„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 21, 30.06.2022:
Hacking gegen Cyber-Attacken?
Im Gespräch mit White Hats.

Moderation: Ute Lange, Michael Münz
Gäste: Immanuel Bär, Tim Schughart, ProSec
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lange: Hallo und herzlich Willkommen zu einer neuen Folge von „Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

***Münz**:* Und ich bin Michael Münz. In dieser Folge sprechen wir mit Vertretern einer Berufsgruppe, die in diesem Podcast schon häufig vorkam, aber nie im guten Licht. Wir sprechen heute mit zwei Hackern. Bevor wir das tun, werfen wir einen kurzen Blick zurück in unsere Podcast-Pause. Ute, wie war die für dich?

Lange: Pause klingt zwar immer nach wenig Arbeit, das war es aber nicht. Ich bin zum ersten Mal seit vielen Jahren umgezogen. Ich hatte sehr unterschätzt, wie viel Arbeit das ist, und musste mich von dieser ganzen Arbeit mit dem Ergebnis, eine schöne neue Wohnung zu haben, mit viel Yoga ein bisschen erholen. Ich freue mich, dass wir heute wieder zum Aufnehmen des Podcast zurückkehren und uns wieder sehen.

***Münz**:* Geht mir genauso. Die Podcast Pause war zwar lang, aber das bedeutet nicht, dass ich in der Zeit nicht genug zu tun gehabt hätte. Der Urlaub kommt bei mir erst noch. Eine Podcast-Pause heißt nicht, dass die Themen, die wir hier behandeln nicht stattgefunden haben. Ich habe auch immer wieder geschaut, was es an Themen gibt, wie ich mich davor schützen kann, dass mir was Unangenehmes in der digitalen Welt passiert. Ein Punkt, den ich aus den vergangenen Wochen mitgenommen habe und gerne hier mit aufnehmen wollte, ist der zweite Bericht zum digitalen Verbraucherschutz des BSI. Der besagt, dass Verbraucherinnen und Verbraucher in Deutschland immer häufiger von Cyber-Angriffen und IT-Sicherheitsvorfällen betroffen sind, auch ohne direkt angegriffen zu werden.

Lange: Kannst du ein paar Beispiele nennen, was dieses ‚indirekt betroffen sein‘ bedeutet?

***Münz**:* Es gab häufiger Cyber-Angriffe auf Kommunalverwaltungen, Krankenhäuser, Unternehmen oder andere Institutionen, wobei auch Verbraucherinnen und Verbraucher beziehungsweise Patientinnen und Patienten betroffen waren. Beispielsweise, weil das Bezahlsystem nicht funktioniert oder eine OP verschoben werden muss. Das heißt, selbst wenn andere angegriffen wurden, bin ich am Ende der Kette der Leidtragende. Das kommt

immer häufiger vor. Das BSI sieht da zwar vorrangig die Hersteller und Anbieter von digitalen Produkten in der Verantwortung, weil sie unsere Daten schützen sollen, aber auch wir als Verbraucherinnen und Verbraucher sind gefordert und dazu angehalten, uns proaktiv besser zu schützen, indem wir zum Beispiel bei der Auswahl der Dienste und Produkte ein besonderes Augenmerk auf die Informationssicherheit setzen.

Lange: Dazu passt ganz gut das, was ich gesehen und natürlich gleich getestet habe, und zwar der HPI Identity Leak Checker vom Hasso-Plattner-Institut. Damit kann ich prüfen, ob meine Identität irgendwo in einem Datenleck aufgetaucht ist. Das bedeutet, dass ich eine E-Mail eingebe und relativ schnell eine recht bunte Übersicht bekomme. Bei mir waren ein paar grüne, ein paar gelbe und auch ein paar rote Felder, die besagten, dass die eine E-Mail, die ich getestet habe, irgendwo bereits unberechtigterweise in einem Datenleck im Internet aufgetaucht ist, und es besser wäre, wenn ich mein Passwort und andere Dinge checke. Ich habe dir das geschickt. Hast du das auch getestet?

Münz*:* Ich habe das auch gemacht und die Ergebnisübersicht in unterschiedlichen Farben bekommen. Diese hat mich sehr an die Zahnpasta-Werbung aus meiner Kindheit erinnert, in der ein Kind fröhlich strahlend einen Kaugummi kauen muss, den Mund wieder öffnet und alles farbig wird. So fühlte sich das für mich auch an. Ein paar meiner E-Mail-Adressen waren in Leaks drin, das heißt es war an vielen Stellen rot. Ich habe die Passwörter geändert, um sicher zu gehen, dass damit nichts passiert, aber stelle gerade wieder ein erhöhtes Aufkommen an Spam fest, wobei ich denke: „Das kann nicht sein! Wo haben die meine Adresse her?“. Das kommt oft vor in letzter Zeit. Außerdem kriege ich jetzt wieder Anrufe von Nummern, die ich nicht kenne. Ich gehe aus Prinzip nicht mehr dran, weil ich keine Lust habe, mit irgendeiner Maschine zu sprechen, die mir versucht, irgendwas anzudrehen oder sich als Microsoft vorstellt, um auf meinem Computer einzuloggen. Das will ich nicht und bin deswegen gerade wieder erhöht wachsam bei solchen Themen.

