„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 10, 30.07.2021:

Bezahlmethoden im Check: Onlineshopping ohne böse Überraschung

Moderation: Ute Lange, Michael Münz
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lange: Hallo und herzlich willkommen zur neuen Ausgabe von „Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz. Wir melden uns auch in diesem Monat wieder nicht aus dem Bundesamt für Sicherheit in der Informationstechnik in Bonn, sondern wegen der Pandemie auch diesen Monat aus dem Home-Office.

Lange: Zunächst einmal herzlichen Dank für Ihre vielen Rückmeldungen zu unserem Aufruf in der vergangenen Woche. Wir wollten von Ihnen gern hören, ob Sie beim Onlinebezahlen schon einmal schlechte Erfahrungen gemacht haben, und, wenn ja, welche? Wir haben etliche Rückmeldungen bekommen und es scheint gar kein so seltenes Phänomen zu sein, aber dazu später mehr.

Münz: Genau! Bevor wir in das Thema „online einkaufen und bezahlen“ einsteigen, wollen wir noch einmal auf zwei Themen eingehen, die wir in diesem Podcast schon behandelt haben und die seit unserer letzten Folge Schlagzeilen gemacht haben. Es geht um zwei spektakuläre Erpressungsversuche, bei denen Hacker Systeme gekapert haben und erst nach einer Lösegeldzahlung wieder freigeben wollen. Diese beiden haben unsere Aufmerksamkeit erhalten.

Lange: Zum einen wurde die US-Firma Kaseya Opfer eines Erpressungsversuchs per Hack. Der Fall ist brisant, weil diese Firma eine Software anbietet, mit der deren Kunden wiederum Softwareupdates in ihren Computersystemen verwalten können. Das heißt, wenn ich da eindringe als Hacker, habe ich natürlich ziemlich weit offene Türen zu anderen Firmensystemen. Das zeigt, dass der Schaden durch einen Hack in einer Firma sich vervielfältigt, auf Tausende von anderen. Etwas Besonderes an diesem Fall ist auch, dass Kaseyas Kunden IT-Dienstleister sind, die wiederum ihren Kunden diese Software anbieten, aber oft nicht unter dem Namen, der jetzt viel in der Presse stand, sondern unter dem jeweiligen Namen ihrer eigenen Firma. Das heißt, viele Firmen wissen vielleicht noch gar nicht – es sei denn, sie haben jetzt schon recherchieren lassen, dass sie genau diese Software auf ihren Systemen haben und unter Umständen schon infiziert sind. Es ist wie ein

Schneeballsystem, ein Dominoeffekt, über den wir auch schon oft gesprochen haben. Du machst eine Tür auf und dadurch gehen eine ganze Menge andere Türen auf.

Münz: Hast du konkrete Beispiele, wie sich das ausgewirkt hat? Konnten Verbraucher und Verbraucherinnen am Ende merken, dass da etwas versiegt ist?

Lange: Ja, allerdings! Ich habe gelesen, dass in Schweden die Supermarktkette Coop betroffen war. Sie musste direkt nach Bekanntwerden des Hacks fast alle ihre Läden schließen. Bei denen ging wohl offensichtlich gar nichts mehr für eine kurze Zeit. Auch deutsche Unternehmen waren von dem Angriff betroffen. Wobei sie glücklicherweise wohl nicht so stark wie in anderen Ländern betroffen waren, weil dieser Hack an einem Freitagnachmittag deutscher Zeit passierte. Viele waren schon nicht mehr so aktiv und konnten auf die Meldung reagieren. Systeme, die diese Software haben, wurden sofort abgeschaltet und es wurde erst einmal abgewartet, bis die Ursache gefunden und auch eine Lösung gefunden war und ist. Die Mitarbeiter beim BSI hier in Bonn haben eine Nachricht bekommen von einem IT-Dienstleister in Deutschland, der auch mitgeteilt hat, dass seine Kunden betroffen seien. Da handelt es sich um etwa 1.000 Computer bei mehreren Unternehmen. Aber das BSI hat auch gesagt, dass es noch gar nicht ausgeschlossen ist, dass nicht später noch Probleme festgestellt werden. Das hatten wir schon einmal in einer anderen Folge: Wenn irgendwo eine Infektion in dem System ist, kann es manchmal Wochen oder Monate dauern, bis man das feststellt oder bis es tatsächlich zum eigentlichen Angriff kommt.

Münz: Weiß man, wer dahintersteckt? Wie ist das ausgegangen?

Lange: Ja, das ist die Hackergruppe REvil. Die stand hinter diesem Hack. Die hat ursprünglich 70 Millionen Dollar für die Freigabe des Schlüssels gefordert. Nach den jüngsten Meldungen hat Kaseya den Schlüssel wohl auch bekommen und kann jetzt hoffentlich alle Systeme ihrer Kunden wieder freischalten.

Münz: Okay, das klingt doch nach einer Lösung!

Lange: Hoffnungsvoll!

