„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 58, 27.08.2025
Deine E-Mails, dein digitales Zuhause

Moderation: Schlien Gollmitzer und Hardy Röde
Gast: Alexander Härtel, Sicherheitsexperte BSI
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Hardy Röde: Schlien.

Schlien Gollmitzer: Hardy.

Hardy Röde: Bist du in Sicherheit.

Schlien Gollmitzer: Inwiefern? Ich bin zu Hause und ich fühle mich relativ sicher. Die Tür ist zu, Schlüssel ist da, soweit so gut.

Hardy Röde: Tatsächlich. Heute noch niemand da gewesen, der vielleicht nicht in deine Wohnung gehört oder in dein Leben?

Schlien Gollmitzer: Nö, bisher noch nicht.

Hardy Röde: Okay.

Schlien Gollmitzer: Im Treppenhaus sind gerade die Nachbarn, die fahren jetzt in den Urlaub.

Hardy Röde: Mails schon aufgemacht, irgendwie Mails gelesen?

Schlien Gollmitzer: Nur deine.

Hardy Röde: Und außer meinen irgendwas Komisches passiert, irgendwas gewesen?

Schlien Gollmitzer: Temu versucht mich die ganze Zeit zu erreichen und ich frage mich, warum die meine E-Mail-Adresse haben. Aber sonst eigentlich nichts Großes los.

Hardy Röde: Das ist Update verfügbar, ein Podcast des BSI für Sicherheit im digitalen Alltag mit Schlien Gollmitzer und Hardy Röde.
Heute in Update verfügbar – etwas andere Mission als sonst. Schlien und ich sprechen über E-Mail-Sicherheit. Und dafür tauchen wir ziemlich tief in unsere E-Mail-Postfächer ein. Und

da finden wir natürlich einen Haufen Nachrichten, bei denen wir erstmal viel grübeln müssen, wo denn bitte dieser Absender unsere Adresse herhat.

Für viele von euch ist E-Mail vielleicht gar nicht das wichtigste Medium in eurer Kommunikation. Vielleicht nutzt ihr irgendeinen Messenger für alles, was privat ist, nutzt Tools wie Slack oder Teams oder WebEx für alles, was mit eurem Beruf zu tun hat.
Für das Austauschen mit Kollegen, fürs Verabreden von Terminen, für Dateien, die man hin und her schickt. Die Nachrichten lest ihr vielleicht auf Socials und das Entertainment kommt da sowieso her. Was machen wir denn dann eigentlich noch per E-Mail? Stellt sich raus? Eine ganze Menge.
Schlien und ich schauen uns in dieser gesamten Folge unsere Haupt-E-Mail-Adressen genau an. Das heißt, die Accounts, mit denen wir den allergrößten Teil unseres digitalen Lebens bestreiten. Bei mir ist es eine GMX-Adresse, bei Schleen ein Account bei Google Mail**.** Und jeder von uns benutzt diese Accounts schon sehr lange.

Schlien Gollmitzer: Seit, glaube ich, 20 Jahren oder sowas, gefühlt. Irgendwann vorher hatte ich mal einen WebDE-Account, da habe ich aber eines Tages das Passwort vergessen und bin dann auf Google umgestiegen und seitdem ist das so. Also es ist noch mein ganz, ganz uralter Nachname in diesem Google-Mail-Account. Insofern, ja, ist schon länger her.

Hardy Röde: Und was ist mit deinem WEB.DE-Account passiert, mit deinem verlorenen Passwort?

Schlien Gollmitzer: Das weiß ich nicht. Ich habe keine Ahnung, das wabert irgendwo rum im Internet, nimmt Speicherplatz weg vermutlich.

Hardy Röde: Hast du dich geärgert? Hast du dir gedacht, ah, Gott sei Dank, endlich kann ich eine digitale Häutung vollziehen.

Schlien Gollmitzer: Ja, ich glaube, das war eher Zweiteres: Es war ganz gut, weil ich muss sagen, so diesen WEB.DE-Account habe ich so in meinen frühen Internetzeiten genutzt – so Teenager-Zeit und dann so in die frühen Zwanziger hinein. Und aus heutiger Sicht, das Ganze nochmal in der Nachschau, würde ich sagen, habe ich den vielleicht ein bisschen zu häufig irgendwo eingetragen. Also es war dann schon auch ein bisschen wild, was da so an Mails reinkam.

Hardy Röde: Top 5 deiner damaligen Lieblings-Spam-Liste, so wenn wir da so zurückdenken. Viagra mit zwei Ausrufezeichen wahrscheinlich.

Schlien Gollmitzer: Viagra war mit dabei, die Penispumpen. Es gab damals schon diese Fake-Bank-Mails, die dann irgendwelche Daten haben wollten. Oder irgendwie irgendwelche Mails, in denen stand…

Hardy Röde: … also klassisches Phishing…

Schlien Gollmitzer: Genau, Phishing-Mails, in denen stand, dass irgendwie mein Account XY bei der Deutschen Post oder was auch immer gehackt worden wäre, und ich muss sofort

auf diesen Link klicken, mein Passwort eingeben oder meine Kreditkartennummer. Also solche Sachen, glaube ich, waren es.

Hardy Röde: Dass wir nicht auf jeden Link klicken sollen, der in unserem Postfach landet, das haben wir wahrscheinlich mittlerweile alle gelernt, weil es dieses klassische Phishing wirklich schon sehr lange gibt und trotzdem ist es irgendwie nicht tot zu kriegen. Im Gegenteil, heute ist es auf eine Weise gefährlicher als je zuvor, bestimmt gefährlicher als in Schliens altem, schon längst vergessene Mail-Account von früher.