Lange: Bevor wir mit der Aufnahme gestartet haben, habe ich so einen Anruf bekommen. Der war zwar von Anonym, wo ich normalerweise nicht rangehe, aber irgendwie hatte ich diesen Impuls. Es war ein Fake-Anruf, deswegen dachte ich „Nein, danke, kein Interesse. Ich lege jetzt auf“. Das führt mich zu einer anderen Geschichte, die ich in den letzten Wochen gelesen habe, und zwar selbst so ein Bundesamt wie das BSI ist von solchen kriminellen Aktivitäten nicht ausgeschlossen beziehungsweise wird sogar für diese missbraucht. Es geht um Spoofing-Anrufe mit der BSI-Rufnummer. Ich musste nachgucken, was das ist. Spoofing bedeutet im englischen „Parodie“. Jemand imitiert das BSI oder andere Unternehmen, vor allem seriöse Behörden, ruft an und möchte sensible und persönliche Daten abgreifen, indem man sich als jemand ausgibt, der normalerweise vertrauenswürdig ist. Das BSI ist darauf aufmerksam geworden, warnt davor und empfiehlt, sofort aufzulegen, wenn ein solcher Anruf eingeht. Mehr dazu findet ihr in den Shownotes. Das scheint im Moment breit umzugehen, also man kann nur vorwarnen.

Münz*:* Dazu passt das Ergebnis einer Studie von der Initiative Deutschland sicher im Netz. Deren Index besagt, dass Verbraucherinnen und Verbraucher derzeit schlechter vor Cyber-

Angriffen geschützt sind als in den vergangenen Jahren. Das hängt damit zusammen, dass es viel mehr Angriffe als in der Vergangenheit gibt, und wir nicht damit hinterherkommen, den Schutz auf dem jeweils nötigen Niveau zu halten. Wir haben in früheren Folgen, v.a. in der über Router, oft den Fall: „Ich habe ein neues Gerät, richte das einmal ein und gucke das nicht mehr an“, gehabt. Man muss am Ball bleiben, Updates installieren oder beispielsweise in diesem E-Mail-Fall Passwörter ändern, wenn wir feststellen, dass wir in Leaks stecken. Das ist etwas was, viele Menschen überfordert und viele fühlen sich nicht sicher. Sechs von zehn Befragten haben angegeben, dass sie mehr Hilfe im Netz benötigen. Ich finde gut, dass wir heute Menschen dabeihaben, von denen wir sicherlich viele Tipps kriegen, wie wir im Alltag weiterhin digital sicher sein können.

Lange: Ich freue mich auch sehr. Wir haben heute Immanuel Bär und Tim Schughart zu Gast. Sie betreiben das Unternehmen ProSec und unterstützen unter anderem Firmen beim Thema IT-Sicherheit auf eine Art und Weise, über die wir von ihnen mehr erfahren möchten. Wir freuen uns, dass ihr da seid. Hallo Immanuel und hallo Tim.

Bär: Servus! Danke für die Einladung.

Schughart: Vielen Dank, dass wir dabei sein dürfen.

Münz*:* Wir sind auf euch bei einer Veranstaltung aufmerksam geworden und dachten, dass wir bei euch zum Thema Hacking viele der Fragen loswerden können, mit denen wir uns in den bisherigen Folgen von Update Verfügbar befasst haben. Mögt ihr euch beide kurz vorstellen?

Bär: Ich fange vielleicht an, weil ich ein Stück weit an dieser Bekanntschaft schuld bin. Ich habe Ute bei einer Veranstaltung eines großen Telekommunikationsanbieters kennengelernt. Ich bin Mitgründer bei ProSec und beschäftige mich intensiv unter anderem mit den Bereichen Faktor Mensch und Social Engineering. Ein Teil meines Jobs liegt auch darin, dass ich versuche, komplexe Sachverhalte von Hacking und IT-Security in möglichst einfache und verständliche Metaphern und Haupt- und Nebensätze zu übersetzen. Das ist auch einer meiner Spitznamen – ‚Übersetzer‘ oder ‚Interface‘. So habe ich mich damals bei Ute vorgestellt.

Lange: Das hat gut funktioniert. Ich habe damals schon viel von dir mitgenommen. Hallo Tim!

Schughart: Hi! Ich knüpfe an, weil ich ganz froh bin, Übersetzer heute dabei zu haben. Ich habe eher den technischen Hintergrund und genau genommen den Hacker-Hintergrund. Es hat sich seit der dritten Klasse bei mir angefangen. Ich bin auch Mitgründer bei ProSec.

Münz*:* Bevor wir in das Thema einsteigen, haben wir für euch, wie auch für alle unseren vorherigen Gästen, eine Entweder-oder-Frage. Wir wollen von euch wissen, ob ihr lieber eine Stunde ungeschützt im Netz surfen oder eine Stunde lang ungespritzt beim Zahnarzt im Stuhl sitzen würdet?

Schughart: Letzteres habe ich schon gemacht. Das ist eine einfache Frage für mich.

***Münz**:* Du bist offensichtlich hart im Nehmen. Wie ist es bei dir, Immanuel?

Bär: Ich würde mich auch wahrscheinlich zwangsläufig für Letzteres entscheiden müssen, weil ich immer nicht so gut auf die Narkotika beim Zahnarzt anspringe. Deshalb bin ich da auch schon zwangsläufig hart im Nehmen.