Münz: Wir hatten von zwei Erpressungsfällen gesprochen und der zweite ist in Deutschland. Ich habe den herausgesucht, weil der auch erhebliche Kollateralschäden hat, die über die eigentlich betroffene Institution hinausgehen. Es handelt sich um den Hack der Verwaltung des Landkreises Anhalt-Bitterfeld. Der liegt nördlich von Leipzig in Sachsen-Anhalt. Das Besondere ist: Dadurch, dass die Verwaltung lahmgelegt worden ist, konnten zum Beispiel auch Sozialleistungen nicht ausgezahlt werden. Das heißt, der Kreis der Betroffenen ging über das eigentliche Angriffsziel hinaus. Es ist besonders perfide, dass letztendlich Menschen betroffen sind, die eigentlich mit dem System als solchem nichts zu tun haben, die aber Sozialleistungen brauchen und diese jetzt gerade durch den Hack nicht bekommen können. Mittlerweile hat ein Team von rund 100 Mitarbeitenden das Notsystem starten können. Es hat die Arbeit in Teilen wieder aufnehmen können. Aber bis alles wieder funktioniert, wird es

wohl noch ein bisschen dauern. Der Landkreis Anhalt-Bitterfeld hat zudem angekündigt, sich nicht erpressen zu lassen.

Lange: Ich nehme an, dass es da um Wohngeld und andere Sozialleistungen geht. Das ist besonders kritisch, weil die, die diese Leistungen in Anspruch nehmen, sie dringend brauchen. Gut, dass das so schnell gelöst werden konnte bzw. ein Notsystem aufgebaut werden konnte! Für mich zeigen allein diese beiden Beispiele, wie wichtig der sichere Schutz von IT-Systemen geworden ist! Das kriegt eine immer größere Bedeutung. Ich habe kürzlich einen Artikel über Digitalisierung und diese zunehmenden gesellschaftlichen Auswirkungen gelesen. Da war ein Bild, das bei mir hängengeblieben ist. Und zwar stand da so in etwa, dass ein einzelner Hacker mit einem Laptop erheblichen Schaden anrichten und ganze Infrastrukturen lahmlegen kann. Das sind genau diese Beispiele. Umso wichtiger war für mich dann die Schlussfolgerung nach den beiden Fällen und auch nach dem Lesen dieses Artikels, der sich noch mit mehr Aspekten beschäftigt hat, dass wir als Normalsterbliche erstens selbst über diese Dominoeffekte Opfer von den Attacken werden können; obwohl wir vielleicht nicht die erste Angriffsstufe sind. Ich habe außerdem daraus gezogen, dass wir aber auch umgekehrt natürlich an vielen Stellen dafür sorgen können, dass IT-Systeme sicher sind, also auch in unseren Firmen etc. Ein Beispiel ist dein Lieblingsthema Phishing und Anhänge in E-Mails, die man lieber vorsichtig betrachten sollte – lieber einen weniger öffnen als nötig. Unser anderes wiederkehrendes Thema sind Passwörter. Die sollen unbedingt sicher sein. Da gibt es ganz viele Tipps und am besten verlinken wir die noch einmal in den Shownotes und weisen auf die Webseiten des BSI hin! Wer immer noch 1 2 3 4 5 6 7 als Passwort hat, sollte jetzt dringend noch einmal darüber nachdenken, dieses zu ändern.

Münz: Das Bild von dem einzelnen Hacker am Laptop geht eigentlich auch in die andere Richtung. Jeder von uns, der am Laptop sitzt und im Netz unterwegs ist, kann letztendlich auch ein Einfallstor sein für solche Hacker. Ich kann durch Phishing oder einfache Passwörter den Zugriff auf andere Systeme erlauben, die sozusagen hinter mir liegen oder die ich verwalte. Ich habe noch einmal für mich verinnerlicht, dass es nicht nur darum geht, dass ich mich und mein Bankkonto schütze – dazu kommen wir ja auch gleich, sondern dass ich letztendlich auch Teil einer Gesellschaft bin, die ich auch schützen kann, indem ich mich an bestimmte Regeln halte. Die verlinken wir in den Shownotes, wie du schon gesagt hast, und dann können Sie, Hörerinnen und Hörer, sich noch einmal anschauen, wo Sie gegebenenfalls noch ein bisschen mehr Sicherheit für sich, aber auch für alle anderen, schaffen können. Damit kommen wir zum eigentlichen Thema der heutigen Folge: online bezahlen. Denn das Einkaufen im Internet hat nicht zuletzt bedingt durch Corona deutlich zugenommen. Ich habe ein paar Zahlen rausgesucht, die das belegen. Im Jahr 2020, also im vergangenen Jahr, belief sich der Umsatz im E-Commerce, also der Handel zwischen Onlinehändlern und uns, in Deutschland auf 72,8 Milliarden Euro. Das sind 23 Prozent mehr als im Jahr davor. Das ist ein sehr starkes Wachstum. Man kann, glaube ich, sagen, dass der Onlinehandel zu den klaren Gewinnern der Coronakrise gehört.

Lange: Von denen gibt es ja nicht so viele, wie wir wissen.

Münz: Aber der Onlinehandel gehört auf jeden Fall dazu!

Lange: Woher hast du denn die Zahlen?

Münz: Ich habe unter anderem in einem Bericht zum digitalen Verbraucherschutz des BSI nachgeguckt. Da heißt es, dass 71 Prozent der deutschen Bevölkerung inzwischen Onlineshopping betreiben.

Lange: Das sind ja fast Dreiviertel!