Alexander Härtel: Ich hatte auch aus meiner Jugendzeit noch einen Account, wo ich dann auch gedacht habe, ja gut, ich habe mich damals als Maximilian Mustermann ausgegeben, das hat halt geklappt beim Registrieren, jetzt verwende ich die E-Mail-Adresse doch häufiger.

Hardy Röde: Das ist Alex Härtel. Er arbeitet beim BSI, dem Bundesamt für Sicherheit in der Informationstechnik. Nein, Maximilian Mustermann ist nicht sein früherer Name. Er hat uns die Geschichte aus einem bestimmten Grund erzählt, der jetzt nicht weiter wichtig ist. Der echte Alex jedenfalls nimmt das Thema E-Mail-Sicherheit heute sehr ernst und hat damit jeden Tag auch ziemlich gut zu tun

Alexander Härtel: Ich bin Teil beim Threat Intelligence Team des BSI und unsere Aufgabe ist es, den Überblick zu behalten über die ganzen Angreifer, die es da draußen gibt. Wie gehen die vor, wie sind die motiviert und wenn zum Beispiel ein Vorfall passiert, sind wir dann auch diejenigen, die gefragt werden, wonach muss ich jetzt Ausschau halten, was kann ich jetzt als nächstes tun – sei es für die staatlichen Behörden, sei es für die Wirtschaft oder halt auch, wie hier, für Bürgerinnen und Bürger.

Hardy Röde: Mehr als die Hälfte aller Internetnutzerinnen und Internetnutzer in Deutschland hat im letzten Jahr irgendeinen Schaden erlitten durch Cyberkriminalität. Die meisten Fälle passieren beim Onlineshopping, wo jeden Tag tausende Opfer von Betrügern werden. Aber fast genauso oft sind Nutzerinnen und Nutzer betroffen von Phishing. Also, sie fallen auf betrügerische Mails rein, mittlerweile oft auch auf Nachrichten im Messenger oder auf Social Media, mit immer derselben Masche: Hallo, hier ist deine Bank, dein Zahlungsdienstleister, dein Online-Broker, wer auch immer. Wir müssen da was überprüfen. Bitte gib doch schnell mal deine Zugangsdaten und dein Passwort ein, sonst wird dein Konto leider gesperrt. Ich konnte erst mal gar nicht glauben, dass das heutzutage so oft passiert und dass Phishing immer noch so ein großes Problem ist. Deswegen habe ich Alex als erstes danach gefragt, wobei das doch der älteste Trick der Welt ist.

Alexander Härtel: Genau, es ist uralt. Was sich halt geändert hat: Früher hat man so gesagt, ja, man erkennt so eine E-Mail an Fehlern im Text drin oder an merkwürdigen Formatierungen in der E-Mail. Das ist halt jetzt nicht mehr der Fall. Also die sehen so täuschend echt aus, auf den ersten Blick erkennt man da nichts mehr. Also diese Themes, also die Gestaltung, entspricht halt wirklich wie dem Original. Da muss man wirklich aufpassen.
Es ist weniger so wie früher, dass man Anhänge hat, in denen dann Malware drin ist oder dergleichen, sondern es wird wirklich mehr in diese Phishing-Richtung und dieses Social Engineering, dass man wirklich manipuliert wird, Informationen preiszugeben, die man eigentlich nicht preisgeben möchte.

Hardy Röde: Wie gut kann man es denn dann überhaupt noch unterscheiden? Gibt es vielleicht Quoten, wo du weißt oder wo man ungefähr abschätzen kann, wie viele Spam-Mails tatsächlich angeklickt werden, also wie viel Erfolg die Kriminellen mit solchen Kampagnen haben? Gibt es da Daten?

Alexander Härtel: Da sind mir keine Daten bekannt. Ich weiß aber, dass allein die Telekommunikationsdienstleister, bei denen die E-Mail-Konten laufen, allein die, bevor es überhaupt das Postfach erreicht, filtern schon zehntausende, hunderttausende pro Tag raus. Also wir haben halt die ganze Zeit Wellen, jeden Tag, jede Stunde und wirklich das Offensichtlichste wird schon rausgefiltert, bevor es den Endnutzer erreicht.

Hardy Röde: Verstehe ich dich richtig: Das heißt, das ist nur die Spitze des Eisbergs? Wir sehen den allergrößten Teil der Angriffswellen sehen wir nicht als normale Nutzer und Nutzerin?

Alexander Härtel: Genau, also so ist so das Feedback, was ich von den Telekommunikationsprovidern gehört habe, bisher, was ich auch dort gesehen habe. Das das meiste wird schon weggefiltert und da kooperieren auch die Dienstleister miteinander, also die informieren sich untereinander über Wellen und Charakteristika, um sowas rauszufiltern. Aber ja, auf der anderen Seite, die Angreifer passen sich auch ständig an, um gerade durch diese Filterung durchzukommen.
Also auch da ist es so ein Katz-und-Maus-Spiel zwischen den Betreibern und uns Verteidigern auf der einen Seite und den Angreifern, die sich immer versuchen anzupassen, um durchzukommen. Die das auch selbst testen, ob sie durch die Filter durchkommen. Das ist die Natur der IT-Sicherheit, wie wir sie heute haben: Alle paar Minuten kann sich das komplette Feld ändern und man wird mit einer komplett neuen Welle konfrontiert und sitzt da, okay, was ist jetzt anders, warum geht das durch? Woran kann ich es erkennen? Oder auch wir als Verteidiger sitzen ja da und fragen uns, ist das jetzt eine legitime E-Mail? Sollte ich die durchlassen, weil die ist ja vielleicht im Interesse des Nutzers? Wenn jetzt zum Beispiel jemand seinen Account zurücksetz, dann muss die E-Mail ja durchkommen. Man will ja auch nicht zu viel wegfiltern. Das ist so ein Hin und Her.

