Class A1 Telco Produkt gebaut haben.

Martina Hammer: A1 Net Protect, dieses Produkt hast du schon erwähnt, das hat A1 zusammen mit euch entwickelt, diesen Cyberschutz. Vielleicht kannst du noch mal kurz erklären, wie genau funktioniert dieses Produkt?

Richard Malovic: Ja, gerne. Also, A1 Net Protect schützt genau auf der Netzbetreiberebene, ist da präventiv, teilweise auch reaktiv, und muss nicht installiert werden. Also, A1 braucht nur ein Ja vom Kunden. Kann man natürlich online, per Telefon oder auch im Shop aktivieren und kostet 1 Euro 90 pro Monat.

Martina Hammer: Pro Monat. Und ich brauche keine spezielle Software zu Hause oder irgendwas am Handy?

Richard Malovic: Genau, so einfach ist es.

Martina Hammer: Okay. Ich sag vielen Dank, Richard, für dieses Gespräch und all die interessanten Details und Informationen.

Richard Malovic: Vielen Dank! Schönes Wochenende noch!

Martina Hammer: Danke, alles Gute.

Wir haben es von Richard gehört: Ein Cyberangriff kann jeden oder jede von uns treffen. Damit komme ich zu meinem nächsten Gast, Natascha Kantauer-Gansch. Natascha ist Chief Customer Officer Consumer bei A1 und verantwortet 1.600 Mitarbeiter, die sich um die Anliegen, Wünsche und Sorgen von Privatkundinnen und -kunden kümmern. Und sie war auch schon in Folge 13, „Customer Centricity", mein Gast. Das gibt es natürlich zum Nachhören.

Natascha, schön, dass wir es wieder geschafft haben. Heute zum Thema Cybersecurity. Herzlich willkommen!

Natascha Kantauer-Gansch: Vielen Dank für die Einladung. Ich freue mich auch, dass wir heute wieder im Gespräch sind.

Martina Hammer: Natascha, du und dein Team, ihr befasst euch ja tagtäglich mit zahlreichen Kundenwünschen, Anfragen, Anliegen. Das werden hunderte sein, vielleicht noch mehr. Gibt es denn auch in letzter Zeit vermehrt Fragen zum Thema Cybersecurity?

Natascha Kantauer-Gansch: Ja, die gibt es definitiv. Wir alle verlagern ja unser Leben sowohl privat als auch beruflich immer mehr ins Netz. Wir kaufen online ein, wir nutzen Onlinebanking, wir nutzen unterschiedliche Plattformen und wir laden auch viele von unseren Erinnerungsmomenten online hoch. Und diese vielen neuen Möglichkeiten, die es gibt, die führen natürlich auch dazu, dass die Anzahl der Angriffe und die Anzahl der Möglichkeiten für Cyberangriffe laufend zunehmen. Wir sehen, dass unsere Kunden heute schon wesentlich sensibler sind, dass sie uns häufiger kontaktieren und nachfragen, ob SMS, E-Mails, Calls, die sie von A1 erhalten, auch wirklich von A1 versandt wurden. Also, die Kunden sind schon besser informiert, und das ist einfach darauf zurückzuführen, dass in den letzten Monaten die Anzahl der Angriffe zugenommen hat. Natürlich auch, weil die Medien laufend darüber berichten, dadurch verzeichnen wir auch mehr Kontakte dazu. Für uns war auch wichtig, hier noch einmal gemeinsam mit dem Marktforschungsinstitut

Integral eine Studie durchzuführen, um ein besseres Gefühl dafür zu bekommen: Wie gut sind denn die Kunden nun wirklich schon … oder die Menschen überhaupt schon informiert? Und die Ergebnisse waren für uns schon sehr überraschend. Wir haben festgestellt, dass ein Großteil der Befragten wirklich sehr gut informiert war. Die meisten kennen einfach die wichtigsten Angriffsarten. Sie können die Begriffe sehr gut zuordnen und sie haben auch schon ein gutes Gefühl dafür, wie sie sich eigentlich schützen können. Also das heißt, das Thema wird medial sehr gut unterstützt. Und nachdem viele Kunden auch – und wir kennen alle die FluBot-Attacke –Betroffene waren oder sind, sehen wir schon vermehrt Anfragen auch bei uns, eigentlich bei allen Kanälen, sowohl im Service Center als auch in den A1 Shops.