Münz: Genau, und fast die Hälfte, also 44 Prozent, der Straftaten im Internet fallen aber auf Betrug beim Onlineshopping zurück. Das heißt, mehr Leute kaufen online ein, aber die Fallzahl für Betrug beim Onlineshopping ist offensichtlich recht hoch. Nachdem wir im vergangenen Jahr das Thema Fakeshops hatten, wollen wir uns deswegen in dieser Folge das Thema Bezahlverfahren anschauen. Wie kann ich sicher sein, dass ich für mein Geld auch die entsprechende Ware oder Dienstleistung erhalte? Was kann ich tun, wenn das Geld zwar unterwegs ist von mir zum vermeintlichen Verkäufer, aber meine Bestellungen nicht auf dem Weg zu mir?

Lange: Das greifst du ein ganz aktuelles Thema auf, weil es diesen Fall häufig gibt in Situationen, in denen Menschen es sowieso schon nicht so leicht haben: Bestellungen werden getätigt und es kommt keine Ware, aber das Geld ist weg. Aktuell etwa, in der Flutsituation bei uns in der Region, gibt es Fakeshops im Internet, die sich gezielt an die Bedürfnisse der Betroffenen richten. Wir haben alle gelesen und gehört, dass jetzt gerade Bautrockner sehr gefragt sind, weil alles voller Schlamm ist. Die Häuser sind feucht. Die Polizei in Bonn hat kürzlich darüber berichtet, dass es jetzt tatsächlich dafür Internetshops gibt, die sehr günstig Bautrockner anbieten. Weil sie so dringend benötigt werden, sind auch viele bereit sofort dafür zu bezahlen. Das Problem ist offensichtlich nur, dass vieles von dieser Ware, die da bestellt wurde, gar nicht ankommt. Das ist echt schäbig: In einer Zeit, in der Menschen sowieso schon fast alles oder alles verloren haben, sie dann noch übers Ohr zu hauen. Aber wir hatten ja auch schon einmal darüber gesprochen. Als wir über Fakeshops gesprochen haben, dass Kriminelle, die sich darauf spezialisieren, eben auch saisonal arbeiten bzw. sich an bestimmten Interessen orientieren. Jetzt sind es Bautrockner.

Münz: Vom letzten Mal habe ich mir die Dirndl-Mafia gemerkt. Auch die Playstation 5 war ein Beispiel, was wir hatten. Wir hatten relativ ausführlich erklärt, wie man vertrauenswürdige Shops erkennt. Wir stellen die Infos in die Shownotes, damit man da auf dem Laufenden ist.

Lange: Ja! Es ist aber nicht nur wichtig, dass man diese Fakeshops erkennt, und dass man sich ein bisschen sorgfältiger informiert, sondern auch, wie man sicherstellen kann, dass man eine sichere Bezahlmethode nutzt. Für welche entscheide ich mich und welche gibt es? Das wollen wir uns heute einmal genauer anschauen. Gibt es denn die eine sichere Methode? Ich hoffe jetzt auf die Antwort, dass ich am Ende weiß, was ich tun muss.

Münz: Jein! Es gibt eine sehr sichere! Aber das ist nicht immer das, was man angeboten bekommt! Es gibt stattdessen mittlerweile ganz viele Online-Bezahlverfahren mit unterschiedlichen Vor- und Nachteilen. Es gibt aber eine, die Betrüger gerne nutzen. Dabei handelt es sich um die Vorkasse: Sprich, ich überweise das Geld und warte dann auf meine Ware.

Lange: Wie bei den Bautrocknern!

Münz: Genau! Das interessante: Wenn ich mich an meine ersten Einkäufe bei Online-Aktionsplattformen erinnere vor 20 Jahren, war Vorkasse immer noch gang und gäbe. Ich habe etwas ersteigert. Dann musste ich warten, dass ich vom Verkäufer die Kontodaten bekomme. Dann habe ich überwiesen. Der Verkäufer hat den Erhalt des Geldes bestätigt und dann erst die Ware losgeschickt. Klar, ich konnte anhand der Bewertungen einen Eindruck bekommen, wie vertrauenswürdig der Verkäufer oder die Verkäuferin ist. Aber das war natürlich keine Garantie. Außerdem hat es vom Kauf bis zum Erhalt der Ware manchmal über eine Woche gedauert; wenn zum Beispiel noch ein Wochenende dazwischen lag und die Überweisung dann noch länger gebraucht hat. Das will ich natürlich nicht. Wenn ich jetzt – und das wollen wir ja alle – etwas im Netz kaufen will, dann möchte ich nicht ewig lange warten, dass es kommt, sondern möchte, dass es schnell geliefert wird.

Lange: Vor allen Dingen machen wir es ja nicht mehr unbedingt nur in der Nachbarschaft. Ich kann mich erinnern, dass es früher manchmal Leute waren, zu denen man hingegangen ist und bei denen man die Ware abgeholt und ihnen Bargeld überreicht hat. Heute kannst du weltweit bestellen und du hast fast keinen Kontakt mehr zu den Verkäufern und Verkäuferinnen.