Hardy Röde: Das war der Punkt im Gespräch mit Alex, an dem ich mir dachte, deinen Job könnte ich nicht machen. Da denkst du, du hast ein Loch gefunden, eine Unsicherheit, die gefixt wurde, einen Angriffspfad, der dichtgemacht ist und dann kommen die Bösen plötzlich von ganz woanders her. Klingt nicht besonders befriedigend. Bei Alex hatte ich allerdings den Eindruck, sowas motiviert ihn erst recht, dann eben die nächste und die übernächste Sicherheitslücke zu finden und die Informationen weiterzugeben, damit sich Behörden oder Unternehmen drum kümmern können. Vielleicht muss man manche Gedanken auch einfach ausblenden. Wir als normale Nutzerinnen und Nutzer machen das ja auch, nur andersrum. Wir gehen unserem normalen digitalen Leben nach. Wir wissen wahrscheinlich grundsätzlich schon Bescheid, was wir im Netz tun sollten und was nicht. Nur kommt uns dann eben manchmal was dazwischen. Dieser ganz normale digitale Alltag.
Wir wissen wahrscheinlich grundsätzlich schon Bescheid, was wir im Netz tun sollten und was nicht. Nur kommt uns dann eben manchmal was dazwischen. Dieser normale digitale Alltag.

Schlien Gollmitzer: Holy crap. Okay, alles klar. Ja, ich nehme alles zurück, was meine Seriosität angeht.

Hardy Röde: Kleiner Spaziergang mit Schlien durch das Spam-Postfach ihres Haupt-E-Mail-Accounts, mit dem sie ja viel seriöser unterwegs sein wollte als mit ihrer alten Teenager-Adresse von früher.

Schlien Gollmitzer: Nein, es sind wirklich nur irgendwelche Accounts, die ich irgendwann mal angelegt habe. Also hier ist irgendwas von Heuer GmbH. Was ist das denn? Zwei Garkammern kann ich hier kaufen. Und eine Doppel-Heißluftfritteuse digital neun Liter. Irgendwann habe ich offensichtlich mal nach einem Job gesucht.

Hardy Röde: Schlien, könnte es vielleicht sein, dass du deine E-Mail-Adresse einfach überall eingibst, in jedes Formular, das nicht bei drei auf dem Baum ist? Kein Shaming natürlich jetzt. Meine eigene Haupt-E-Mail-Adresse, die wirklich das Zentrum meines digitalen Lebens ist. Die ist in den letzten Wochen neu bei einer Finanz-App, einem E-Auto-Ladeanbieter, einer Innenarchitektur-Website mit Farbmustern, einem Verkehrsverbund in Deutschland, einer Zeitung in England, einem digitalen Notizanbieter in den USA und bei einer Lese-App gelandet. Und das waren eben nur die letzten paar Wochen.

Schlien Gollmitzer: Ja, es ist nichts Schlimmes mit dabei. Irgendwelche Jobs, wo ich halt irgendwann mal was online gekauft habe, offensichtlich. Die versuchen, mich verzweifelt wieder zu erreichen, schaffen es aber nicht über meinen Spam-Filter hinaus. Das Gute ist, der löscht sich ja von alleine nach einiger Zeit. Deswegen ist gar nichts anderes drin. Also es sind tatsächlich genau diese, sagen wir mal, acht verschiedene Leute, die verzweifelt versuchen, mich zu erreichen und wollen, dass ich wieder was kaufe oder ein neues Hobby anfange.

Hardy Röde: Das heißt, du verwendest dann doch dein Konto, mit dem du dann angefangen hast, auch als Journalistin zu arbeiten, Leute zu kontaktieren, da wirklich täglich im Austausch stehst. Verwendest du nicht nur für berufliche Sachen, oder?

Schlien Gollmitzer: Nein. Das ist so wie meine Hausadresse halt einfach. Also so wie meine Adresse daheim, quasi die ganz analoge Adresse. So verwende ich meine E-Mail-Adresse.

Hardy Röde: Die würdest du auch einfach bedenkenlos jedem geben, oder?

Schlien Gollmitzer: Naja, meine Hausadresse hat sowohl das Finanzamt als auch du, als auch Amazon. Sarah von Hobby.de hat anscheinend auch diese Hausadresse. Die Deutsche Post, die Telekom und Freunde, die zum Grillen vorbeikommen und Spam mitbringen, zum Auf-den-Grill-legen.