Schughart: Aber ich würde mich trotzdem dafür entscheiden.

***Münz**:* Alles klar. Danke euch.

Lange: Ihr, liebe Zuhörerinnen und Zuhörer, könnt das nicht sehen, aber Immanuel und Tim tragen weder Skimützen vor ihrem PC, noch haben sie ihre Hoodies weit ins Gesicht gezogen. Das sind Klischees in der Berichterstattung über eure Berufsgruppe, die Hacker. Wir kennen diese Gruppe bislang nur als Halunken. Es handelt sich entweder um Erpresser, Script-Kiddies oder staatlich beauftragte Bösewichte. In welche Kategorie passt ihr beide?

Schughart: Das legale Berufsbild. Der Beruf dazu ist Security Analyst. Das, was wir als Hacker im offensiven Bereich machen, ist dann Penetration-Testing, also das Hacken von Systemen, das aber legal per Auftrag abläuft. Ich finde den Begriff „staatlich beauftragte Bösewichte“ spannend, weil das immer eine Frage der Perspektive ist. Wenn ich etwas für einen Nachrichtendienst in Deutschland unter deutschem Auftrag mache, bin ich für die Deutschen nicht der Bösewicht, aber vielleicht für die andere Nation.

Bär: Ich habe eine Frage an Ute. Kannst du dich noch erinnern, was ich anhatte, als wir uns kennengelernt haben?

Lange: Ich glaube einen Hoodie.

***Münz**:* Eine Skimütze?

Bär: Nein, es war sehr warm und ich habe eine Art Sakko und Jeans getragen. Das nur zu unserem ersten Kennenlernen.

Lange: Also auch kein Klischee getroffen. Also, ihr seid beauftragt und seid legal. Was heißt das konkret? Was macht euch anders? Tim hat schon den Perspektivwechsel angesprochen. Was ist euer Alltag?

Bär: Wir fangen vielleicht damit an, warum wir damals angefangen haben. Tim hatte die ursprüngliche Idee und hat mich gefragt, ob ich Lust habe, als Übersetzer in das Projekt, das jetzt ein tolles Unternehmen und ein tolles Team geworden ist, mit einzusteigen. Ein wichtiger Aspekt war dabei für uns die Frage: „Können wir es schaffen, mit Hacking Menschenleben zu retten?“. Zu dem Zeitpunkt gab es schon den einen oder anderen Bericht, bei dem zum Beispiel Krankenhäuser oder bestimmte kritische Infrastrukturen, von denen Menschenleben abhängen, stark unter Beschuss sind. Dabei war ein Ansatz: warum nicht mit den destruktiven Fähigkeiten Schutzmechanismen entwickeln, indem wir böse Hacker nutzen, aufklären und detektieren? Das ist etwas Grundsätzliches, dass uns anders macht, und warum wir damit angefangen haben. Es ist sehr wichtig, dass, Ethical Hacker nicht nur

auf dem Papier steht, sondern, dass man es mit einem ethischen Ansatz und einem korrekten moralischen Kompass macht.

Schughart: Uns unterscheidet die Moral, in der wir in der Gesellschaft alle groß geworden sind, und, ich hoffe, die gleichen identischen Werte. Wir wollen zwar Geld verdienen, weil wir Unternehmer und Beschäftigte sind, die auch Gehalt haben wollen, aber tun das nicht auf Kosten anderer, also wir wollen unseren westlichen Werten dabei treu bleiben. Das ist der Unterschied.

Münz*:* Es ist wahrscheinlich nicht so, dass es einen Studiengang oder eine Ausbildung für das gibt, was ihr gemacht hat. Wahrscheinlich seid ihr Autodidakten. Wie seid ihr zu dem geworden, was ihr jetzt seid? Was habt ihr als Äquivalent zu einem Ausbildungszertifikat an der Wand hängen?

Schughart: Ganz viele Zertifikate. Du hast richtig gesagt, dass es keine klassische Ausbildung gibt, zumindest nicht in dem Bereich. Es gibt mittlerweile Studiengänge, die ein paar Sachen davon aufknüpfen, aber keine Ausbildung, um einen Hacker im legalen Bereich zu werden. Ich habe in der dritten Klasse angefangen. Zu meiner Zeit gab es CDs, auf denen es manchmal Gutscheine für 90 Freistunden ISDN gab, die natürlich schnell weg waren. Das erste, was ich gemacht habe, war Lernen zu programmieren, um Codes zu probieren. Dann hatte ich quasi meine erste Internet Flat. Das war einer der ersten Hacks, die ich gemacht hatte. Da kam das Interesse her, das zu tun, vor allem durch das Wachstum vom persönlichen Können, wobei man nur Internetquellen bedient, und Trial and Error macht. Durch Ausprobieren und Scheitern wird man besser. Zertifikate? Es gibt ganz viele. Das eine Unternehmen der Wirtschaft fordert Zertifikat X, das andere Y. Das BSI hat auch strenge Zulassungsvoraussetzungen für den Penetration-Tester. Die sind alle mal mehr, mal weniger fundiert oder stellen einen Wildwuchs dar, weil es diese klassische Ausbildung leider immer noch nicht gibt. Deswegen habe ich vieles gemacht: viele Ausbildungen, viele Zertifikate bekommen, auch studiert, aber nicht genau diesen Bildungsgang.