Münz: Da stimmt! Da hast du völlig recht! Es gibt mehrere Optionen zum Bezahlen, die man sich angucken oder auch nutzen kann. Ich für mich guckt mittlerweile immer nach Bezahlmöglichkeiten per Online-Bezahlanbieter, also PayPal oder Giropay. Ich lege mir dort ein Konto an, verbinde dieses mit meinem Bankkonto und wickele es darüber ab. Zum einen geht es schnell – das Geld ist oft innerhalb weniger Sekunden oder Minuten bei dem Verkäufer angekommen, zum anderen habe ich so einen Überblick, wohin ich überall Geld überwiesen habe. Spätestens bei der Steuererklärung freue ich mich, dass alle Daten an einem Ort sind. Mittlerweile schätze ich auch sehr, dass diese Online-Bezahldienste eben nicht nur online funktionieren, sondern auch offline helfen können. Ich bin einmal mit dem Taxi gefahren und ich frage bei jeder Taxifahrt, ob ich mit Karte zahlen kann, weil ich selten Bargeld habe. Der Taxifahrer sagte: „Ja klar, kein Problem!“. Dann fuhren wir und als wir ankamen, funktionierte das Kartenlesegerät nicht. Oft werden Bluetooth-Geräte genutzt, die sich mit dem Handy verbinden müssen. Das hat nicht geklappt und so weiter und so fort.

Lange: Ich hatte das auch schon. Das ist total doof!

Münz: Es ist ja nicht so, dass ich nicht bezahlen will. Dann haben wir überlegt, was funktionieren könnte und was nicht funktioniert. Am Ende fiel mir ein, ob es vielleicht über einen Online-Bezahldienst klappen könnte. Wir hatten beide beim selben Dienst einen

Account. Er hat mir seinen Namen genannt und ich konnte ihm das Geld dann von der Rückbank per Handy auf sein Handy überweisen. Es war echt eine coole Notlösung an der Stelle, wo ich auch gedacht habe: „Okay, Online-Bezahldienste helfen auch offline“. Du hast gerade das Stichwort weltweit genannt: Wenn ich im Ausland Sachen bestelle, ist ein Online-Bezahldienst eine super unkomplizierte Methode, um das Geld von einem Land ins andere zu bekommen.

Lange: Das klingt jetzt fast zu schön, um wahr zu sein. Alles tutti! Gibt es denn auch Nachteile? Auf was sollte ich achten, wenn ich diese Bezahlmethode wähle? Welche Tücken verbergen sich da vielleicht?

Münz: Es wird oft damit geworben, dass es so eine Art Versicherung dafür gibt, dass du dein Geld zurückbekommst, wenn deine Ware nicht kommt oder so. Aber das ist wie bei so vielen Rücktrittsversicherungen: Es müssen bestimmte Bedingungen eintreten, damit dieser Schutz in Kraft tritt. Du kommst zum Beispiel bei dem einen Dienst den Kaufpreis zurück, wenn der Händler das Produkt nicht verschickt hat. Wenn der aber sagt, er habe es verschickt und es kam nicht bei dir an…

Lange: Und der Nachbar freut sich jetzt daran!

Münz: Meine Nachbarschaft ist natürlich ganz ordentlich und brav. Da würde so etwas nie passieren! Aber ja, in so einem Falle wäre dann die Ware weg und das Geld auch! Aber ich bin echt froh: Bislang ist mir bei diesen Bezahlverfahren eigentlich nichts passiert. Ich habe nochmal Zahlen dazu nachgeschaut. Ich bin mit dieser Auffassung nicht allein, denn rund ein Viertel der Onlineshopper nutzt laut einer Umfrage des Instituts des Handels aus dem Mai 2021 solche Online-Bezahldienste. Kauf auf Rechnung ist auch mit rund einem Drittel dabei; Lastschrift und Bankeinzug auch. Das sind die drei häufigsten genutzten Dienste, um Sachen, die ich online bestelle, zu bezahlen.

Lange: Meine Variante ist noch nicht genannt. Ich habe mich in der Vorbereitung für die Folge ein bisschen umgeschaut, was ich denn viel mache, weil mir ehrlich gesagt noch nichts Gravierendes passiert ist. Wir hatten Einspielungen oder Hinweise von Hörern und Hörerinnen. Wir haben auch ein bisschen gelesen. Du hast vorhin die Zahlen genannt, dass sehr viele Menschen davon betroffen sind. Ich bisher noch nicht! Ich weiß nicht genau, woran es liegt, aber ich habe einmal geschaut, was ich so viel mache. Ich habe auch schon die Online-Bezahldienste genutzt, aber ich habe festgestellt, dass ich sehr viel meine Kreditkarte nutze und die bei vielen wiederkehrenden Vorgängen hinterlegt habe. Ich bin Vielfahrerin bei der Bahn bzw. war es vor Corona und hoffe auch, dass das demnächst wieder möglich ist, weil mir das ein bisschen fehlt, durch die Welt zu kommen. Da habe ich in der App alles hinterlegt: meine ganzen Daten, meine Kreditkarte. Ich finde das super. Einmal eingerichtet, inklusive dieses extra Sicherheitsverfahrens, das es da ja jetzt auch gibt bei Kreditkarten! Das geht super flott. Ich war letzte Woche bei einer Freundin und hatte mich kurzfristig entschieden: Da war das mit meiner App auf dem Handy und am Gleis in einer Minute fertig! Das war schneller als der Fahrkartenautomat am Gleis, denn da muss man immer erst den richtigen Tarif finden und dann klappt der ja nicht. Dann habe ich nicht das richtige Kleingeld

oder er will die Karte nicht. Ich finde das super und wenn das einmal eingerichtet ist, ist das auch gar nicht so kompliziert. Der Vorteil ist: Wenn ich mal eine Abbuchung auf der Kreditkarte habe, die mir ein bisschen seltsam vorkommt, dann kann ich das natürlich sofort melden. Sollte mal jemand, was mir Gott sei Dank noch nicht passiert ist, meine Kreditkarte missbrauchen oder sie kommt abhanden, dann kann ich sie schnell sperren bzw. ich kann die Zahlung wieder zurückfordern. Das finde ich ganz angenehm!

