„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 60, 3.11.2025
Was macht einen guten Passwortmanager aus?

Moderation: Schlien Gollmitzer und Hardy Röde

Gast: Lars Bartsch – K12 Technischer Verbraucherschutz und Marktbeobachtung (BSI)

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Schlien Gollmitzer: Hardy?

Hardy Röde: Schlien?

Schlien Gollmitzer: Kannst du dich noch erinnern, was wir im April besprochen haben?

Hardy Röde: Ah, Moment, warte, es ging um Heuschnupfen.

Schlien Gollmitzer: Nein, ich meine tatsächlich in dem Fall jetzt so IT-sicherheitstechnisch, also im Podcast, was wir da besprochen haben.

Hardy Röde: Irgendwas Wichtiges war da.

Schlien Gollmitzer: Ja, es war sogar was sehr, sehr Wichtiges, und zwar haben wir ja im April in unserer Folge 54 schon mal davon gesprochen, dass wir uns im Oktober 2025 von Windows 10 verabschieden müssen.
Hardy Röde: Ja.

Schlien Gollmitzer: Und jetzt ist, Hardy?

Hardy Röde: Oktober 2025.

Schlien Gollmitzer: Ganz richtig, sehr gut auf den Kalender geschaut, und zwar haben wir jetzt sogar schon Ende Oktober, wenn dieser Podcast rauskommt, und seit dem 14. Oktober gibt es keine Sicherheitsupdates mehr für Windows 10.

Hardy Röde: Ah, sie machen also ernst.

Schlien Gollmitzer: Also, der Support ist jetzt beendet, und das ist natürlich ein erhebliches Risiko für alle Rechner, die eben mit diesem Betriebssystem noch laufen.

Hardy Röde: Aber es gibt doch die Möglichkeit, sich noch irgendwie so eine Verlängerung zu kaufen. Das haben wir damals erzählt, also ein Update zu bekommen oder weiterhin Updates für eine bestimmte Zeit.

Schlien Gollmitzer: Ja, richtig. Und tatsächlich ist die Nachricht jetzt für alle, die sich von ihrem alten Rechner oder von Windows 10 eben noch nicht trennen konnten, noch ein bisschen besser. Wobei, ist sie das? Wir schauen es uns an.

Hardy Röde: Das ist Update verfügbar, ein Podcast des BSI für Sicherheit im digitalen Alltag mit Schlien Gollmitzer und Hardy Röde. Als Nicht-Windows-Nutzer von Beruf habe ich das natürlich nur nebenbei verfolgt, dieses Thema. Was ich aber weiß und die letzten Tage nochmal abgefragt habe bei den Kolleginnen und Kollegen aus dem BSI, ist, dass viele Nutzerinnen und Nutzer, die Windows 10 auch auf ihrem Rechner haben, da ihre Fragen damit haben.

Schlien Gollmitzer: Selbstverständlich.

Hardy Röde: Mit denen rufen sie manchmal beim BSI tatsächlich an oder schreiben eine Mail. Kann übrigens jeder und jede machen. Ihr könnt das auch. Es gibt das Support-Center des BSI. Das hilft bei allen IT-Sicherheitsfragen, und freundlicherweise schreiben wir euch die Kontakte in die Shownotes. Was jetzt speziell Windows 10 angeht und eben das Ende dieser Updates, sind tatsächlich ein paar Fragen da immer wieder aufgetaucht.

Schlien Gollmitzer: Naja klar, man hat es ja auch in einigen Medien jetzt mittlerweile mitbekommen, dass da eben im Oktober was ansteht. Aber was da genau so alles zu beachten ist, das ist dann doch teilweise etwas unklar geblieben. Habe ich auch selbst gemerkt.

Hardy Röde: Wir hangeln uns jetzt einfach, würde ich sagen, an den Fragen entlang, die am häufigsten beim Support-Center im BSI aufgetaucht sind.
Und du hast dich mit der Materie beschäftigt und kannst sie hoffentlich beantworten.

Schlien Gollmitzer: Hit me.

Hardy Röde: Die Antwort hast du schon ein bisschen angedeutet. Stimmt es denn jetzt tatsächlich, dass der Windows-10-Support kostenlos verlängert wird? Und das haben viele Leute sich gefragt.

Schlien Gollmitzer: Zu Recht haben sie sich das gefragt. Tatsächlich kann man jetzt auch nach diesem eigentlichen Support-Ende – 14. Oktober war ja der Stichtag – noch Sicherheitsupdates für Windows 10 rausholen, aber eben nur unter bestimmten Bedingungen und auch nur für die nächsten zwei Jahre wieder begrenzt.

Hardy Röde: Das heißt also, das ewige Leben wird es nicht geben für die Windows – 10 - Kiste?
Nee, wir haben uns ja auch irgendwann mal von Windows 95 verabschiedet, wenn wir uns daran nochmal erinnern möchten. Nein, Microsoft wird danach tatsächlich endgültig nur

noch Windows 11 und eben kommende Versionen mit Sicherheitsupdates versorgen. Das heißt, ihr habt jetzt einfach nochmal zwei Jahre länger Zeit, euch von eurem schönen, lieben Röhrenmonitor zu verabschieden und euch dann vielleicht doch irgendwann mal mit einem Nachfolgerechner auseinanderzusetzen.
Was ich mich dann fragen würde als Nutzer oder Nutzerin, was viele, viele Leute auch im Service-Center gefragt haben: Wie kriege ich denn diese kostenlose oder ein bisschen kostenlose Verlängerung, wenn ich tatsächlich noch zwei Jahre rausholen will, und worauf muss ich achten? Was sind das für Bedingungen, von denen du geredet hast?