Bär: Vielleicht auch von meiner Seite eine kleine Ergänzung dazu: Ich möchte an der Stelle noch ein kleines Klischee auflösen. Es ist in den seltensten Fällen so, dass man wie im Hollywoodfilm morgens aufwacht, sich den Hoodie anzieht, dann kommt ein Sonnenstrahl, und man denkt sich, man wird jetzt Hacker. Ich bin beispielsweise in Nigeria groß geworden, der erste Teil meiner Vita war nicht so entspannt. Ich musste von dort fliehen und wollte danach über gewisse familiäre Zusammenhänge Informationen beschaffen. Ich habe mit 13 oder 14 mit Informationsbeschaffung über meine Vergangenheit angefangen. Nicht weil ich dachte, dass ich irgendwann eine Firma gründen kann oder in einem Hacker-Film auftauche, sondern weil mich einfach bestimmte Sachen interessiert haben. So fing das mit Informationsbeschaffung und dem Einstiegspunkt Faktor Mensch an.

Münz*:* Gab es bei euch beiden einen Punkt oder ein Erlebnis, bei dem ihr entschieden habt, dass ihr nicht wie viele andere Schaden anrichten, sondern genau das Gegenteil tun möchtet? Gab es einen bestimmten Anlass dafür, auf die „andere Seite“ zu gehen?

Schughart: Man kann sehr einfach illegal damit Geld verdienen. Viel einfacher als es legal zu tun, weil man als Firma Faktoren wie Projektmanagement etc. braucht, die ein Hacker nicht braucht. Es ist mir aufgefallen, dass es in der Szene auf Masse gehackt wird. Man weiß nicht, was man hackt, wenn man viel Geld verdienen will. Man geht einfach auf ganz viele Systeme, automatisiert und verschlüsselt die und fängt danach an zu erpressen. Irgendeiner zahlt schon. Weil man nicht weiß, wen man trifft, kann es auch sein, das vielleicht Krankenhäuser gehackt worden sind oder andere Einrichtungen. Man hat keine moralische Intention, etwas Böses zu tun aber hat es am Ende doch getan. Nur wenn man es auf Masse macht, verdient man viel Geld. Das war der Moment, als ich gesagt habe, dass ich es nicht machen kann. Es ist gänzlich gegen das, wofür ich stehe und leben will. Ich verdiene lieber nichts und weiß lieber nicht, ob ich erfolgreich werde. Es hat Jahre gedauert, bis ich in den Bereich beruflich reingegangen bin, weil ich es einfach nicht wollte.

Bär: Das war ja auch genau einer der Punkte, mit dem du damals an mich herangetreten bist – denn dieser moralische Aspekt, der ist ein „warum" für den ich auch gerne mit antreten will. Ich weiß noch, dass ich mir ein paar Wochen vorher auf einem dieser größeren Hacker-Kongresse ein Proof-of-Concept angeschaut hatte, das hat gezeigt, wie ein Herzschrittmacher gehackt wird. Diese Kombination war ein sehr sehr starkes „warum".

Lange: Ihr habt schon ein paarmal Penetration-Tests genannt. Vielleicht gucken wir, was das heißt, weil das euer Alltag ist. Ihr habt auch gesagt, dass ihr das beauftragt und legal macht. Was macht ihr ganz genau? Damit wir uns vorstellen können, wie das bei euch und Firmen, die Ähnliches machen, abläuft.

Schughart: Ich versuche, einfach zu erklären, und Immanuel übersetzt, wenn es zu technisch wird. Es gibt Unternehmen oder Institutionen, die von Hackerinnen und Hackern wissen wollen, wo Probleme liegen, wo es Sicherheitslücken gibt, von denen sie nichts wissen. Sie beauftragen ein Sicherheitsunternehmen wie uns, wozu sie eine gewisse Form von Projektmanagement haben, damit das Ganze legal ist. Man muss immer wissen, was man testen darf und was man macht, wenn etwas kaputt geht. Dazu haben wir professionellere Versicherungen, damit nichts passiert. Wir legen oft in Teams los, das heißt wir koordinieren mehrere Hackerinnen und Hacker, die gewisse Felder abprüfen. Im Falle der physischen Sicherheit kopieren sie beispielsweise Zutrittskarten oder knacken Schlösser, damit sie physisch einbrechen können. Bei Faktor Mensch geht es um klassische Social-Engineering-Angriffe, beispielsweise Phishing-E-Mails, Vishing-Anrufe beziehungsweise Spoofing-Telefonate. Am Ende zeigen wir dem Kunden in einer Präsentation, wo es Defizite oder Potenzial gibt und was damit gemacht werden muss. Dann ist die Dienstleistung als Penetration Test oder Red Teaming beendet.

Bär: Vielleicht gehört an der Stelle eine Übersetzungsbox dazu. Ich glaube, jeder kennt Phishing und andere Varianten wie zum Beispiel Spear-Phishing. Bei Vishing steht das V vorne für Voice und Smishing steht für Angriffe per SMS.