Martina Hammer: Melden sich dann auch direkt Cybercrime-Opfer bei euch? Wenn ja, was erzählen sie denn? Oder was möchten sie denn gerne wissen von euch? Du hast es kurz angesprochen, es geht vielleicht um SMS, die verschickt werden …

Natascha Kantauer-Gansch: Wenn sich die Opfer direkt bei uns melden, dann fragen sie natürlich, was wir als A1, als Provider, unternehmen, also welche Vorkehrungen wir treffen, dass wir unsere Kunden auch schützen für die Zukunft. Das ist uns auch ein großes Anliegen, es gibt hier Möglichkeiten, das machen wir, aber die Kunden möchten auch besser verstehen und unterstützt werden, welche Maßnahmen sie selber ergreifen können, um sich zu schützen. Und hier unterstützen wir auf der einen Seite mit einem sehr geschulten Team, also mit unseren MitarbeiterInnen, die wir noch mal speziell auf das Thema geschult haben in den letzten Monaten. Und wir bieten auch Produkte an, wie zum Beispiel A1 Net Protect oder den A1 Cyberschutz oder A1 Internetschutz. Diese Produkte unterstützen einfach auch noch mal unsere Kunden vor weiteren Schäden.

Martina Hammer: Angenommen, ich werde jetzt Opfer einer Phishing-Attacke, lade mir einen Trojaner aufs Handy, der dann massenweise SMS verschickt. Was soll oder kann ich als A1 Kunde dann tun?

Natascha Kantauer-Gansch: Also, was wir immer empfehlen, ist, dass man sofort den Flugmodus aktiviert, denn durch die Aktivierung des Flugmodus unterbricht man alle Verbindungen. Das heißt, auch die mobile Datenverbindung wird unterbrochen und man verhindert auch, dass SMS versandt werden. Und darum geht es ja genau. Das ist die erste wichtige, schnelle Maßnahme, Verbindungen zu unterbrechen, die im Hintergrund laufen. Und die zweite wichtige Maßnahme ist, das Handy dann … das Mobiltelefon auf die Werkseinstellungen zurückzusetzen und erst danach wieder zu aktivieren. Das sind die zwei Maßnahmen, die wir immer empfehlen und die auch den größten Schutz bieten.

Martina Hammer: Solche Trojaner verursachen doch auch Kosten. Wer kommt denn dafür auf?

Natascha Kantauer-Gansch: Das ist eine sehr gute Frage. Grundsätzlich müssen natürlich die Kunden dafür aufkommen. Aber wir haben natürlich gesehen … gerade bei den ersten FluBot-Attacken waren viele Kunden betroffen und teilweise auch verzweifelt, weil sie überhaupt nicht wussten, was hier passiert. Es wurden diese Fake-Paket-SMS versandt und viele Kunden haben dann auch auf die Links geklickt und damit Berechtigungen vergeben. Und dadurch sind natürlich auch höhere Kosten entstanden. Hier war es uns sehr, sehr wichtig, dass wir den Kunden auch entgegenkommen, dass wir hier individuelle Lösungen finden. Und wir haben auch die Kosten zum Großteil für die Kunden dann übernommen.

Martina Hammer: Den Cyberschutz von Kundinnen und Kunden hast du schon kurz erwähnt. Was macht denn A1 jetzt schon für diesen Cyberschutz für seine Kunden?

Natascha Kantauer-Gansch: Ja – nachdem wir beobachtet haben, dass die Anzahl der Angriffe einfach sehr stark steigt und immer mehr Kunden auch betroffen sind, haben wir diese sogenannte Cybercrime-Sperre eingeführt. Worum geht es hier? Sobald wir erkennen, dass von einem Mobilfunktelefon plötzlich vermehrt SMS in großer Anzahl versendet werden, aktivieren wir diese Sperre für dieses eine Mobilfunktelefon, also für diese eine Rufnummer. Und damit wird verhindert, dass weitere SMS versendet werden können. Es wird auch verhindert, dass aktive Anrufe getätigt werden können, und es wird eben diese mobile Datenverbindung unterbrochen. Und das bedeutet dann, dass die Kunden sich … also, die Kunden werden auch von uns noch mal informiert per SMS, dass sie sich bitte an uns wenden. Die Kunden können natürlich auch trotz dieser Sperre immer Notrufanrufe tätigen. Das ist ganz wichtig. Und sie können auch uns erreichen. Also unsere Serviceline. Wir bitten die Kunden, dass sie uns kontaktieren und sobald sie das gemacht haben, setzen wir gemeinsam mit den Kunden eben das Mobiltelefon auf die Werkseinstellungen zurück, und dann deaktivieren wir die Sperre wieder, weil dann ist der Schutz wieder gegeben und das Risiko minimiert.