Schlien Gollmitzer: Naja, es ist im Grunde erstmal relativ einfach, kann man sagen. Und zwar gehst du bei Windows 10 in die Einstellungen. Das kennst du ja wahrscheinlich, wenn du mit dem Betriebssystem schon gearbeitet hast. Und unter Updates und Sicherheit, da musst du dich dann mit deinem Microsoft-Konto anmelden. Oder wenn du halt noch keins hast, dann kannst du auch einfach schnell dort eins anlegen. Und dann kannst du dich ganz einfach für das sogenannte Extended Security Update registrieren. Und jetzt mit dieser Anmeldung hängt es natürlich auch wieder so ein bisschen zusammen. Überall, wo wir uns anmelden, hinterlassen wir unsere Daten. Das kennen wir ja schon. Also, ist es wirklich kostenlos, oder zahlen wir wieder mal mit unseren Daten?

Hardy Röde: Und wenn ich es richtig verstanden habe, ohne dieses Microsoft-Konto absolut kein Update.

Schlien Gollmitzer: Ganz genau, richtig. Das braucht man auf jeden Fall. Aber es gibt noch eine Bedingung. Genau genommen hat man da nämlich zwei Optionen. Entweder muss man sich mit dem Microsoft-Konto alle 60 Tage lang am System eben anmelden, um weiterhin Updates zu bekommen, oder man bezahlt eben dann wiederum eine Gebühr von um die 30 Dollar. Davon hatten wir in der Folge 54 eigentlich auch schon berichtet. Da waren es auch schon diese 30 Dollar.

Hardy Röde: In jedem Fall gibt es dann die Updates für zwei weitere Jahre kostenlos für Windows 10. Also bis Oktober 2027, wenn ich richtig rechne, für mein altes System.

Schlien Gollmitzer: Das hast du sehr gut gerechnet, Hardy. Von 2025 zwei Jahre drauf sind es 2027 exakt. Dieses Update, das ist jetzt so ein kleiner Bonus, das kannst du mit dem gleichen Microsoft-Konto sogar noch für neun weitere Rechner im Haushalt freischalten. Keine Ahnung, wer zehn Rechner in seinem Privathaushaltshaus hat.

Hardy Röde: Ich könnte dir Geschichten erzählen.

Schlien Gollmitzer: Ich habe nicht mal so viele Zimmer in meiner Wohnung, aber okay.

Hardy Röde: Alte Handys könnten sich so angesammelt haben. Also, wenn wir jetzt in der Radio-Werbung wären, würden wir sagen, das ist ja ein Wahnsinns-Angebot, Schlien.

Schlien Gollmitzer: Das schnurrt ja wie ein Kätzchen, Hardy. Tatsächlich.

Hardy Röde: Aber es kreisen ja auch in den letzten Monaten immer mehr Anleitungen rum im Netz, auf YouTube zum Beispiel und anderswo, dass man Windows 11 vorgaukeln kann. Du, mein Rechner, der kann das schon alles, was du hier forderst. Also, dass man da so ein paar Umwege geht und auch dann das Windows-11-Update auf die bestehende Maschine, den bestehenden Rechner drauf installieren kann. Eigentlich ganz einfach, sagen diese ganzen YouTube-Videos. Ich in meiner Nerd-Ecke lese das auch so ein bisschen mit. Und die Frage ist auch oft beim BSI im Postfach gelandet. Wäre das eine Alternative?

Schlien Gollmitzer: Na, Hardy, bitte. Was glaubst du denn wohl, was die Profis vom BSI dazu sagen?

Hardy Röde: Wir raten davon ab, oder? Denn Trickserei ist nicht gut. Es geht eher in Richtung Abraten. Ja, ganz klar mit solchen Spielereien. Wer damit umgehen kann, vielleicht eben die Technik so ein bisschen überlisten kann. Aber tatsächlich muss man schon ein bisschen sagen, mit Sicherheit hat es relativ wenig zu tun.

Schlien Gollmitzer: Die Anleitungen können ja auch nicht versprechen, dass dann eben im Einzelfall tatsächlich das Ganze gut geht und nicht doch noch zu Problemen führt. Und vor allem, das ist auch nur ein Spiel auf Zeit mal wieder, weil wie lange das Ganze gut geht, lässt sich auch jetzt noch nicht sagen, weil eben Microsoft jederzeit wieder die Voraussetzungen ändern kann für solche Rechner. Und um das vielleicht auch noch mal ganz klar und deutlich zu sagen: Ohne regelmäßige Sicherheitsupdates – warum wir da so drauf pochen beim Betriebssystem – sind einfach unsere Rechner offene Scheunentore, kannst du sagen, für Schadsoftware, für Cyberangriffe natürlich. Und man darf davon ausgehen, dass Kriminelle jetzt eben nach diesem Support-Ende – die haben sich das ganz hart angemarkert in ihrem Kalender, 14. Oktober –, dass da natürlich verstärkt Angriffe auf eben diese nicht mehr geschützten Windows-10-PCs laufen werden und dass das definitiv kommen wird und passieren wird.

Hardy Röde: Und die eine Frage, die auch oft gekommen ist an das Service-Center im BSI, die ist damit im Grunde auch schon beantwortet. Kann ich Windows 10 einfach trotzdem weiter benutzen? Also, wenn ich zum Beispiel immer eine aktuelle Virenschutzsoftware drauf installiere, ist es eine gute Idee? Ich ahne, die Antwort ist nein.

Schlien Gollmitzer: Ja, und es bleibt auch ein ziemlich klares Nein oder ein sehr klares Nein sogar. Ob mit oder ohne Virenschutzsoftware: Windows 10 ohne Updates ist ab jetzt ein sehr unsicheres System. Das sage ich jetzt mit voller Deutlichkeit.
Das könnt ihr euch aus dem Podcast genauso rausschneiden und dann übers Bett oben drüber hängen, so als Wandtattoo eventuell. Also, eure Daten sind tatsächlich damit bedroht. Mit allen Folgen, die das Ganze natürlich haben kann, auch für euer Geld und für andere Bereiche in eurem Leben.