Lange: Wir haben früher auch über Anrufe gesprochen, bei denen etwas vorgegeben wird, was nicht stimmt, und Menschen glauben das. Über Faktor Mensch würde ich gerne mehr

hören. Was sind so gängige Schwachstellen, wenn Unternehmen euch beantragen. Haben sie meistens das Gefühl oder wissen schon, dass da etwas nicht in Ordnung ist? Was sind die häufigsten Vorkommnisse, die ihr beobachtet?

Bär: Ich fange ein bisschen allgemeiner an. Am Ende des Tages ist es fast egal, ob es jetzt ein Unternehmen mit 50-, 500- oder 5000-Beschäftigten ist. Häufig fangen erste Herausforderungen mit der Detektion an. Sind Unternehmen in der Lage, Angriffe in der Qualität zu erkennen? Andere Themenfelder wäre klassische Netztrennung oder Segmentierung. Wenn ich es schaffe, auf einen bestimmten Teil, einen Client, ein Gerät oder einen Webserver vorzudringen, schaffe ich es auch, in den Rest zu eskalieren. Ansonsten gibt es Themen wie Updates und Patch-Management. Als ich letzte Woche bei einem Vortrag in Berlin war, habe ich gefragt, wer einen Staubsauger-Roboter zu Hause hat. Drei Viertel der Hände gingen hoch.

Lange: Michael hat einen.

Münz*:* Aber keinen mit WLAN. Ich habe extra einen ohne WLAN gekauft. Ich bin mir sicher, dass der nichts kann.

Bär: Da ist ein Webserver drauf.

Münz*:* Nein, es gibt keinen. Ich habe extra einen ohne WLAN gekauft. Ich bin mir sicher, dass der nichts kann.

Schughart: Aber der hat bestimmt Bluetooth, oder?

Münz*:* Auch nicht. Der kann gar nichts.

Lange: Aber saugen!

Münz*:* Das kriegt er hin. Ich hatte genau aus dem Grund nicht ein Gerät gekauft, das alles kann, sondern eins, das durch die Gegend fährt und ständig vor ne Wand – so einen habe ich.

Bär: Am Ende des Tages haben alle Bereiche eine sehr ähnliche Herausforderung. Sie digitalisieren, das heißt, dass man Schnittstellen schafft, und Schnittstellen sind Angriffsvektoren. Ob es ein Staubsauger-Roboter zuhause ist, ob es eine Fertigungsanlage beim Maschinenbauer oder eine neue Telefonanlage ist, die man noch nicht so richtig im Griff hat, das sind typische Bereiche.

Schughart: Die letzte Schwachstelle ist der Mensch. Da gibt es seit Jahrtausenden immer die gleichen Schwachstellen, beispielweise Neugier, Angst, klassischen Emotionen, die wir immer wieder ausnutzen, wenn es technisch nicht funktioniert. Wenn wir sonst nicht reinkommen, darüber klappt es immer.

Münz*:* Ehrlich gesagt klingt es ein bisschen gemein. Wir hatten schon oft diese Beispiele, die im Zweifelsfall funktionieren.

Schughart: Man kennt das Beispiel mit den USB-Sticks. Wenn der irgendwo liegt, soll man den nicht einstecken. Was glaubt ihr, was passiert, wenn ich einen USB-Stick in der IT - Abteilung hinlege und „Mein Bitcoin-Wallet“ darauf schriebe? Wenn es gezielt für die Zielgruppe geeignet ist, funktioniert das. Selbst wenn ich weiß, wie es funktioniert, bin ich nicht unhackbar. Genau das Gegenteil ist der Fall. Man darf sich selbst nicht für sicher und besser als die anderen halten, weil genau dann wird man der erste sein, dem es passiert.

Bär: Ich geh noch einen Schritt weiter: wenn der Hacker oder die Hackerin gute Marketing-Strategen sind und das Targeting verstehen – also da sind dann auch ein paar spannende Projekte dabei. Eines, das richtig Spaß gemacht hat, war bei einem großen Kosmetikhersteller. Da wurde geschaut, dass kleine goldene USB-Sticks in der Nähe von einem Mini Cooper etc. ausgelegt waren. Ute, du kannst dir überlegen, wer die Zielgruppe war. Das hat gut funktioniert. Es hat viel mit individuellem psychologischem Targeting zu tun. Ich bin gerade am Grinsen und du auch ein wenig.

Münz: Zum Thema USB -Sticks: ich war vor Kurzem an einer großen Konferenz, und eine Kollegin hat mich am Vorbereitungstag gefragt, ob ich einen USB-Stick hätte, weil sie irgendwas an ihrer Lichtanlage speichern musste. Ich habe ihr einen USB-Stick gegeben und erst danach gedacht, ob das eine gute Idee war. Ich habe den danach entsorgt und werde den nie wieder benutzen, vor allem wegen dem, was ich jetzt von euch höre. Im Zweifelsfall ist da irgendwas drauf, was einem gefährlich werden kann.

Schughart: Das Gleiche gilt für QR-Codes. Ich habe es Cross-Paper-Scripting genannt, als Gag von Cross-Site-Scripting abgeleitet, als wir infizierte QR-Codes in der Zeitung gedruckt haben und geguckt haben, ob Leute die scannen. Ja, sie scannen QR-Codes in der Zeitung. Das hat mich gewundert, ich hätte es nicht getan. Ein QR Code ohne Informationen auf einer großen Seite funktioniert.