Münz: Das ist tatsächlich etwas, was ich bei Kreditkarte auch gut finde. Das Sicherheitsgefühl, das ich da habe, ist relativ hoch, was die Rückerstattung angeht. Es ist aber so ein Kreislauf: Ich habe nichts hinterlegt mit Kreditkarte. Ich muss dann jedes Mal wieder meine Daten übermitteln und jedes Mal bei dieser Sicherheitsabfrage, von der du gesprochen hast, überlegen, was nochmal mein Passwort war. Am Ende finde ich diese Online-Bezahldienste, die ich eingerichtet habe, praktischer.

Lange: Ich sage nur Passwortmanager, Passwortmanager. Wir kommen immer auf ähnliche Themen zurück. Hast du den immer noch nicht eingerichtet?

Münz: Das ist gar nicht das Thema dieser Folge, Ute. Es geht hier um Online-Bezahlverfahren.

Lange: Manches ist aber verknüpft miteinander.

Münz: Ja sicher, alles ist mit allem verknüpft. Darüber reden wir vielleicht noch ein anderes Mal. Was ich eigentlich sagen wollte, ist: Ich bin mit meinen Online-Verfahren irgendwie halbwegs sicher vom Gefühl her. Von daher ist es so weit okay. Ich meine, wenn du Kreditkarten am häufigsten nutzen, hast du mit Verfahren wie Sofortüberweisung oder so eine Raten-Dienstleistung oder so bislang noch keine Erfahrung gesammelt?

Lange: Bisher nicht! Ich versuche, mich auf möglichst wenige Methoden zu konzentrieren. Das ist so ein bisschen mein persönlicher Lerneffekt, seit wir den Podcast machen. Ich habe das alles nochmal so ein bisschen in den Blick genommen. Ich finde das Motto „weniger ist mehr“ ganz gut, was meine Daten und Sicherheit anbelangt. Außerdem habe ich festgestellt, dass ich auch ein bisschen weniger impulsiv bin in meinen ganzen Online-Aktivitäten, vor allen Dingen auch beim Shoppen. Ich schlafe jetzt immer noch eine Nacht darüber, wenn irgendwie so ein tolles Angebot über den Bildschirm flitzt. Wenn es am nächsten Morgen immer noch so attraktiv ist und ich es unbedingt brauche oder haben möchte, dann kann ich mich ja dann noch entscheiden. Vielleicht bewahrt mich das auch ein bisschen vor Schaden. Denn wenn es zu günstig ist und zu gut, um wahr zu sein, dann ist es das ja vielleicht manchmal auch.

Münz: Ja, das stimmt. Das hast du vorhin auch schon gesagt. Das ist auch ein Punkt, den wir auch ich bei Fakeshops hatten. Sachen, die zu gut sind, um wahr zu sein, sind meist nicht wahr. Ich wollte noch das Thema Sofortüberweisung einbringen, die gibt es ja auch. Da bin ich aber auch tatsächlich zu faul. Früher, bevor es die IBAN-Umstellung gab, konnte ich meine Kontodaten auswendig. Da wäre es kein Problem gewesen. Die Zeiten sind vorbei, sodass ich bei Sofortüberweisung mittlerweile ein bisschen zu faul geworden bin. Ich bleibe

jetzt einfach bei dem Verfahren, was ich jetzt für mich etabliert hat, und wo ich am meisten Komfort sehe.

Lange: Ist dir denn schon mal etwas passiert? Also bis auf die Anspitzernummer, über die wir gesprochen haben! Da war es aber das Porto?

Münz: Genau, da war es das Porto. Nein, so richtig passiert ist mir nichts. Ich hatte mal einen Fall bei Kreditkarte und Rückerstattung. Da hatte ich auf dem Konto eine Abbuchung von, ich glaube, 800 Euro, die dann über meine Kreditkarte abgebucht worden waren von einem Online-Wettbüro oder so einem Online-Glücksspiel-Anbieter. Da habe ich aber auch nur zwei Telefonate mit meiner Bank gehabt und das Geld zurückbekommen. Das war ein gutes Gefühl. Das war das einzige Mal, wo ich so eine Bewegung hatte, wo ich dachte, dass da etwas schiefläuft. Gleichzeitig hatte ich aber auch das Glück, dass das Geld wieder zurückkommt. Von daher: Schwein gehabt! Was machst du, wenn du auf Nummer sicher gehen willst?