Hardy Röde: Aber noch eine letzte Frage für den Augenblick, die auch oft gekommen ist. Was ist mit den Alternativen zu Windows 10 und Windows 11? Wenn ich jetzt sage, ich kann oder will mir nicht ein neues Gerät, einen neuen Laptop, einen neuen PC kaufen, weil der eigentlich technisch noch total in Ordnung ist. Was sind denn mögliche andere Betriebssysteme?

Schlien Gollmitzer: Ja, eben das muss man vielleicht auch nochmal deutlich sagen. Es gibt ja nicht nur Windows oder Microsoft mit dem entsprechenden Betriebssystem. Einige nutzen ja, einige von uns nutzen ja sogar Systeme von Apple, ohne Namen nennen zu wollen. Und wer sich eben nicht mehr abhängig machen will von den Launen eines Softwaregiganten, sei es Apple oder Microsoft, für den käme dann zum Beispiel Linux ja in Frage.

Hardy Röde: Also, wer sich da genauer damit beschäftigen will, weil er zukünftig nicht mehr davon abhängig sein will, ob es noch offizielle Updates gibt für sein Gerät oder nicht, der kann sich Linux anschauen. Und wir legen euch auch nochmal unsere Folge 54 von *Update verfügbar* ans Herz. Da haben wir auch schon unter anderem in Richtung andere Betriebssysteme geguckt. Und wenn ihr gerne mehr hören und erfahren möchtet zu diesem Thema, was ja vielleicht noch ein bisschen weitergeht mit Windows 10 und Windows 11, schreibt uns gerne eine Nachricht oder einen Kommentar zu dieser Folge. Wir lesen es und wir gehen auch gerne nochmal auf das Thema ein. Stichwort alte Folgen von Update verfügbar, Schlien, steckt dir eigentlich auch noch unser Thema E-Mail-Sicherheit in den Knochen, von der wir es vor zwei Ausgaben hatten im August 2025?

Schlien Gollmitzer: Die Folge 58 war das, gell? Jetzt, wo du es so ansprichst, klingelt plötzlich in meinem Kopf irgendein Alarmwecker. Da war was. Ich wollte noch weitere E-Mail-Adressen anlegen, gell? Bin ich bisher noch nicht weit gekommen, um ehrlich zu sein. Aber schaue ich mir nochmal, lege ich mir nochmal hin. Den Ball nehme ich nochmal auf.

Hardy Röde: schlienprivat.googlemail.com. Ich muss sagen, ich denke da wirklich noch oft dran. Wir haben uns mit dem Kollegen Alex Hertel aus dem BSI unterhalten, der sehr, sehr genau drauf schaut, was kriminelle Hacker so machen. Eben auch mit unseren Zugangsdaten, unseren Mail-Adressen. Ich habe seitdem auf seinen Rat hin mein E-Mail-Game so ein bisschen schon angepasst. Also, diese getrennten E-Mail-Adressen wirklich ernst genommen.

Schlien Gollmitzer: Dich hat es auch ein bisschen härter getroffen als mich, um ehrlich zu sein. Ja, ich hatte Handlungsbedarf.

Hardy Röde: Also, Stichwort nicht mehr das ganze digitale Leben über eine einzige Adresse abzuwickeln. Da habe ich zumindest ein bisschen für Ordnung gesorgt.

Schlien Gollmitzer: Wie gesagt, ich habe es auf Wiedervorlage. Definitiv. Ich habe schon so ein kleines Brainstorming mit mir selbst veranstaltet. Ich habe schon gute Ideen für tolle E-Mail-Namen.

Hardy Röde: Ja, was ich jedenfalls noch nicht gemacht habe, war einer der weiteren Tipps. Ha, die brauchst du wirklich. Über 600 Accounts, die du in deinem Passwortmanager mit rumschleppst.

Schlien Gollmitzer: Also in meinem Account-Stadel mal aufräumen, wäre immer noch an der Zeit. So wie man halt die ollen Klamotten auch irgendwann mal aus dem Schrank rausschmeißt, wenn man ganz ehrlich zu sich ist und sagt, werde ich nie wieder anziehen.

Hardy Röde: Und die schwärmen halt immer noch rum. Aber zumindest gut aufbewahrt im Passwortmanager.

Schlien Gollmitzer: Ich bin sowohl beim Klamotten aussortieren als auch bei verschiedenen Accounts aussortieren nicht besonders gut. Aber ich habe auch keine 600 Accounts. Das muss man auch noch mal dazu erwähnen. Hört euch die Folge nochmal an, dann wisst ihr ganz genau, wovon wir hier reden.

Hardy Röde: Vielleicht hast du 600 Klamotten. Also beim Passwortmanager, der hat schon wirklich viel in meinem digitalen Leben verändert und verbessert. Ich benutze einfach den, der bei mir im Betriebssystem eingebaut ist. Und das gibt es sowohl bei Windows als auch bei Mac Betriebssystemen für die Smartphone Plattformen natürlich auch Android und iOS. Und ich habe mich damals dafür entschieden, weil ich von den vielen Programmen, die es dafür gibt, also wirklich auch ein großes Angebot sehr, sehr gut bewährter Programme da bin ich ehrlich gesagt ein bisschen ratlos davor gestanden. Was ist jetzt sicher? Welcher Hersteller geht welchen Weg technisch? Wo gibt es Sicherheitslücken, die völlig unerwartet auftreten? Und es war für mich, obwohl wir uns ja öfters mit dem Thema Cybersicherheit auseinandersetzen, unterm Strich schwer zu durchschauen.

Schlien Gollmitzer: Ja, hättest du da mal die Profis gefragt, natürlich.

Hardy Röde: Oh, hätte ich das mal gemacht. Also die Profis beim BSI haben sich tatsächlich um mein Thema gekümmert und haben eine...

Schlien Gollmitzer: Hardy hat jetzt schon so eine kleine Privatriege beim BSI, die sich um deine persönlichen Probleme kümmern zum Thema Cybersicherheit.