Bär: Jetzt nutzen wir es bei Employer-Branding, um Beschäftigte zu gewinnen.

Lange: Aber damit habt ihr nichts Böses im Sinn, sondern wollt mehr Leute rekrutieren. Das führt mich zu einer Frage, die mich beschäftigt, und zwar ob es einen Markt für Menschen mit euren Kenntnissen und Erfahrungen gibt. Wir haben vorhin von zunehmenden Angriffen gesprochen. „Boomt“ das Geschäft für euch?

Schughart: Was die Nachfrage bei Kunden angeht, definitiv, das ist kein Geheimnis. Was die Mitarbeitendenseite angeht, besteht das Problem darin, dass das Zeitfenster klein ist. Es gibt viele, die es tun, das sieht man an den Zahlen, aber wir wollen keinen, der straffällig geworden ist, selbst wenn er sich nicht erwischen lassen hat. Wir wollen Leute genau an dem Punkt abholen, wo sie noch nichts Böses getan haben und ihnen eine bessere Perspektive zeigen, und zwar legale und berufliche, mit der Möglichkeit, Leute, die gleich gesinnt sind, kennenzulernen und sich austoben zu können, ohne sich verstecken zu müssen. Das Zeitfenster ist also begrenzt, und ich würde mir wünschen, dass es irgendwann eine gute Ausbildung gäbe, damit man den Leuten eine Perspektive gibt.

Münz: Kann man auch als Quereinsteiger dabei sein? Ich frage für einen Freund.

Schughart: Wir und auch andere Firmen haben viele Quereinsteiger, weil es diesen Beruf nicht gibt. Wer sagt, dass man etwas nicht kann, wenn man es als Hobby 20 Jahre gemacht hat, nur weil man beruflich etwas anderes tut? Bei uns alles hat es irgendwann als Hobby und Leidenschaft entstanden. Ein Mensch kann vieles gut machen, ohne ein Zertifikat zu haben.

Bär: Am Ende des Tages ist es oftmals die sich aufbauende Affinität auf einem Grundtalent. Nehmen wir einen sehr guten Softwareentwickler, der bei uns im Team aufgebaut werden kann, um sich bei Web-Applications oder Mobile-Applications weiterzuentwickeln. Es gibt Menschen, die mit Netzwerkinfrastrukturen und Switch-Technologie sich zu Hause fühlen. Sie können sehr schnell im infrastrukturellen Penetration Testing Fuß fassen, wenn sie den richtigen Ansatz und das richtige Wollen haben. Es kommt darauf an, dass man auf den Themenfeldern aufsetzt und dann seinen Weg findet.

Schughart: Wir haben im Marketing einen Kollegen gewinnen können, der Social Engineering für uns im Hintergrund mit baut, weil er sehr gut die Psychologie von Menschen versteht. Er bildet die Szenarien entsprechend aus, obwohl er vorher nie was von IT gehört hat, nicht mehr als ihr als Anwenderinnen und Anwender. Die Szenarien sind cool.

Bär: Wir haben auch einen Diplom-Philosophen im Lösungsbereich.

Schughart: Das heißt allerdings nicht, dass das Lernen einfach ist. Man muss fleißig sein.

Lange: Dein Freund hat Perspektive, Michael. Ich würde kurz auf eine Sache zurückkommen, die du erwähnt hast, Tim. Weil ihr euch gut auskennt, seid ihr nicht gefeit vor Angriffen. Ist euch schon etwas passiert, was euch jetzt nicht peinlich ist, hier zu offenbaren?

Schughart: Natürlich. Wir wissen zwar nicht, ob wir erfolgreich gehackt worden sind, aber wir haben schon Angriffe gehabt, die uns sehr nervös gemacht haben. Wenn sie jetzt schon irgendwo drin sind, wo sind sie denn? Wir konnten auch nicht innerhalb von einer Stunde sagen, was genau passiert ist. Wie Immanuel sagt, es ist ziemlich gefährlich, wenn man nicht weiß, was genau passiert und wo derjenige was versucht. In diesem Fall kann man nicht gut reagieren. Wir haben häufiger die Situation und lernen auch von solchen Angriffen, bei denen wir selbst „Opfer“ werden. Es sind jetzt keine Daten abgeflossen beziehungsweise, wir wissen nicht, dass jemand erfolgreich war. Ich kenne das Gefühl ganz gut, wenn man nicht weiß, ob jemand gerade erfolgreich ist oder nicht.

Bär: Das hat auch nicht nur mit uns direkt zu tun, sondern zum Beispiel mit unseren Familien. Es gab einen Anruf von meiner Frau Julia, die meinte, dass jemand den Internetanschluss durchmessen wollte. Ich habe sie sofort gefragt, ob er sich ausgewiesen hat, ob sie aus dem Fenster geguckt hat, ob das gesamte Szenario gepasst hat. Wir konnten es hinterher nachvollziehen und es war alles gut, aber solche Dinge gehören mit dazu.