Lange: Ich kaufe häufiger auf Rechnung, habe ich im Überblick gesehen; vor allem dann, wenn ich die Shops noch nicht kenne und nicht so sicher sein kann, ob das alles klappt. Dann kann mir ja gar kein Schaden entstehen. Die Ware kommt und ich kann entscheiden, ob ich sie behalten möchte oder nicht. Wenn ja, dann bezahle ich in der angegebenen Frist! Das Dilemma bei dieser Methode ist, dass sie nicht so häufig angeboten wird wie andere Methoden. Aber hinsichtlich der Sicherheit habe ich da das allerbeste Gefühl, weil ich da ja praktisch auf dem Fahrersitz bin. Ich zahle nur dann, wenn es mir gefällt und wenn ich es tatsächlich behalten will. Das Einzige, was ich gegebenenfalls tun muss, ist nachzufragen, wo die Ware bleibt, wenn sie denn etwas länger dauert und ich sie tatsächlich noch haben möchte. Aber mein Geld ist eben nicht woanders, sondern es bleibt bei mir, bis ich entscheide, dass ich es woanders hinschicke. Von daher finde ich die Lösung ganz gut!

Münz: Es ist schade, dass die Methode nicht überall angeboten wird. Ich finde es natürlich auch super, wenn es so wäre. Dann würde ich es wahrscheinlich auch so machen.

Lange: Es ist nicht immer eine Option. Manchmal wird es eine Option, wenn du häufiger in einem Shop kaufst, wenn die dich auch schon kennen, wenn eine Art Beziehung hergestellt wurde zwischen Verkäufer und Käuferin oder umgekehrt. Dann kann man das nutzen. Ich finde das persönlich am allersichersten. Ich glaube, das BSI sieht das ähnlich, wenn ich die Unterlagen richtig gelesen habe, die auf der Webseite sind. Aber wir hatten ja gefragt! Ich würde jetzt gern zu den Rückmeldungen von unseren Hörern und Hörerinnen kommen. Es haben sich einige gemeldet, sowohl Sprachnachrichten aufgenommen als auch Geschichten geschrieben. Wir haben jetzt erst einmal Martha, die uns etwas erzählen möchte.

Martha: Hallo, ich bin Martha! Ich liebe Onlineshopping. Es ist so bequem. Aber letztens hatte ich wirklich Panik. Ich habe nämlich eine seltsame Abbuchung auf meinem Konto bemerkt für eine Bestellung in einem meiner Lieblings-Onlineshops, die ich so nie getätigt habe. Ich habe dann festgestellt, dass jemand wohl meinen Account gehackt und dann genutzt haben muss. Ich hatte bei diesem Onlineshop das Lastschriftverfahren als

Bezahlmethode hinterlegt. Ich konnte also die Abbuchung glücklicherweise rückgängig machen über meine Bank. Aber den Stress und diese Aufregung will ich nicht noch einmal erleben. Deswegen habe ich jetzt ein anderes Passwort für den Account. Das davor war, gelinde gesagt, echt schlecht! Ich verrate es jetzt hier nicht! Außerdem habe ich es so eingerichtet, dass ich jetzt immer noch eine Nummer bekomme auf mein Handy, die ich dann auch noch angeben muss bei der Anmeldung. Was ich allen empfehlen kann: Checkt regelmäßig euer Konto!

Münz: Okay, Martha ist nicht nur etwas widerfahren, sondern sie hat hier auch noch eine Menge Tipps gegeben, wie ihr das nicht noch einmal passiert. Gerade Hinweise auf Passwörter sind ja so ein Ding, womit du mir immer wieder Salz in die Wunde streust. Das ist schon eine ganz gute Methode, um sicherzustellen, dass man nicht Betrügern auf den Leim geht. Das fand ich gut. Eine schöne Einsendung, vielen Dank! Wir haben noch den Hörer Patrick, der uns auch etwas gesendet hat. Wir hören kurz rein!

Patrick: Moin, hier ist Pratick! Mir ist tatsächlich erst kürzlich etwas passiert. Ich habe bei Amazon bestellt, habe dann auch per E-Mail meine Bestellbestätigung bekommen. Alles ganz normal! Dann habe ich bemerkt, dass in meinem Spam-Ordner eine weitere Amazon- oder angebliche Amazon-E-Mail war, die sich auf die Bestellung bezog, ohne den Artikel noch einmal konkret zu nennen. Da stand einfach nur, dass es Probleme bei Ihrer Bestellung gab. Und weil ich eben kurz vorher bestellt hatte, dachte ich: „Klar, das passt auf jeden Fall zusammen“. Deswegen habe ich auf diesen Link geklickt. Da stand nämlich, dass man quasi den Bestellprozess nochmal durchführen soll. Ich musste mich mit meinem Amazon-Login noch einmal verifizieren. Das heißt, ich habe die Daten angegeben. Im Nachhinein weiß ich natürlich, dass es ein großer Fehler war. Im ersten Moment habe ich aber nicht darüber nachgedacht. Auf der zweiten Seite sollte ich meine Kontodaten auch noch einmal verifizieren. Da habe ich dann ein mulmiges Gefühl bekommen und habe das Ganze gestoppt. Ich habe im nächsten Schritt sofort auch auf der echten Amazon-Seite meine Login-Daten geändert. Ich habe tatsächlich dann auch direkt in dem Zuge endlich die Zwei-Faktor-Authentifizierung aktiviert. Ich hatte mir das schon lange vorgenommen. Ich habe mich immer davor gedrückt, aber das war jetzt der Anlass dafür. Es ist zum Glück nichts passiert! Aber dadurch, dass ich eben kurz vorher diese Bestellung getätigt hatte, habe ich nicht darüber nachgedacht, dass diese E-Mail im Spam-Ordner tatsächlich auch Spam war. Das war auf jeden Fall ein Erlebnis! Das wollte ich gern mit euch teilen!