Alexander Härtel: Ich würde eher dazu tendieren, zu sagen, dass man mehrere Adressen hat. Also einige Dienstleister bieten einem auch die Möglichkeit, unter einem Konto verschiedene Adressen zu haben, die im selben gebündelt werden. Das ist, was ich zum Beispiel verwende. Aber wenn man die Möglichkeit nutzt, zumindest zwei, drei Adressen zu

haben, kann man die halt auch thematisch trennen. Dass man zum Beispiel sagt, ich habe eine Adresse, die ist wirklich nur für Shopping und die verwende ich nur, wenn ich Sachen bestelle und dergleichen. Ich habe eine Adresse, die ist wirklich für die Kernanwendungen, die meine Identität ausmachen, sei es mit Banken, Zahlungsdienstleistern oder auch da, wo ich meine Cloud-Daten gesichert habe. Das ist ja was, das will ich nicht verlieren. Und da habe ich besonderen Schutzbedarf. Ja, und dann auch noch den Berufskontext. Da kommen halt auch gegebenenfalls beruflich noch andere Anforderungen, die ich privat nicht habe, an die Sicherheit.

Hardy Röde: Wenn ich jetzt sage, meine Hausadresse kennt ja auch jeder, sowohl das Finanzamt als auch meine Freunde, als auch der Lieferdienst, als auch irgendwie ein Onlineshop oder so. Ist das ein guter Vergleich? Oder was würdest du sagen, wo hinkt der vielleicht?

Alexander Härtel: Das ist eine gute Frage. Also natürlich kann man das irgendwo vergleichen. An beide Sachen können Post oder jetzt hier E-Mail zugestellt werden. Allerdings der Unterschied kommt, wenn wir uns angucken, wie ist es skaliert. Wenn wir jetzt in die Digitalisierung einsteigen, wir haben E-Mail. Das erlaubt es mir sehr einfach als Angreifer, Sachen rauszuschicken. Wenn ich jetzt hingehen müsste, ich müsste einen Brief ausdrucken, ein Porto dafür bezahlen und das rausschicken – wesentlich mehr Aufwand mit einer Privatadresse da Schindluder zu treiben oder natürlich kann ich auch Sachen hinbestellen.Aber so eine E-Mail – da ist der Aufwand ein paar Sekunden, wenn ich das automatisiere. Das ist gerade die Skalierung ist da, wo der Vergleich dann hinkt und es zusammenfällt.

Hardy Röde: Was ist denn aus deiner Sicht das Riskanteste, was ich mit meiner Mailadresse in irgendeinem Webformular machen kann, wo ich das einfach so eintrage? Wo sollen denn die Alarmglocken am lautesten schrillen?

Alexander Härtel: Man muss irgendwo einsehen, so häufig, wie man die E-Mailadresse verwendet: Irgendwann wird sie abfließen. Irgendwann wird sie im Internet durch den Äther fliegen. Aber gerade dann, wenn ich Zugangsdaten auch noch preisgebe oder weitere Informationen über mich selbst im Zusammenhang mit der E-Mail-Adresse. Dann sollte ich aufpassen. Also wenn man jetzt zum Beispiel irgendwo shoppen geht im Onlineshopping. Da gibt man dann eine ganze Reihe an Informationen über sich preis. Da sollte man schon aufpassen, was man da noch mitangibt. Zugegeben, da wird man eher nicht nach Passwort gefragt, aber dann kommen die Bankeninformationen ja dann als nächster Schritt. Genau.

Hardy Röde: Aber jetzt hake ich noch mal einen Punkt ein, den du gerade so nebenbei gesagt hast. Heißt es, ich muss im Grunde früher oder später damit rechnen, dass überall, wo ich jemals meine E-Mail-Addresse reinschreibe, sie irgendwann mal abfließen wird, wie du gesagt hast, also dass sie legal weiterverkauft wird oder illegal oder halblegal. Ich habe die AGBs angeklickt und habe dem Marketing ohne Grenzen zugestimmt, bis zu: die Datenbank wird geknackt und jemand nimmt sie sich unter den Arm und verkauft sie weiter. Ich muss einfach damit rechnen, dass sowas passiert?

Alexander Härtel: Leider ja. Also auch angesichts dessen, was wir im Ransomware Umfeld sehen, ist es nicht mehr die Frage, ob ein Unternehmen, eine Organisation angegriffen wird,

sondern es ist mehr die Frage, wann. Und wenn es passiert, dann fließen auch gerade solche Informationen ab. Und nach unserer Erfahrung, wenn Angreifer einmal in die Daten gekommen sind, die löschen sie nicht wirklich. Die verkaufen sie weiter, sie nutzen sie selbst. Und dann werden gerade solche Zugangsdaten oder auch solche E-Mail-Adresslisten dann auch weiterverkauft unter Angreifern.
Desto größer das Unternehmen, desto größer die Liste, desto mehr Wert hat sie dann auch für die Angreifer. Es werden tausende, zehntausende Nutzer gleichzeitig angeschrieben. Das heißt, eine Adresse hat vielleicht nicht mal den Wert von einem Cent in so einer ganzen Liste. Dementsprechend auch die Angreifer wollen Listen mit Hunderttausenden, Millionen an E-Mail-Adressen. Vielleicht ist die Chance, dass nur, weiß ich nicht, ein Prozent von den Millionen, die sie anschreiben, darauf reagieren. Aber das sind dann halt trotzdem Tausende.