Martina Hammer: Welche Lösungen könnt ihr darüber hinaus noch anbieten?

Natascha Kantauer-Gansch: Ich habe es schon kurz erwähnt – wir haben uns natürlich in den letzten Monaten noch einmal intensiv damit beschäftigt, welche sogenannten Cybersecurity-Produkte relevant wären für unsere Kunden und welche wir hier anbieten sollten. Und ich möchte drei nennen. Das ist auf der einen Seite A1 Net Protect. A1 Net Protect ist ein Produkt, das die Kunden davor schützt, dass eine Schadsoftware installiert wird, beziehungsweise auch vor betrügerischen Seiten. Es ist sehr, sehr wichtig und wird von den Kunden auch sehr, sehr gut angenommen. Ein zweites Produkt ist der A1 Internetschutz. Hier geht es eher darum, dass die Daten am PC geschützt werden vor Schadsoftware, vor Viren, vor Trojanern, die wir alle gut kennen. Dieses Produkt haben wir gemeinsam mit dem österreichischen Unternehmen Ikarus entwickelt. Und dieses Produkt, wenn man sich dafür entscheidet, kann man auch auf bis zu fünf Windows-Geräten nutzen. Also ist es auch für die ganze Familie dann letztendlich geeignet. Und dann? Es passiert ja manchmal trotzdem, dass es auch zu einem finanziellen Schaden kommt. Ich glaube, wir alle kennen das: Wir haben online eingekauft und plötzlich wird das Paket nicht zugeschickt. Oder es kann auch passieren, dass Betrüger dann letztendlich Zugang zum Onlinekonto erlangen, dass sie also Daten stehlen können. In dem Fall ist es uns wichtig, dass wir auch eine Versicherung anbieten, und das ist der A1 Cyberschutz, wo wir den finanziellen Schaden teilweise übernehmen, der entstanden ist, bzw. auch Kosten übernehmen, wenn es zu einem Datenverlust gekommen ist und man die Daten wieder erzeugen muss. Da entstehen auch Kosten, und die werden auch teilweise übernommen. Das ist der A1 Cyberschutz für Opfer, die betroffen sind, und wenn ein finanzieller Schaden entstanden ist.

Martina Hammer: Du hast gesagt, die Leute werden sensibler. Werden diese Angebote auch gut angenommen?

Natascha Kantauer-Gansch: Ja, definitiv. Wir beraten, wie gesagt, hier viele Kunden, und wir sehen natürlich, dass die Kunden, obwohl sie gut informiert sind, einen unterschiedlichen Informationsstand haben; und das Thema Cybersecurity oder das Thema Cyberkriminalität, das löst natürlich auch immer Angst aus, und deswegen ist es uns wichtig, dass wir über verschiedene Kanäle im persönlichen Gespräch, in den A1 Shops, im telefonischen Gespräch, aber auch über Kampagnen, die wir dann im digitalen Bereich versenden, unsere Kunden laufend informieren und hier die Produkte gut erklären. Und wir sehen, dass die Produkte wirklich gut angenommen werden.

Martina Hammer: Also auch Information und Prävention sind dabei ganz wichtig. A1 Net Protect, das war auch schon Thema bei meinem Gespräch mit Richard. Dieses Tool ist ja nicht nur in Österreich schon im Einsatz, oder?

Natascha Kantauer-Gansch: Ja, das ist sehr erfreulich. In Österreich haben wir gestartet und war der Launch des Produkts. Und inzwischen wird das Produkt auch in Mazedonien, in Kroatien, in Serbien und in Bulgarien erfolgreich verkauft. Es wächst, es wächst. Genau.

Martina Hammer: Liebe Natascha, kannst du vielleicht abschließend … kannst du uns noch, sozusagen, die Top Five Tipps für Privatpersonen nennen, um nicht Opfer einer Cyberattacke zu werden?