Hardy Röde: Es war Zufall, aber ich lerne ja auch in jeder Folge hier dazu. Es gab eine technische Untersuchung von Passwortmanagern, die das BSI zusammen mit dem Forschungszentrum Informatik durchgeführt hat, erst vor Kurzem, und da sind exemplarisch zehn Passwortmanager rausgegriffen worden, die so aus allen Bereichen kommen, in denen diese Programme angeboten werden.

Schlien Gollmitzer: Okay, Hardy, damit wir jetzt nicht gleich den kompletten Überblick verlieren, solltest du vielleicht noch mal kurz erklären, was diese Manager genau machen.

Hardy Röde: Wie funktionieren Passwortmanager? Ein Passwortmanager ist im Grunde ein digitaler Tresor, ein Ort, an dem all deine Passwörter aufbewahrt werden, am besten sicher verschlüsselt. Auch andere Daten kannst du so aufbewahren, zum Beispiel deine Kreditkartennummer oder den Code für deinen Türschluss. Du musst einmal deine Zugangsdaten drin speichern, also zum Beispiel deine Mailadresse und das Passwort, und dazu die Website oder App, für die du sie nutzt. Nach dem Speichern kannst du sie dann jederzeit wieder aus dem Tresor rausholen. Für mehr Sicherheit schließt du den Tresor aber ab. Zum Aufsperren verwendest du ein Masterpasswort oder auf vielen Geräten auch biometrische Identifikation, zum Beispiel Gesichtserkennung oder den Fingerabdruck.

Schlien Gollmitzer: In einem guten Passwortmanager ist alles verschlüsselt, also selbst für den Anbieter des Programms nicht lesbar. Der Schlüssel ist einmalig. Er wird zum Beispiel

aus deinem Masterpasswort plus einer sehr langen Zufallszahl erzeugt. Das heißt aber auch, auf das Masterpasswort musst du gut aufpassen. Wenn du es verlierst, gibt es keine Chance, die verschlüsselten Daten im Tresor wieder aufzusperren. Es ist bequem, es ist sicher.
Da fragt man sich, was sind eigentlich die Nachteile? Vielleicht haben tatsächlich zum Beispiel manche Nutzerinnen und Nutzer die Sorge, dass dieser Tresor so sicher dann eben doch nicht ist, weil es auch immer mal wieder Meldungen gibt, dass ein Passwortmanager tatsächlich doch geknackt worden ist, weil eine Schwachstelle in der Software ausgenutzt worden ist. Und deswegen haben also die BSI-Kolleginnen und Kollegen sich zehn Exemplare, wie gesagt von verschiedenen Passwortmanagern, sehr, sehr genau angeschaut und sie technisch untersucht. Halten die wirklich, was sie versprechen? Den Link zu allen Ergebnissen dieser Untersuchung findet ihr in den Shownotes.

Hardy Röde: Und bei mir im Interview ist jetzt Lars Bartsch. Er hat die Untersuchung geleitet. Hallo Lars, schön, dass du bei uns bist. Sag uns doch erstmal kurz, was genau du beim BSI alles machst.

Lars Bartsch: Ja, vielen Dank für die Einladung. Ich bin seit rund fünf Jahren im BSI als Referatsleiter. Das Referat nennt sich technischer Verbraucherschutz und Marktbeobachtung. Und hier bin ich mit meinem Team unterwegs. Wir führen technische Untersuchungen von Produkten und Diensten am digitalen Verbrauchermarkt durch.
Also im Prinzip direkt an der Schnittstelle von Anbietern und Verbrauchern. Und von daher ist das ein sehr, sehr interessantes Thema für uns.

Hardy Röde: Das heißt, ihr schaut sowohl den Firmen auf die Finger, die Produkte machen, als auch den Nutzerinnen und Nutzern sozusagen auf die Tastatur, was sie brauchen. Verstehe ich es richtig?

Lars Bartsch: Das kann man so ausdrücken. Wir versuchen mit den Herstellern, mit den Anbietern, einen Dialog zu führen. So würde ich das Ausdrücken, um Erkenntnisse zu generieren. Auf der einen Seite und auf der anderen Seite, um für unsere Anforderungen zu werben oder auch unsere Anforderungen durchzusetzen.

Hardy Röde: Und jetzt habt ihr gerade eine große technische Untersuchung durchgeführt über Passwortmanager. Warum macht ihr das überhaupt? Warum beschäftigt ihr euch mit Passwortmanagern?

Lars Bartsch: Die Motivation ist für uns erstmal ganz klar. Es geht um Accountschutz. Es geht um dieses allgegenwärtige Sicherheitsthema Accountschutz. Fast alle von uns haben dutzende Accounts, die wir in irgendeiner Form verwalten. Dort verknüpft sind persönliche Infos, Kontobuchungen, Bestellungen, alle möglichen sensiblen Daten. Das ist im Prinzip der Kernbereich des digitalen Alltags, was sich auf unseren Online-Accounts abspielt. Wir haben E-Mail-Accounts, die als Rückfalloptionen vielleicht auch dienen. Wir betreiben Online-Gaming oder alles Mögliche. Und letztlich mag ja keiner die Frustration von Accountübernahmen. Wenn sowas passiert, wenn Datenleaks passieren, wenn Identitätsdiebstahl passiert und was eben auch zu Rufschädigungen und digitaler Gewalt führen kann, finanzielle Schäden verursachen kann. Das heißt, es ist für uns halt erst mal

dieser Grundansatz, Accounts müssen abgesichert werden und dafür brauchen wir geeignete Werkzeuge.

Hardy Röde: Jetzt wären Passwörter ein ganz gutes Werkzeug, um sein digitales Leben abzusichern. Und trotzdem stellt ihr ja auch fest, habt ihr festgestellt in der Vergangenheit schon in anderen Untersuchungen, dass das immer wieder Verbraucherinnen und Verbraucher im Alltag vor Probleme stellt. Was sind denn die Probleme, die wir als ganz normale Nutzerinnen und Nutzer mit Passwörtern haben?