Hardy Röde: Meine Mail-Adresse würde also zu einer Ware, die weniger als einen Cent wert ist auf irgendwelchen dunklen Marktplätzen von Cyber-Kriminellen für Cyber-Kriminelle. Sehr schöne Vorstellung. Ganz kurz das Thema Ransomware-Attacken. Die hat Alex ja erwähnt.
Vielleicht kriegt ihr davon ab und zu in den Nachrichten was mit, wenn eine Erpresserbande mal wieder ein sehr großes Unternehmen hackt. Da wird dann meistens das ganze interne Netzwerk lahmgelegt und es werden immer viele Daten gestohlen. Geschäftsunterlagen, Unternehmenszahlen, die interne Kommunikation, digitale Werke wie Designs oder technische Entwicklungen und immer auch Tausende oder Millionen Daten von Kundinnen und Kunden dieser Firma. Ransomware-Attacke heißt also, Hacker brechen ein, kopieren alles, was sie finden, verschlüsseln alle Datenbanken des Unternehmens und fordern dann Lösegeld, um sie wieder aufzusperren. Auf Englisch Ransom.
Manchmal sind Unternehmen durch so eine Attacke derart in der Klemme, dass sie tatsächlich bezahlen, manchmal mehrere Millionen. Manchmal bekommen sie danach ihre Daten zurück. Was Alex angesprochen hat, selbst wenn die Erpresser Geld bekommen vom Unternehmen also eigentlich erfolgreich waren, verkaufen sie meistens trotzdem die geklauten Daten noch mal weiter. Manchmal eben für diesen weniger als einen Cent pro Adresse.
Aber wenn sie Millionen Datensätze gestohlen haben, lohnt sich der Einbruch gleich ein zweites Mal für die Kriminellen. Unternehmen müssen in so einem Fall alle Kunden und Kommunikationspartner informieren. Hey, in unsere Systeme wurde eingebrochen.
Deine Daten wurden vermutlich geklaut. Bitte ändere dein Passwort. Zumindest in Europa ist es Pflicht.
Kleines Dankeschön an die Datenschutz-Grundverordnung. Da wurde das nämlich eingeführt. Firmen anderswo in der Welt machen das manchmal nicht. Kann also sein, dass ich gar nicht mitkriege, wenn mein Name, meine Mail-Adresse, vielleicht noch andere Daten von mir wie Telefonnummer, Kreditkartennummer und so weiter in einem solchen Pulk von Millionen Datensätzen durch die Gegend schwirren und von Kriminellen weiterverkauft werden.
Es gibt eine Website, auf der können wir aber zumindest selber nachschauen, ob eine Mailadresse in einem solchen Hack aufgetaucht ist. haveibeenpwned.com heißt sie.
Bitte nicht mitschreiben, das tippen wir euch besser in die Show-Notes, weil kompliziert. Pwn geschrieben PWN. Das ist ein Slang-Wort ursprünglich von Computerspielen, ein angeblicher Vertipper von OWN und es steht für: Du gehörst mir.

Schlien Gollmitzer: Ah ja, die kenne ich. haveibeenpwned.com.

Hardy Röde: Check if your email address is in a data breach. Schon mal deine eine Haupt-Gmail-Adresse da eingegeben?

Schlien Gollmitzer: Ja.

Hardy Röde: Wirklich? Ich noch nie. Also ich habe es getan vor unserem Gespräch und meine Mailadresse taucht in zehn Daten-Lags auf. Und das hat mich erst mal ganz schön so überrascht. Und deine?

Schlien Gollmitzer: Drei.

Hardy Röde: Oh, alles klar.

Schlien Gollmitzer: Das sind auch bekannte Daten-Lags, die passiert sind. Das habe ich auch tatsächlich verfolgt. Also steht auf der S eite steht da die history quasi der – wie übersetzt man denn breaches? – Datenlecks genau. Drei steht da bei mir. Ja, das finde ich süß. Da steht einfach: Oh no, pwned.This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

Hardy Röde: Okay.

Schlien Gollmitzer: So und dann haben wir einmal im Juni 2018. War es dieser Klamotten-Hersteller? Davon wusste ich. Ebenfalls im Juni 2018 war es dieses. Was war das nochmal? Ah ja, genau. Das ist das auch ein Klamotten-Hersteller. Und im Oktober 2017, das weiß ich noch, da war es. Wie nennt man das jetzt wieder so ein Familienfinder-Dings? Wie nennt man denn so was?

Hardy Röde: Ja, so eine Genealogie-Website.

Schlien Gollmitzer: Genau, so eine Genealogie-Website. Und da weiß ich noch, das habe ich damals mitbekommen und habe aber da auch sofort reagiert. Also ich habe in allen drei Fällen sofort reagiert, weil ich das mitbekommen hatte, dass das passiert ist.
Also die kannte ich jetzt alle drei schon.

Hardy Röde: Wie hast du das damals mitbekommen?

Schlien Gollmitzer: In den entsprechenden Nachrichten. Da habe ich es gesehen.
Da wurde darüber berichtet. Und ich habe wie gesagt, ich nutze diese Seite regelmäßig, um immer wieder nachzuschauen, was da so los ist.

Hardy Röde: Da schaust du tatsächlich öfters nach?

Schlien Gollmitzer: Da schaue ich öfter nach und ändere dann auch entsprechend die Passwörter. Oder gebe falsche Daten an oder lösche die Accounts.