Schughart: Als ich mit meiner krebskranken Frau im Krankenhaus war, konnte sie nicht behandelt werden, weil das Krankenhaus gehackt worden ist und die Systeme still standen. Es kam für mich so rüber, dass man nicht dagegen tun kann, wenn man gehackt wird. Und

ich war so sauer, dass ich das WLAN mit einer SQL-Injection gehackt habe, habe dem Geschäftsführer eine Nachricht in die Postbox gelegt und sagte, er soll sich bitte bei der Firma ProSec melden, weil man sich durchaus davor schützen kann. Er hat sich gemeldet, und wir haben das Problem aufgelöst. Wir haben es umsonst gemacht, weil es auch nicht immer um das Geld geht.

Bär: Ja, ich erinnere mich noch, wie sauer du warst.

Münz*:* Jetzt dauert seit 130 Tagen der Krieg in der Ukraine an. Wir haben an vielen Stellen mitbekommen, dass da digital viel gemacht wird. Ist das etwas, was bei euch auch ankommt? Habt ihr das Gefühl, dass die Situation in den letzten drei, vier Monaten sich verändert hat? Auch bei euch?

Schughart: Die Nachfrage ist logischerweise wieder hochgegangen, weil viele Unternehmen Angst haben. Stichwort #bloodytrade. Jemand, der für Russland oder die Ukraine Geschäfte macht, ist jeweils von der anderen Nation im Fokus. Das trifft auf Zulieferer zu, die diese Unternehmen beliefern. Die waren direkt unter dem Stichwort #bloodytrade massiv unter Beschuss. Außerdem gibt es aber auch positive Angriffe, das heißt, man versucht, ein Unternehmen zu hacken, wenn man denkt, dass es richtig ist. Beispielswiese Killnet, die aus Versehen deutsche Unternehmen treffen, weil sie denken, dass es da eine Wirtschaftsbeziehung besteht, was teilweise nicht stimmt. Wir haben unabhängig vom Unternehmen als Freizeitprojekt eine Software geschrieben, die westliche Nachrichtendienste nutzt, um früh zu erkennen, wenn böse Hacker sich austauschen und Sachen publik machen, um die westlichen Werte zu unterstützen und zu vertreten.

Lange: Wir hätten gerne noch einmal eine Übersetzungsbox für den ein oder anderen Begriff, den Tim genutzt hat.

Bär: Ich habe auf meinen Einsatz gewartet. Wir fangen dem Hashtag #bloodytrade an, um das in eine Metapher zu packen. Man kann bei Twitter #bloodytrade angeben schauen, was passiert. Eine sehr große Anzahl von Banken wurden in einem Symbol zusammengefasst und auf ein Militärfahrzeug gephotoshopt, das wurde bei Twitter geteilt und ist innerhalb von einer Woche mehrere tausende Mal auf LinkedIn und Twitter retweetet worden. Der Aufruf dahinter war, diese Bankenbereiche anzugreifen, weil die böse sind und im Endeffekt die Panzer bezahlen. Wir haben schon immer über Schwachstellen, Sicherheitslücken, Scams und Angriffe berichtet. Hier haben wir eine neue Dimension, und zwar Aktivistinnen und Aktivisten, die mit Kreuzzugsgedanken gerechtfertigt denken: ich poste jetzt etwas und rufe alle anderen dazu auf, jemanden anzugreifen, und dann verschwimmen die Grenzen. Sind das Scriptkiddie? Ist es eine Anonymous? Wer das ist wird fast nicht mehr interessant. Das ist eine Situation, der sich Unternehmen in der Zukunft gegenübersehen. Was heißt das im Umkehrschluss? Man muss nicht mehr nur auf Firewall oder auf IT-Logging aufpassen, sondern sollte auch die Marketingabteilung Bots schalten, um zu wissen, ob das Unternehmen irgendwo gerade auf dem Schirm ist und ob es in wenigen Stunden zum Beispiel an der Firewall knallen kann? Das ist eine neue Herausforderung und eine zweite

Dimension, also nicht nur IT-Logging, sondern auch grob übersetzt eine Art Marketing-Logging.

Lange: Danke für die Übersetzung. Ich hätte eine Frage für unsere Zuhörerinnen und Zuhörer sowie für Michael und mich, weil wir in dem Podcast immer dazulernen. Gibt es aus eurer Sicht Tipps und Tricks für uns, Verbraucherinnen und Verbraucher, Normalsterbliche, die nicht unbedingt über eure Kenntnisse verfügen? Michael hatte eine Studie erwähnt, dass sechs von zehn Internetnutzenden dieser Studie zufolge Hilfe im Netz brauchen. Vielleicht können wir am Ende dieser Folge noch etwas anbieten. Wir sprechen sehr oft über Updates und Passwörter, aber was sind andere Dinge, auf die wie achten könnten, um uns noch besser zu schützen? Vor allem wenn ihr an Social Engineering denkt.