Lars Bartsch: Wir haben den Cybersicherheitsmonitor, eine regelmäßige Untersuchung, liebevoll von uns CyMon genannt, intern. Und da sehen wir zum Beispiel, Passwortmanager nutzen gerade mal 16 Prozent aller Verbraucher im Browser, es gibt auch die eigenständigen Passwortmanager, das nutzen gerade mal 10%. Also wir können erst mal feststellen rein empirisch, wir haben hier doch eine geringe Verbreitungsgröße. Aber das ist erst mal das, was wir feststellen und wir stellen auch fest, wir haben wenig Bewegung über die Zeit. Und das ist für uns halt erst mal eine Lage, die wir uns anschauen müssen.

Hardy Röde: Das heißt, kurze Zwischenfrage, das heißt, dass nicht wesentlich mehr Leute zu Passwortmanagern greifen, über die Jahre und mitkriegen, dass das was Gutes ist, sondern dass die, die es jetzt schon machen, die machen es und dass sich da aber nicht viel bewegt, richtig?

Lars Bartsch: Genau, so kann man das sagen. Also es ist für uns erst mal ein Handlungsauftrag. Auf der anderen Seite sehen wir eben in der gleichen Befragung, dass 44 Prozent aller Verbraucherinnen und Verbraucher ihre Passwörter für sicher halten. Da ergibt sich ja ein Problem, so ein logisches Problem tut sich da auf und bringen mich eben zu der These, dass Verbraucher ihre Passwörter zwar für sicher halten, diese aber offensichtlich über viele Accounts gleich verwenden. Weil sonst haben wir ein Problem, uns die zu merken, wenn wir eben keine Passwortmanager benutzen. Und das ist halt eine These zunächst mal, die halt uns dazu bringt, nochmal hervorzutun, was ist eigentlich unser erstes Gebot für starke Passwörter oder für starken Accountschutz, wo ich angefangen habe. Das erste Gebot ist, nutzt ein individuelles Passwort für jeden Account. Sonst seid ihr mit einer Schwachstelle, mit einem Leak komplett betroffen.

Hardy Röde: Dann schwenken wir wieder ein zu den Passwortmanagern. Was habt ihr euch genau angeschaut? Welche Produkte in dieser Untersuchung und wie seid ihr vorgegangen?

Lars Bartsch: Ja, was haben wir uns angeschaut? Also wir wollten zuerst mal sehen, was geht am Markt? Was geht am Verbrauchermarkt? Welche relevanten Produkte werden überhaupt angeboten? Das heißt, wir machen eine umfassende systematische Marktanalyse und haben in dem Fall festgelegt, dass wir uns zehn Passwortmanager genauer anschauen für eine Gefährdungsanalyse. Das haben wir mit unserem Projektpartner zusammen gemacht, mit dem Forschungszentrum Informatik. Wir müssen Risiken identifizieren und wir wollen Verbrauchern Empfehlungen ableiten. Das ist so ein zentraler Teil. Der andere Teil, wir wollen mit den Herstellern in den Fachaustausch treten. Also, habe ich ja schon erwähnt, welche Anforderungen sind wichtig? Welche Maßnahmen treffen die Hersteller? Wie können wir auch als BSI von den Herstellern lernen? Das ist auch genauso wichtig.

Hardy Röde: Dann springen wir doch mal gleich rein in ein paar eurer Ergebnisse und vielleicht fängst du gleich mit den Themen an, wo ihr gesagt habt, da funktioniert es noch nicht. Da gibt es Nachholbedarf bei den Herstellern. Bei diesen Technologien, da seid ihr nicht damit zufrieden als BSI.

Lars Bartsch: Was stellen wir fest jetzt in dieser Produktauswahl? Wir stellen zum Beispiel fest, dass in einigen Fällen die gespeicherten Passwörter so abgelegt werden, dass die Hersteller theoretisch oder praktisch darauf zugreifen können, auf die Daten.

Hardy Röde: Das sollte nicht so sein, würde ich mal sagen.

Lars Bartsch: Das sollte nicht so sein, ja. Das ist aus unserer Sicht eben auch ein No-Go. Selbst wenn man den Herstellern vertraut, ist es einerseits technologisch praktisch nicht erforderlich und eben auch nicht opportun. Und es erhöht natürlich auch potenziell die Angriffsfläche unnötigerweise. Das ist der erste Punkt. Der zweite Punkt ist, um ein bisschen technischer zu sprechen, dass manche Anbieter etablierte kryptographische Mechanismen, ich sage mal zweckentfremdet nutzen oder in nicht empfohlenen Konfigurationen nutzen.

Hardy Röde: Kannst du es konkreter machen, was das bedeutet? Es steht sicher drauf, aber es ist nicht sicher drin. Könnte man es so zusammenfassen?

Lars Bartsch: Kann man so sagen. Ich meine, wenn man Passwortmanager sagt, dann steht per se das sicher drauf. Und davon muss man auch verlässlich ausgehen können. Und kryptographische Mechanismen, die beispielsweise End-of-Life sind, wo man halt sagen, okay, die sind nicht mehr sicher, werden aber hier verwendet. Wie gesagt, deswegen sind wir im Dialog mit den Herstellern.

Lars Bartsch: Ich komme aber auch wieder ein bisschen von dieser technischen Schiene weg. Wir stellen eben auch fest, dass manche Passwortmanager, also die speichern ja nicht nur Passwörter. Passwortmanager speichern ja auch andere sensible Daten klassischerweise.
Benutzername oder die zugehörige Website. So, und auch hier, manche Anbieter speichern diese Daten unverschlüsselt ab. Da ist das Passwort vielleicht verschlüsselt, aber der Nutzername oder die Website nicht.

Hardy Röde: Das sollte auch nicht so sein, wenn ich mal mit gesundem Menschenverstand da reingehe.