Hardy Röde: Selber Spaziergang. Meine Adresse. Dass meine Adresse mehr als dreimal so oft in Datenlecks auftaucht wie Schliens, das habe ich vorhin schon gespoilert. Zusammen mit Alex schaue ich auf haveibeenpwned.com und frage ihn dort, wie ich das finden soll, dass meine Daten erst vor ein paar Monaten immer wieder geklaut worden sind. Hier bei einem Dienst, mit dem ich mir Pinboards und Listen für meine Arbeit zusammengestellt habe.
Und jetzt lese ich, das ist der aktuellste Leak. Im Januar 2024 wurden da Daten abgezogen. Über 15 Millionen E-Mail-Adressen. Und unten steht compromised data, also die enthaltenen Datensätze oder Datenarten waren E-Mail-Adressen, Namen und Nutzernamen. Wie sehr sollen mir denn jetzt schon die Haare zu Berge stehen, wenn ich sowas sehe, Alex?

Alexander Härtel: Es ist kein Grund, in Panik zu verfallen. Wie gesagt, man muss damit rechnen. E-Mail-Adressen fließen irgendwann ab. Von daher, das kann so ein Hinweis sein, okay, deswegen habe ich seitdem mehr Phishing oder mehr Spam bekommen. Das kann es einem so ein bisschen erklären, das Verhalten, das man beobachtet. Relevanter wird es, wenn wir uns den nächsten Leak angucken.

Hardy Röde: Ja, wo ich überhaupt nicht verstehe. Also das ist ein Leak September 2023, also auch relativ aktuell. Das hat einen Namen, da muss ich sagen, muss ich passen: naz.api über 100 gigabyte Stealer Logs and credential stuffing lists posted to a popular hacking forum. Da, glaube ich, brauche ich jetzt eine Übersetzungshilfe, was in diesem komischen breach drin war und wie das funktioniert.

Alexander Härtel: Fangen wir mit dem ersten Fachbegriff an, den Stealer Logs. So ein Log wird produziert von einem sogenannten Infostealer oder Informationstealer. Das ist eine Malware, die man sich einfangen kann auf verschiedensten Wegen, deren einziger oder gezielter Job es ist, wenn die Malware einmal ausgeführt wird auf dem Rechner, alle möglichen Daten über den Nutzer zu sammeln: Zugangsdaten aus dem Browser, gegebenenfalls ein Passwort Safe, wenn der offen ist. Kryptosachen, die auf dem Rechner laufen, so Krypto-Wallets. Das wird alles eingesammelt und zu einem Log zusammengefasst und der wird dann hochgeladen auf dem Server des Angreifers. Und das ist, was hier ein Stealer Log ist. Und im Endeffekt, woraus dieser Leak besteht, ist eine ganze Sammlung an solchen Stealer Logs, die zusammen 100 Gigabyte angehen. Jetzt muss man sich noch vor Augen führen, so ein Stealer Log hat in der Regel keine Bilder drin. Das sind nur Zeilen nacheinander: zum Beispiel für diese Webseite, wo unter dem Benutzernamen und dem Passwort sind die Zugangsdaten und das über Zeilen und Zeilen, Millionen an Zeilen an solchen Zugangsdaten. Das kann schon sehr, sehr sensitive Dateien über mich beinhalten.

Hardy Röde: Das kann schon sehr, sehr sensitive Dateien über mich beinhalten. Und da müssten wahrscheinlich dann sehr viele Alarmglocken auf einmal angehen, oder?

Alexander Härtel: Genau, wenn man so sieht, dass die Adresse in einem Stealer Log drin ist, das ist dann wahrscheinlich nicht nur, dass eine Kombination aus E-Mail- Adresse und Passwort betroffen sind, sondern im Zweifel Dutzende oder Hunderte, je nachdem, wie viele Accounts man selber pflegt und was man zum Beispiel auch im Browser hinterlegt hat, an Zugangsdaten. Wenn ich mich einlogge, sagt der Browser ja auch direkt, möchtest du die Zugangsdaten speichern? Und gerade das greifen die Angreifer hier ab. Man kann dann so

gucken, anhand des Datums, also hier September 2023, auch wenn nicht wirklich klar ist, wann der Stealer Log generiert wurde. Der kann im September generiert worden sein. Das kann aber auch schon im Mai oder im Januar gewesen sein von dem Jahr.
Im Endeffekt alle Accounts, die ich davor habe, sollte ich mir dann mal angucken, gegebenenfalls das Passwort ändern oder halt auch auf einen zweiten Faktor noch wechseln. Und den implementieren bei Sachen, die mir wichtig sind. Einen Schritt, den man vielleicht noch machen sollte, wenn es ein Dienst ist, den ich noch aktiv nutze: Dann sollte ich vielleicht gucken, hat sich was, seit das in dem Leak drin war, gab es Login-Versuche, die nicht von mir stammen. Gibt es zum Beispiel Aktionen, die in dem Account gemacht wurden?
Ich war auch selbst schon mit meiner Adresse mal in so einem Leak drin und da waren auch, vor allem so für Online-Spiele, für so Spiele-Datenbanken, meine Zugangsdaten mit drin. Da habe ich dann auch danach gesehen, da gab es Login-Versuche aus Afrika, aus Südamerika, aus Asien in den Folgewochen und Monaten, das mir vorher gar nicht so bewusst war, weil ich vielleicht auch die E-Mails ignoriert habe, die auf dem Account kamen. Wo mir dann auch das Herz kurz in die Hose gerutscht ist, wo ich dann so dachte, oh, oh, zum Glück alle Login-Versuche gescheitert. Aber da kann man dann auch noch mal gucken. Gab es Aktionen, die zu meinem Nachteil gelaufen sind?