Natascha Kantauer-Gansch: Ja, sehr gerne. Und ich gebe diese Tipps nicht nur für unsere Kunden, sondern auch an viele Freunde und Bekannte weiter, weil sie eigentlich ganz einfach sind und uns wirklich schützen können. Ich glaube, es ist ganz wichtig, dass wir bei unerwarteten Nachrichten sehr, sehr vorsichtig sind und nicht klicken, auch wenn wir im Stress sind oder es eilig haben. Hier ist es ganz wichtig, immer zu hinterfragen, bin ich mit dem Unternehmen eigentlich in Kontakt oder habe ich hier Kontakt gehabt? Also wirklich noch mal ganz gezielt darauf zu schauen, von welchem Unternehmen werden die Nachrichten versandt und wie könnte mich das eigentlich betreffen? Ein zweiter wichtiger Tipp ist, keine Anhänge in verdächtigen E-Mails zu öffnen. Das heißt, wenn ich mir nicht sicher bin, ob die E-Mail auch wirklich vom richtigen Absender kommt, auf keinen Fall einen Anhang öffnen, weil das führt meistens dazu, dass die Schadsoftware installiert wird, und dann beginnt ein größeres Problem. Der dritte Tipp, den ich immer gerne weitergebe, ist, dass man auf Formulierungen achtet. Wenn man hier genau darauf schaut, dann erkennt man schon, dass immer wieder Tippfehler enthalten sind, was eigentlich unüblich ist. Wir alle wissen, welche Möglichkeiten es gibt, heutzutage Tippfehler zu vermeiden. Und gerade bei diesen SMS und so weiter merkt man, dass hier Tippfehler bewusst eingearbeitet werden. Auch das kann ein wichtiger Hinweis sein, dass man besonders vorsichtig ist. Der vierte Tipp von mir ist, immer die URL oder Domain zu kontrollieren. Das heißt, man hat doch ein gutes Gefühl, wenn da jetzt .at oder .com steht. Und plötzlich, wenn da zusätzliche Zahlen eingearbeitet werden oder Buchstaben, dann ist das auch wiederum ein Hinweis, dass es sich um einen Betrüger handeln könnte und dass der Absender einfach gefälscht ist. Ja, und der fünfte Hinweis: die E-Mail-Adresse des Absenders. Ich glaube, das ist auch ein guter Tipp, da genau darauf zu schauen, ob diese E-Mail-Adresse bekannt ist oder nicht, ob eben hier auch noch mal Buchstaben oder Zahlen eingefügt wurden. Und das kann wirklich helfen, bevor man die E-Mail öffnet, größeren Schaden zu vermeiden. Das sind die fünf Tipps – wenn man die ein bisschen im Kopf hat, die können schon sehr dabei unterstützen, Angriffe abzuwehren, sage ich jetzt. Erfordern nicht so eine große Expertise, nur ein bisschen mehr Aufmerksamkeit, Sensibilität. Und wichtig ist, dass man diese Tipps auch immer wieder wiederholt. Wir versuchen, die auch über unsere Social-Media-Kanäle zu kommunizieren, auch in den Gesprächen mit unseren Kunden noch einmal genau zu erläutern und zu versenden. Und ich glaube, damit … wenn wir das alle gemeinsam machen, auch mit den Medien, dann können wir einfach die Bevölkerung, ja, educaten, ausbilden und den Angreifern das Leben ein bisschen schwermachen.

Martina Hammer: Ein bisschen Misstrauen ist also angebracht. Es sind oft so komische Formulierungen, eine komische Ansprache, wo man dann ein bisschen nachdenkt.

Natascha Kantauer-Gansch: Ganz genau, so ist es ja, wenn die Kunden unsicher sind. Wie gesagt, wir sind jederzeit für sie da, und das sehen wir wirklich auch, dass sie uns dann auch ganz konkret kontaktieren, wenn sie eine E-Mail mit Verdacht erhalten.

Martina Hammer: Alles klar. Dann sage ich vielen, vielen Dank für die vielen Infos, Natascha. Vielen Dank für das Gespräch.

Natascha Kantauer-Gansch: Danke, alles Gute. Ciao.

Martina Hammer: Cybersecurity, Cybercrime. Ein Thema, das mittlerweile jeden und jede von uns betrifft – und da waren einige gute Tipps heute dabei, um sich vor Cyberattacken zu schützen. Ich hoffe, es war interessant für euch. Danke fürs Zuhören und bis zum nächsten Mal.