Lars Bartsch: Genau, also ganz klassisches Beispiel. Je nach Art der Daten ist das natürlich unterschiedlich kritisch. Wenn ich zum Beispiel eine sichtbare Webadresse habe, eine Datingplattform, dann sollte die möglicherweise entsprechend geschützt sein. Damit mein Umfeld vielleicht nicht sieht, welche Zugangsdaten ich dort verwalte, auch wenn das Passwort, wie gesagt, nicht sichtbar ist. Bei Klartext ist immer ein Alarmzeichen, gerade bei Passwortmanagern. Ich habe noch zwei negative Punkte, will aber auch positiv schließen. Manche Hersteller halten sich tatsächlich auch sehr bedeckt mit der Dokumentation. Das heißt, wenn das eingeschränkt ist, diese Dokumentation, dann kann man nur noch auf Vertrauen bauen, sage ich mal so. Also hier empfehlen wir einfach auch stärker einen Open-

Source-Ansatz, weil dieser proprietäre Ansatz gerade, also proprietär im Sinne von verschlossen, wir können nicht reingucken, dieser Ansatz eben gerade bei Sicherheitsprodukten nicht für besonderes Vertrauen sorgt und eben auch nicht nachprüfbar ist. Ja, dann vielleicht auch was ganz Banales auch, was durchaus bemerkenswert ist, dass bei manchen Produkten die Einrichtung des Master-Passwortes nicht standardmäßig aktiviert war. Das hat uns durchaus überrascht. Natürlich brauchen Passwortmanager ein Master-Passwort oder irgendeine Art von Zugangsschutz.

Hardy Röde: Also wie ein Schlüsselkasten, der dauernd offensteht, bis man sich aktiv entschließt, ihn zuzusperren.

Lars Bartsch: Ja, absolut. Also auch das ist sehr, sehr bemerkenswert.

Hardy Röde: Klingt dann insgesamt aber schon nach einer ganzen Menge Dingen, die da schiefgelaufen sind. Die Liste ist echt beeindruckend. Bei den zehn Produkten, die ihr untersucht habt, sind denn dann überhaupt noch welche übrig geblieben, die ihr empfehlen könnt oder wo ihr sagt, da machen die Hersteller alles richtig. Und da gibt es jetzt wirklich einfach das beruhigende Gefühl für mich als Nutzer oder die Informationen von euch. Da kann ich darauf vertrauen.

Lars Bartsch: Also grundsätzlich tut man es natürlich schwer, einzelne Produkte herauszustellen. Aber aufgrund unserer Ergebnisse können wir zunächst sagen, dass die KeePass-Reihe, da gibt es verschiedene Derivate von, die wir uns hier angeschaut haben, doch sehr gut abschneiden. Wichtig ist uns natürlich, dass bestimmte Funktionalitäten, die optional sind, natürlich sicher oder unsicher ausgelegt werden. Und da ist es natürlich die Frage an die Nutzer, brauchen wir diese Funktionalitäten und nutzen wir überhaupt dieses Produkt oder habe ich ein anderes Produkt, was vielleicht nicht in der Liste ist. Also da immer mit dem Disclaimer dazu. Es gibt noch viele Produkte, die wir nicht untersucht haben und die wir vielleicht auch in der Form hervorheben könnten oder nicht. Wir haben sie jetzt schlichtweg nicht betrachtet und das ist ganz wichtig zu berücksichtigen.

Hardy Röde: Du hast schon die Funktionen angesprochen, die verschiedene Passwortmanager mitbringen, verschiedene Produkte. Welche sind denn essenziell? Was sagt ihr denn, was sollte drin sein? Mindestens in so einer Passwortmanager-Software. Was soll so ein Passwortmanager denn tun? Frag ich mal nochmal so banal.

Lars Bartsch: Also, der verwaltet natürlich unsere Zugangsdaten, er verwaltet andere sensible Infos wie ein Notizbuch und das in einer sicheren Umgebung, also in einem abgeschlossenen Raum. Die Metapher hatten wir schon. Also für mich ist so die Kernbotschaft, stellt euch mal vor, ihr verliert euren Fahrradschlüssel und du verlierst deinen Fahrradschlüssel und du musst dann darum bangen, dass jetzt jemand deine Wohnung aufschließen kann oder mit deinem Auto wegfährt. Das wäre ein No-Go. Das heißt, jedes Schloss hat einen individuellen Schlüssel und darum muss auch jeder Account ein individuelles Passwort haben und da komme ich jetzt zu der Kernfunktionalität, weil das kann ein Passwortmanager problemlos machen. Er kann sich viele Dinge für dich merken. Das ist nicht das Problem. Die zweite Kernanforderung, so ein Passwortmanager hat natürlich einen integrierten Passwortgenerator. Das heißt, er kann selbstständig Passwörter erstellen und hat idealerweise auch ein transparentes Maß für die Passwortstärke.

Hardy Röde: Die also sicher sind nach den gängigen Standards, wie komplex ein Passwort sein soll und schwer zu erraten.