Hardy Röde: Aber wie kann ich denn dann umgehen mit so einer Information, dass ich in so einer 100 Gigabyte Datenbank so einer Liste drin war, wie dieses naz api? Was sind denn da Schritte, die ich jetzt bei mir auf dem Rechner in meinen Diensten unternehmen kann? Zum Beispiel, um zu prüfen, ob tatsächlich so ein Infostealer, so eine Malware bei mir auf dem Rechner aktiv ist oder war.

Alexander Härtel: Was man halt grundsätzlich sagen kann, das Antiviren-System, was mittlerweile mit Windows mitgeliefert wird, ist schon ziemlich gut. Also es gibt nicht den dringenden Bedarf, andere Sachen zu installieren. Was man dann halt situativ machen kann, ist so ein Tool von einem der beliebigen Dienstleister runterzuladen und einen unabhängigen Scan durchzuführen, um zu gucken, ob was Verdächtiges auf dem Rechner drauf ist. Jetzt muss man bei Infostealern dazu sagen, viele der Infostealer, die mir bekannt sind, die werden einmal ausgeführt, sammeln die Daten und sind dann weg. Gerade, dass ich halt nicht nachvollziehen kann, wann war der Infostealer genau drauf. Ich kann nicht in den Leak detailliert reingucken.
Auf der anderen Seite gilt dasselbe, wie wenn ich auch in anderen Leaks drin bin. Wenn jetzt meine E-Mail-Adresse und Passwörter verwendet wurden, sollte ich die Dienste durchgehen, wo ich den Verdacht habe, dass mir ein Schaden entstehen könnte und gegebenenfalls das mal ändern. Dass man sich, also für sich selber sagt, ich habe im August 2025 mal geguckt, ich komme drin vor, dann ändere ich die Passwörter. Ich mache mir mal diesen halben Tag Aufwand und gehe meine Accounts durch und ziehe das alles mal wieder gerade mit einem Passwortmanager. Und dann ist auch wieder gut.
Dann kann ich mal ein paar Monate später noch mal gucken. Ist was in der Zwischenzeit passiert? Aber dass ich für mich selber so eine Gedankenlinie ziehe. Okay, bis zu dem Zeitpunkt alles, was davor kommt, was für mich relevant ist, habe ich mir mal angeguckt. Das ist so diese allgemeine Nutzerhygiene, die man mal machen sollte. Gerade, weil du ja auch schon gesagt hast, man sammelt über hunderte Dienste, Nutzerkonten und so. Braucht man die wirklich alle? Wahrscheinlich nicht. Genau, das sollte man Teil der Nutzerhygiene machen.

Hardy Röde: Okay, ein halber Tag Nutzerhygiene. Dinge, auf die ich keine Lust habe. Ich habe mich in dem Moment im Gespräch mit Alex schon zum zweiten Mal so gefühlt wie in dem Moment davor. Diese Machtlosigkeit von: Du stopfst ein Loch, aber dann reißt jemand, garantiert sofort wieder ein anderes auf und kompromittiert auf einem neuen Weg deine digitale Sicherheit. Bloß – dieses Mal muss ich das halt einfach tun und kann das niemandem überlassen. Niemand wird freiwillig für mich meine aktuell 169 Accounts durchgehen, in denen ich diese eine GMX-Adresse als Nutzernamen verwende, und dann 169-mal die Passwörter ändern oder noch besser: auf Zwei-Faktor-Authentifizierung umstellen. Das muss es einfach selber tun.
Auf der anderen Seite: Sowas passiert im Durchschnitt auch nicht jede Woche, oder jeden Monat, noch nicht einmal jedes Jahr. In solchen Riesen-Datenlecks war diese eine GMX-Mailadresse bisher fünfmal enthalten, über einen Zeitraum von fast 20 Jahren. Und: Vielleicht waren das auch nicht jeweils komplett neue Datenbestände. Diese Listen werden unter den kriminellen Hackern auch immer wieder kopiert und in neue Datensammlungen verpackt. Deswegen ist gar nicht klar, ob überhaupt ein Infostealer auf meinem Rechner zu Besuch war.
Jedenfalls hätte ich in fast 20 Jahren höchstens fünfmal alle Accounts so genau durchgehen müssen, wie Alex sagt, also: Bei den Wichtigsten nochmal extra schauen, ob da Mist passiert ist, und bei der Gelegenheit vielleicht gleich wieder zehn oder zwanzig Accounts stilllegen – weil: Natürlich brauche ich keine 169 Accounts für irgendwas im Leben.
Und – Fun Fact: Wahrscheinlich habe ich das in den letzten fast 20 Jahren sogar sowieso drei-, vier-, fünfmal gemacht. Nicht, weil ich auf haveibeenpwned.com meine Adresse in Hacks gefunden hätte, sondern wegen der ganz klassischen Sachen: Handy verloren, sicherheitshalber alle wichtigen Passwörter geändert. Mail gekriegt von einem Unternehmen, das gehackt worden ist, sicherheitshalber gleich auch die anderen Passwörter geändert. Passwortmanager neu installiert, alles reinkopiert, sicherheitshalber alle wichtigen Passwörter geändert. Und so weiter.
Ich würde mein digitales Leben ist jetzt kein besonders krasses Messie-Leben bezeichnen, aber sogar meinen Keller habe ich in dieser Zeit öfters aufgeräumt als die Accounts mit dieser einen, wichtigsten Mail-Adresse.

Was würdest du sagen, wie sollen wir auf E-Mail blicken? Also welchen Stellenwert sollten wir dem in Bezug auf unsere Onlinesicherheit einräumen?