Münz: Ja, bei Patrick kommt weniger das Thema online bezahlen, sondern mehr das Thema Phishing auf. Das kommt in dieser Folge, aber auch in früheren Folgen, immer mal wieder vor. Ich ziehe daraus die Lehre, dass man bei solchen E-Mails wirklich immer gucken muss, ob sie authentisch sind. Bei Patrick gab es diesen zeitlichen Zusammenhang, weswegen er dachte, dass es seine aktuelle Bestellung betreffen muss. Aber es schadet offensichtlich nicht, noch einmal genau hinzuschauen. Passt es wirklich? Ist das wirklich meine Bestellung? Ist es an mich gerichtet? Auch das ist wieder so ein Thema neben den Passwörtern: Nicht auf jeden Link klicken, den man bekommt, und dann womöglich Daten preisgeben oder das Einfallstor sein für Software, die man dann auf dem Rechner eingespielt bekommt!

Lange: Das hatten wir schon einmal, als der Kollege Herr Dwucet aus dem BSI da war. Er hatte ja genau so eine Situation mit einer Paketsendung. Was hatte er noch einmal gesagt? Wenn wir so in unseren Routinen sind und so „husch, husch“ machen oder „schnell, schnell“, dann kann das passieren. Lieber noch einmal durchatmen und die E-Mail wieder zu machen und vielleicht etwas später noch einmal angucken, wenn man etwas aufmerksamer ist! Sonst kannst du schnell mal auf so einen Link geklickt haben!

Münz: Das stimmt. Ich erinnere mich daran, dass er das erzählt hat. Ich glaube, es war die zweite Folge. Das ist schon ein bisschen her! Danke auch Patrick für die Einsendung! Die enthielt auch wichtige Aspekte, die wir an der Stelle auch noch einmal betonen wollten. Es war richtig viel Information dabei: unterschiedliche Systeme, Vor- und Nachteile, Hörer-Rückmeldungen. Ute, was nimmst du jetzt mit aus dieser Folge?

Lange: Ich versuche noch einmal zu rekapitulieren. Die Vorkasse scheint mir risikobehaftet. Das scheint auch eine Methode zu sein, die gerne genutzt wird, um einen übers Ohr zu hauen. Also vielleicht lieber nicht! Rechnung birgt die wenigsten Risiken. Lastschrift hatte Martha ja auch in ihrer Geschichte; dass sie das Geld problemlos wieder bekommen hat. Wir beide haben unterschiedliche Präferenzen. Das heißt, je nachdem, wie gut ich den Shop kenne oder mich vorher informiert habe, kann es die ja geben; oder wie bequem man ist. Du sagst ja, dass du eine lange IBAN nicht gerne eintragen magst. Deswegen kommt Sofortüberweisung für dich nicht infrage. Aber ich denke, je weniger Methoden man nutzt, desto besser – das ist bei mir ein bisschen hängengeblieben. Nicht nur, weil es mein eigenes Credo ist, sondern deswegen: Je besser ich die Methode kenne und desto vertrauter ich mit ihr bin oder desto mehr sie in meine persönlichen Abläufe passt, desto eher habe ich sie eingerichtet. Rechnung ist super sicher! Lastschrift ist sicher! Bei allen anderen Methoden immer gucken, ob der Shop vertrauenswürdig ist oder nicht. Es ist gut, Erfahrungen zu sammeln, bevor man sich zu eng an etwas bindet.

Münz: Mir fällt in dem Zusammenhang diese Videokampagne vom BSI ein, die es gerade gibt, wo Onlineshopping thematisieren. Es gibt einen Clip, bei dem ich mich ein bisschen ertappt fühlte. Das ist der Clip mit dem jungen Mann im Sneakerstore.

Lange: Zu gut, um wahr zu sein!

Münz: Wie er diese Sneaker streichelt! Ich hätte dann wahrscheinlich spätestens jetzt gedacht, dass das tatsächlich zu gut ist, um wahr zu sein. Aber ja, der fällt dann auf die Nase. Außerdem fand ich den Clip super witzig, in dem die Verkäuferin am Tresen den Kunden nach der PIN fragt…

Lange: Und dann plappern die alle ihre Nummern laut im Laden herum!

Münz: Genau! Das würdest du ja in echt nicht machen. Das ist dieser Grundsatz, nicht zu viele Daten anzugeben! So viele Daten wie nötig angeben! So wenig Daten wie möglich mit anderen teilen! Wenn einem etwas echt zu günstig vorkommt, dann auf jeden Fall eine Nacht darüber schlafen! Oder lieber noch einmal recherchieren, ob das sein kann. Alle Vor- und Nachteile von den Methoden, die wir genannt haben, hat das BSI auch auf seiner Seite

zusammengefasst. Da gibt es auch eine schöne grafische Umsetzung, wo alle Vor- und Nachteile dargestellt werden. Bleibt nur noch die Frage: Was mache ich denn, wenn das Kind in den Brunnen gefallen ist? Was mache ich, wenn mein Geld tatsächlich weg ist und ich merke „Mist, reingefallen!“?