Lars Bartsch: Ganz genau. Wir sprechen auch gern von starken Passwörtern. Also die Zufälligkeit ist da das Relevante. Das muss gegeben sein. Es ist sehr wünschenswert, dass ein Zwei-Faktor-Möglichkeit gegeben ist. Also zwei Faktor-Authentisierung und das ist zweierlei. Also auf der einen Seite kann das eine Funktion sein, um den Passwortmanager selber zu entsperren. Auf der zweiten Seite kann das relevant sein für bestimmte Zugangsdaten, dass ich in den Passwortmanager diesen zweiten Faktor mit hinterlegen kann. Klassisch ist da One-Time-Passwort, OTP, die sich zum Beispiel zeitbasiert in bestimmten Abständen immer ändern. Was noch wichtig ist an Funktionalität, die Warnung vor gefälschten Websites. Auch das können Passwortmanager gut bewerkstelligen als Phishing-Schutz. Das heißt, die Zugangsdaten werden von dem Passwortmanager nur freigegeben, wenn die konkret damit verknüpfte Domain auch zutrifft. Also ich will mich bei meinem E-Mail-Anbieter einloggen und der Passwortmanager checkt, bin ich wirklich auf der richtigen Webadresse. So und damit verhindere ich effektiv Phishing. Klassischer Angriffsvektor „Typosquatting“ beispielsweise. Also man nutzt kleine Unterschiede. Man kriegt eine Phishing-Mail, da steht halt nicht Google mit zwei O, sondern Google mit drei O. Und das Auge übersieht das sehr schnell. Gerade wenn man hektisch was anklickt. Ja und natürlich, was auch wichtig ist, nachhaltig ist, sage ich mal, ist eine Backup-Funktion.
Kann man darüber streiten, ob das jetzt in dem Programm selber integriert sein muss.
Es kommt dann wieder sehr stark auf den digitalen Alltag der jeweiligen Person an, also traue ich mir das auch zu, dass ich, ich sage mal die Passwortdatei selbstständig kopiere, dass ich das auch regelmäßig mache, das dann separat verwahre. Oder vertraue ich auf der anderen Seite einen Anbieter und machen Cloud Backup, weil ich dann einfach „usable“ für mich habe. Das sind ganz unterschiedliche Nutzungsszenarien. Aber wichtig ist, macht einen Backup, egal ob Cloud oder lokal. Und deswegen ist es auch eine wichtige Funktion.
Vielleicht wenn ich noch schließen kann mit dem letzten Punkt. Der „digitale Nachlass“ ist auch so ein großes Thema. Auch hier gibt es Passwortmanager, die solche Notfall-Hintertüren mit anbieten. Also es gibt einen Weg, wo man ohne Kenntnis der eigentlichen Zugangsdaten trotzdem Zugriff bekommt. Und das kann schwierig sein. Das muss gut implementiert sein, um keinen zusätzliche Angriffsvektor zu bieten. Auch hier noch einmal das Stichwort digitale Gewalt, also wenn es um das soziale Nahfeld geht, ist so ein Nachlass möglicherweise problematisch oder halt möglicherweise sehr hilfreich, das muss man sich individuell angucken.

Hardy Röde: Du hast das Thema Backup schon angesprochen und jetzt ist tatsächlich mein Passwortmanager, wenn ich da ganz viele Passwörter drinstehen habe sehr, sehr hilfreich, sehr sehr komfortabel. Wenn ich dir so zuhöre bei der Liste an Features, das möchte ich eigentlich nicht missen im digitalen Alltag. Das ist eigentlich viel zu gut, um es nicht zu nutzen. Aber alles steckt natürlich da drin. Also wenn ich da nicht mehr reinkomme, sei es, weil die Passwortdatei auf irgendeine Weise verloren geht, wo alles drinsteht oder wenn ich auch das Masterpasswort vergesse und das nicht mehr herstellen kann, dann schau ich vielleicht ein bisschen komisch drein und der Tag nimmt einen anderen Verlauf als geplant. Wie kann ich mich dann davor schützen, als Nutzerin, als Nutzer?

Lars Bartsch: Ja, da gibt es verschiedene Antworten. Also die eine Antwort ist, mach ein Backup davon. Also auch von dem Masterpasswort sollte ein Backup gemacht werden. Das muss jeder für sich entscheiden letztlich. Auf der anderen Seite kann es auch sinnvoll sein, eben einen anderen Weg zu gehen. Also es gibt auch Passwortmanager, die die bieten an, so ein Notfallblatt auszudrucken, wo diese wichtigen Informationen zusammengefasst sind. Das kann durchaus eine Lösung sein, weil für die meisten oder für viele Menschen eben dieser physische Zugriff auf ein Dokument eine hohe Relevanz hat. Und dann ist das eine sinnvolle Strategie neben der Merkfähigkeit oder wie schon genannt anderen Notfall-Hintertüren auch im Sinne des „digitalen Nachlasses".

Hardy Röde: Jetzt habt ihr zwei Browser integrierte Passwortmanager euch angeschaut und ansonsten nur eigenständige Software für verschiedene Plattformen. Ich kann mir vorstellen, dass viele Nutzerinnen und Nutzer einfach aus Bequemlichkeit, weil es schon da ist, einen Browser integrierten Passwortmanager nutzen. Was sagt ihr da generell? Hat das eine grundsätzliche Vorteile, das andere Nachteile? Was empfiehlt ihr da?

Lars Bartsch: Ja, also bei Pauschalaussagen kann man oft nur relative Angaben machen. Das würde ich auch hier machen. Das heißt, es ist besser als nichts, weil man hat einfach eine niederschwellige Zugänglichkeit, man hat eine direkte Integration. Also jeder, der es nutzt, kennt das. Es wird auch regelmäßig gefragt. Ich log mich irgendwo ein, der Browser fragt mich: „Soll ich das für dich speichern?" Das heißt, es ist sehr „usable", es ist sehr praktisch. Das ist die eine Seite und jeder, jede sollte sich damit beschäftigen. Reicht mir das, reicht mir es auch an Funktionalität, wenn ich alles, was ich jetzt zum Beispiel an Funktionalität aufgezählt hat, ist in den Browser-Passwortmanagern mit enthalten. Das ist die eine Seite und die andere technische Seite ist, das ist so eine wünschenswerte Anforderung, Programm und Funktionalitäten möglichst zu trennen. Das heißt auf der einen Seite der Browser, auf der anderen Seite habe ich die sichere Verwahrung meiner Passwörter. Wenn ich das zusammenlege, dann habe ich theoretisch erst mal eine komplexere Angriffsfläche. Ich muss immer daran denken, dass so einen Browser kann man beschreiben als ein separates Betriebssystem, das heißt es ist eine sehr, sehr komplexe Anwendung heutzutage und der Passwortmanager, der dort integriert ist, ist vielleicht nicht immer im Hauptfokus der Hersteller, sondern da geht es um andere Faktoren. Da geht es darum, dass man ein gutes Browsing-Erlebnis hat usw. Also wenn man sich dessen bewusst macht, muss man für sich dann eine Entscheidung treffen. Wie gesagt, meine pauschale Antwort wäre besser als nichts. Aber sicherlich nicht konkurrenzfähig, auch was die Funktionalität angeht mit einem eigenständigen Passwortmanager.