Alexander Härtel: Ich würde es gerne vergleichen mit dem Personalausweis. Klar, ein Personalausweis hat noch eine höhere Anforderung, weil es ein staatliches Ausweisdokument ist, aber wenn ich mich im Internet bewege, ist halt trotzdem die E-Mail-Adresse ein zentrales Instrument, mit dem ich dem Internet sage, hallo ich bin derjenige und darunter werde ich auch bekannt im Internet. Es ist auch nach wie vor so: Egal wie sich die Anmeldeverfahren weiterentwickeln mit zweitem Faktor oder auch zukünftig mit Passkey – am Ende brauche ich trotzdem immer noch die E-Mail-Adresse, die mich als Nutzer identifiziert, als eine singuläre Identität dem Anbieter gegenüber. Und so sollte man es auch behandeln, selbst wenn man keine E-Mails schreibt oder es empfängt. Es ist Endeffekt die eigene digitale Repräsentation. Und dementsprechend sollte man darauf auch achten, wie man auf sich selbst achtgibt.

Schlien Gollmitzer: Boah, Hardy, wie krass, was für eine aufregende Reise wir jetzt hier gerade unternommen haben. Also ich bin direkt so ein bisschen reisefertig jetzt, fühle mich wie nach der Ankunft aus dem Urlaub wieder zurückkommt. Aber es war irgendwie so viel los in diesem Urlaub, dass ich jetzt erst mal eine Woche Urlaub brauche, um wieder runterzukommen.

Hardy Röde: Ich melde mich nochmal bei Schlien, nachdem ich mit Alex gesprochen habe, und er mit mir durch die dunklen Ecken ihrer und meiner E-Mail-Accounts gelaufen ist. Es war kein Urlaub. Es war tatsächlich eine Dienstfahrt auf einem schon teilweise sehr schwankenden Schiff, würde ich eher sagen.

Schlien Gollmitzer: Tatsächlich. Superspannend dieses Gespräch, das du mit Alex noch geführt hast. Was mir jetzt auch vor allem noch so hängen geblieben ist oder auch aufgeklärt und wachgerüttelt hat: Ich habe ja gesagt, dass ich meine E-Mail-Adresse so ein bisschen wie meine Heimadresse eigentlich verwende.

Hardy Röde: Mhm, die kann jeder wissen.

Schlien Gollmitzer: Ich nehme mit tatsächlich, ich sollte das wirklich anders handhaben. Ich sollte vielleicht doch mich, sagen wir mal, auf breitere Beine aufstellen oder wie sagt man da, auf mehrere Beine aufstellen. So ein bisschen solider mit breiterem Kreuz mit verschiedenen E-Mail-Adressen für verschiedene Gründe, z.B. beruflich, wie Alex ja auch gemeint hat. Oder die Shopping-E-Mail-Adresse, um den Newsletter-Rabatt-Code abzugreifen oder sowas und das nicht unbedingt mit meinem Sparkassen-Account zu verknüpfen, wäre sicher eine gute Methode. Aber dann ist es ja wirklich so, dass man das anders denken muss. Man muss E-Mail-Adresse nicht denken wie Heimadresse zu Hause, sondern eher wie so eine Art Personalausweis eigentlich.

Hardy Röde: Ja, mit dem zusätzlichen Luxus, dass du jetzt dir drei oder vier oder fünf verschiedene Personalausweise zulegen kannst für diese ganzen Zwecke, was eher ein Vorteil für dich ist. Also, dass du die Möglichkeiten, die wir im digitalen Raum haben, natürlich für dich nutzt, ganz legitim zu sagen: Der Ausweis, mit den ich mich gegenüber meiner Bank oder dem Einwohner-Meldeamt oder bei den ganz wichtigen zentralen Diensten für mein digitales Leben, meinem Cloud-Dienst oder so anmelde. Das ist ein anderer Ausweis – und den kriegen auch nur die zu sehen – als der Ausweis, mit dem ich mich als Schlien oder Hardy bei den Shopping-Retailern oder Online-Versendern identifiziere. Und das ist, glaube ich, wirklich einfach eine sehr gute Maßnahme, wenn man es durchhält. Also wenn man da irgendwie mal Muse hat, und man sagt, ich mach mal vielleicht zwei, und dann guckt, wie das funktioniert.

Schlien Gollmitzer: Ich habe ja jetzt nach unserem Dienstreisen-Urlaubsausflug eine Woche Urlaub, da kann ich mich ja jetzt konzentriert da dransetzen. Aber da habe ich dann jetzt auch einiges zu tun, Hardy. Mal schauen, ob ich rechtzeitig zur nächsten Folge wieder zurück bin und dir dann ein Update geben kann.

Hardy Röde: Das habe ich mir auch vorgenommen. Das ist unser Update. Und wie immer, wenn euch diese Folge gefallen hat, dann liked und folgt uns gerne. Update verfügbar, gibt's

auf allen Podcast-Plattformen. Da freuen wir uns sehr, wenn ihr uns ein Sternchen gebt oder eine Bewertung schreibt.

Schlien Gollmitzer: Weitere Infos zum Thema unserer heutigen Folge findet ihr natürlich wie immer in den Show-Notes und für alle anderen Fragen zum digitalen Alltag und zur Cybersicherheit findet ihr das Team des BSI auch auf Instagram, auf Mastodon und auf YouTube.

Hardy Röde: Dann bis zum nächsten Update.

Schlien Gollmitzer: Bis zum nächsten Update.