Schughart: Gut, dass zu Beginn des Podcasts Identity Leak Checker vom HPI erwähnt wurde. Ich kann das mit Have I been pwned ergänzen. Das sind ähnliche Dienste, bei denen man mit Quellen, die vielleicht noch nicht im HPI drin sind, prüfen kann, ob man mit seiner privaten E-Mail-Adresse irgendwo betroffen gewesen ist. Wenn ja, bitte sofort die Kennwörter ändern. Der zweite Punkt ist die Nutzung von Passwort Managern. Das sind keine neuen Informationen, und die Hälfte der Zuhörerinnen und Zuhörer schüttelt jetzt wahrscheinlich den Kopf. Ich kenne das, aber schlechte Kennwörter bleiben immer noch das Hauptproblem. Nutzt nicht ein Kennwort für Amazon, Facebook, LinkedIn und Instagram, sondern trennt die Kennwörter und macht die möglichst komplex. Das kann ich nur leider immer wieder runterbeten. Was die Frage zum Faktor Mensch betrifft – seid euch bewusst über die Schwächen, die man als Mensch hat, weil man sie nicht abstellen kann. Wenn Emotionen wie Neugier oder Angst eintreten, reflektiert und macht euch klar, dass ihr genau in dem Moment, wenn ihr euch ängstlich fühlt, die E-Mail vielleicht noch ein zweites oder drittes Mal beziehungsweise eine Stunde später lest, sobald die Emotionen mehr unter Kontrolle sind. Dann seid ihr weniger anfällig.

Bär: Ich habe einen Hauptimpuls, egal vor wem ich stehe, und zwar Kopf und Kontext. Ich kann versuchen, zu merken, ob ich das, was mir geboten wird, wie zum Beispiel einen Knopf, auf den ich klicken soll, befolgen oder nicht befolgen soll. Kann das in den Kontext meiner Situation gerade passen? Ich habe in meinem Vortrag, als Ute und ich uns kennengelernt haben, bewusst ein Video von meiner Mutter gezeigt. Sie ist Seniorin, 83 und hat ein Seniorenhandy. Dieses Seniorenhandy ist zum Glück kein Smartphone. Sie hat eine Smishing-SMS bekommen mit der Benachrichtigung, dass sie ein Paket bekommen hat. Zum Glück hat das nicht in ihren Kontext gepasst, weil meine Mutter nicht die Onlineshopping-Queen ist, aber es war ein sehr gutes Beispiel, um klarzumachen, dass die Gegenseite auch nicht doof ist und immer intelligenter und kontextuell denkt. Während Corona bestellt man mehr über Amazon und andere Dienste, also es kommen immer mehr solche Meldungen. Wir müssen umso mehr digitale Awareness und Kopf und Kontext bei all dem einsetzen, was wir tun, gerade in Grenzsituationen.

***Münz**:* Vielen Dank! Es war sehr viel dabei, und vor allem eure Erklärungen zum Faktor Mensch haben mich sehr nachdenklich gemacht. Das war sehr aufschlussreich. Danke, dass ihr dabei wart!

Bär: Danke, dass wir dabei sein durften!

Schughart: Danke euch!

Lange: Wir machen normalerweise ein Wrap-up, aber jetzt war so viel dabei, dass wir die Folge selbst noch mal hören und nächstes Mal hier nochmal anschließen. Einiges muss ich in meinen Alltag ein bisschen mehr integrieren. Das, was wir hier merken, seitdem wir den Podcast machen, ist, dass wir für die digitale Welt genauso eine Sensibilität brauchen wie für die analoge. Wir lassen nicht unseren Schlüssel draußen in der Tür stecken oder legen ihn nicht in einen Blumentopf, sodass die ganze Nachbarschaft weiß, wo er ist, es sei denn wir wohnen in einer Nachbarschaft, der wir vertrauen können. Wir ziehen einen Helm auf, wenn wir Fahrrad fahren, wir laden keinen über einen Balkon ein. Michael und ich hoffen, dass ihr, Zuhörerinnen und Zuhörer etwas mitgenommen habt. Wir packen die Infos in die Shownotes und freuen uns sehr, dass ihr heute dabei wart. Vielen Dank dafür!

***Münz**:* Wenn ich nächstes Mal irgendwo einen USB-Stick liegen sehe, werde ich nach euch beiden gucken! Das ist bei mir hängengeblieben. Danke euch und bis zur nächsten Folge. Im Juli gibt es noch ein paar Wochen, in denen wir über alles nachdenken können. Danach geht es gleich weiter. Wir werden mit einem Experten zum Thema Biometrie und Deepfakes sprechen. Da gab es zwei Anlässe, über die einem zum Nachdenken angeregt haben. Das wollen wir in der nächsten Folge Ende Juli aufgreifen.

Lange: Bis dahin liket und folgt Update Verfügbar auf euren Podcast Plattformen. So verpasst ihr keine Folge. Ihr könnt auch gerne in ältere Folgen reinhören. Das würde uns sehr freuen. Hinterlasst uns Kommentare und kontaktiert uns gerne über die BSI-Kanäle auf Facebook, Instagram, Twitter oder YouTube. Schönen Sommer und bis bald. Tschüss!

***Münz**:* Oder schickt uns eine Mail an bsi@bsi.bund.de. Wir freuen uns auf Post und wünschen euch bis dahin alles Gute! Bis zur nächsten Folge! Tschüss!

Besuchen Sie uns auch auf:

https://www.bsi.bund.de/
https://www.facebook.com/bsi.fuer.buerger
https://twitter.com/BSI_Bund
https://www.instagram.com/bsi_bund/
https://social.bund.de/@bsi

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185-189, 53133 Bonn