Hardy Röde: Ich glaube als Poweruser oder - userin wird man von selber zu einem Passwortmanager greifen, weil es auch einfach eine wahnsinnig komfortable Möglichkeit ist, mit den Passwörtern umzugehen. Und sie ist auch noch sicher. Also es gibt kaum einen Grund, ihn nicht zu verwenden. Wenn ich aber zum Beispiel - keine Ahnung - einmal im Vierteljahr mein Onlinebanking benutze, dafür ein bestimmtes Passwort eine Nutzererkennung habe, dann ist mir der Passwortmanager möglicherweise zu viel Aufwand und ich kann sehr, sehr gut verstehen, was rätst du denn dann solchen Menschen? Wie sollen sie mit ihren Passwörtern umgehen?

Lars Bartsch: Also im konkreten Szenario, das wirklich ganz selten mit Passwörtern konfrontiert ist, da ist einfach die Hürde, sich mit so einer Software zu beschäftigen, zu hoch. Das ist so, das heißt, unsere Quintessenz daraus ist lieber eine sichere analoge Speicherung als eine unsichere digitale Speicherung. Das mag sich fürs BSI ungewöhnlich anhören, aber wir müssen durchaus auch sehen, dass je nach Nutzungsszenario, je nach unterschiedlichen Zielen, die zu erreichen sind, das eben auch besser ist und antworten. In dem Szenario, wo du sagtest, eine Person braucht nur einmal im Monat einen Bankauszug digital, in so einer Weise kann das sinnvoll sein, wenn man sich bewusst ist und das ist auch der springende Punkt. Macht euch bewusst, was ihr für Anforderungen habt. Und an der Stelle muss man halt mit vielen Funktionseinschränkung dann auch leben. Also ich werde kaum erfahren, wenn mein Passwort an irgendeiner Stelle ge-leaked wurde. Ich muss mir natürlich auch anderweitig zum Backup Gedanken machen. Wer kommt da noch an meinen Safe ran? Und ist das eine gute Entscheidung, dass diese Person dran kann?

Hardy Röde: Wenn ich nach dem Hören dieses Gesprächs und dieser Update verfügbar Folge mir denke: „Ach komm, vielleicht sollte ich es mal versuchen und sehe aber da so eine riesen Hürde vor mir.“ Was empfiehlst du mir? Wie schaffe ich einen guten ersten Schritt? Was ist ein schnelles Erfolgserlebnis, wenn ich mir einen von euch empfohlenen Passwortmanager einrichten will?

Lars Bartsch: Ja, da würde ich auch ganz „hands-on“ sagen. Einfach machen. Also aus zuverlässigen Quellen das Ding einfach mal runterladen, installieren auf der bevorzugten Plattform und dann einfach mal damit rumspielen. Also probiert und guckt, ob ihr davon einen Mehrwert habt. Gerade wenn es darum geht, ein sicheres Masterpasswort anzulegen und sich nicht mehr merken zu müssen.

Schlien Gollmitzer:
Das ist schon wieder so ein super interessantes Interview, das du da geführt hast, Hardy. Und schon wieder rattert es in meinem Kopf. Wie soll es jetzt weitergehen? Für welchen Passwortmanager entscheide ich mich letztlich? Ich merke, es gibt also Unterschiede und man kann sich da sozusagen den personalisierten mehr oder weniger raussuchen für genau meine Bedürfnisse, die ich so habe.

Hardy Röde:
Ja, genau. Also wenn du zum Beispiel sagst, ich brauche das überhaupt nicht, dass der über alle meine Geräte hinweg meine Passwörter und Zugangsdaten synchronisiert, wenn ich einfach immer mein Handy dabei habe und das immer benutze, wenn ich ein Passwort nachschauen oder mich einloggen möchte, dann reicht auch einer, der sich nicht synchronisiert, über die Geräte hinweg. Und das schließt natürlich sofort wieder eine potenzielle Sicherheitslücke durch die Synchronisierung aus.
Also es lohnt sich da auch zu schauen, was brauche ich wirklich? Das habe ich schon auch mitgenommen aus den Gesprächen von außen

Schlien Gollmitzer: Ja, aber er erfordert von mir dann viel Disziplin, weil ich darf auf gar keinen Fall mein Masterpasswort oder mein Handy verlieren. Das halten wir auf jeden Fall schon mal fest. Also ich werde mir diese Liste jetzt dann gleich noch mal anschauen, die wir

in den Shownotes zusammengefasst haben, diese Tests entsprechend und werde mir dann den besten raussuchen. Mein großer Vorteil ist Hardy, ich muss nicht 600 Accounts umziehen, sollte ich mich für einen anderen Manager entscheiden

Hardy Röde: Du hast es gut, Schlien.

Schlien Gollmitzer: Das war's auch schon wieder mit unserer Folge 60 von Update verfügbar. Wie immer noch mal der Hinweis, wenn euch diese Folge gefallen hat und wenn ihr auf keinen Fall weitere Folgen verpassen möchtet, dann hinterlasst uns doch gerne ein Like, ein Herzchen, ein Sternchen, eine Glocke oder was hinterlässt man denn alles so egal was auch immer ihr entbehren könnt, hinterlasst es uns gerne. Oder auch mal einen kritischen Kommentar, wenn ihr wollt, auf der Podcast Plattform eurer Wahl.

Hardy Röde: Viel zum Nachlesen gibt es auch. In dieser Episode haben wir euch alles in die Shownotes gesteckt und für alle anderen Fragen zum digitalen Alltag und zu Cybersicherheit da findet ihr viele, viele Informationen vom Team des BSI auf Instagram, Bluesky, Mastodon und auf YouTube. Auch da lohnt sich das Abonnieren.

Schlien Gollmitzer: Bis zum nächsten Update.

Hardy Röde: Bis zum nächsten Update.