Lange: Ja, das gibt es vom BSI eine SOS-Karte mit Tipps, wie man dann am besten vorgeht. Wenn zum Beispiel nach einer Bestellung keine Ware ankommt, du die aber schon bezahlt hast, erklärt die Karte, was du tun kannst. Welche Schritte sind möglich und ab welchem Punkt solltest du eine Strafanzeige stellen, damit der Betrug zur Anzeige kommt? Das ist auch wichtig, damit so ein Fakeshop vielleicht geschlossen wird oder sich vom Markt zieht, weil er aufgefallen ist. Was passiert in einem Fall wie von Martha, als jemand anderes mit ihrem Profil bestellt hat? Sie hatte einen Identitätsklau. Was kannst du dann machen? Was sind die Schritte? Es gibt auch Tipps zu Passwörtern. Die Karte sind zwei DIN-A4-Seiten, die man sich ausdrucken, aber auch online angucken kann; also wenn wirklich mal etwas schiefgeht. Aber wir hoffen ja, dass die vielen Tipps und Tricks, über die wir heute gesprochen haben, Menschen davor bewahren, hier betrogen zu werden.

Münz: Nicht nur das, was wir erzählt haben, sondern auch das, was unsere Hörerinnen und Hörer, also Martha und Patrick, erzählt haben! Da war das eine oder andere dabei, das jeder von uns berücksichtigen kann im digitalen Alltag. Dafür sind wir ja da!

Lange: Ja, und das gibt es auch alles noch einmal in den Shownotes!

Münz: Ja, genau! Damit sind wir fast am Ende dieser Folge angekommen, aber auch nur fast. Wir möchten nämlich gleich zwei Folgen ankündigen für die nächsten Wochen. Die eine kommt wie gewohnt in vier Wochen und dreht sich anlässlich der diesjährigen Gamescom um das Thema Gaming.

Lange: Ach, Überraschung!

Münz: Ja, ja! Wir sprechen mit jemandem darüber, was man an Sicherheitstipps in erster Linie bei Onlinespielen bedenken sollte. Denn ich weiß noch, als ich vom C64 gesessen habe, hab ich alleine davor gesessen. Mit anderen zu spielen, hieß, dass jemand neben mir saß. Mittlerweile habe ich den Faden schon verloren. Aber ich weiß, dass die Gamer miteinander vernetzt sind oder auch online Sachen kaufen müssen, um bestimmte Challenges in ihren Spielen zu bewerkstelligen. Wir wollen mal hören, was man alles bedenken muss, um sich abzusichern. Vielleicht ist das für den einen oder anderen, der uns zuhört und spielt, ganz interessant! Aber vielleicht ist es auch interessant für den einen oder anderen, dessen Nachwuchs spielt. Vielleicht wird sich gefragt, was das Kind eigentlich den ganzen Tag in seiner Bude macht, und ob es gut aufgehoben ist. Ich verspreche mir den einen oder anderen Hinweis, den wir in der nächsten Folge mitbekommen werden.

Lange: Ich freue mich auch schon darauf! Das ist eine ganz andere Welt! Das finde ich super!

Münz: Auf jeden Fall! Und dann haben wir noch eine Sonderfolge in Planung!

Lange: Ja! Wir wollen uns mit der Bundestagswahl beschäftigen und wie sicher diese ist bzw. was für deren Sicherheit getan wird. Es kommt ein Kollege des BSI zu uns bzw. wir verknüpfen uns wieder online, so wie wir es die letzten Monate gemacht haben. Wir wollen von ihm nicht nur hören, wie die Zählungen oder auch die Briefwahl abgesichert werden, sondern auch, was Empfehlungen für den Umgang mit Desinformationskampagnen sind. Das haben wir ja zuletzt auch bei den Wahlen in den USA und in Frankreich beobachtet. Das spielt eine große Rolle mittlerweile, wenn gewählt wird. Wir wollen auch hören, wie Kandidatinnen und Kandidaten, die sich zur Wahl stellen, unterstützt werden. Wie können die vor Angriffen gesichert werden? Ich verspreche mir sehr viele interessante Aspekte. Das BSI ist schon sehr lange mit anderen Behörden in der Vorbereitung und im Austausch, um diese Wahlen so sicher wie möglich zu machen, auch natürlich in unserem Interesse.

Münz: Das wird auf jeden Fall auch eine spannende Folge! Ich bin schon gespannt, was wir in dieser erfahren werden! Wir freuen uns, Sie wieder dabei zu haben. Bis dahin liken und folgen Sie bitte „Update verfügbar“ auf Ihrer Podcastplattform! So verpassen Sie keine der weiteren Folgen!

Lange: Wie immer gilt: Kontaktieren Sie uns gern über die BSI-Kanäle, über Facebook, Instagram, Twitter und YouTube. Es gibt die E-Mail-Adresse bsi@bis.bund.de. Wir freuen uns immer über Ihre Post! Bis wir uns bzw. Sie uns wieder hören, wünschen wir Ihnen alles Gute! Bleiben Sie gesund und hoffentlich unbeschädigt von weiteren Regenfällen oder Fluten! Wir freuen uns auf Sie! Bis dann! Tschüss!

Münz: 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