„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 12, 25.08.2021:
Level up! – Accountschutz für Gamer

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

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

Münz: Ich bin Michael Münz und wir melden uns auch diesen Monat wieder nicht aus dem Bundesamt für Sicherheit in der Informationstechnik, sondern aus dem Home-Office mit einer Folge zum Thema Gaming.

Lange: Bevor wir starten, möchten wir uns bedanken für das Feedback für die letzten beiden Folgen. Wir hatten das Thema online bezahlen – wie man das sicher macht – und das Thema Bundestagswahl. Gerade zum ersten Thema haben wir noch ein paar Tipps bekommen, die wir euch nicht vorenthalten wollen. Michael, magst du erzählen?

Münz: Ja, genau! Wir hatten noch eine Rückmeldung zum Thema giropay und paydirekt. Es hatte uns ein Hörer darauf aufmerksam gemacht, dass beim Thema Datensparsamkeit für ihn oder für sie – das können wir aus der Zulieferung nicht ganz genau erkennen – giropay/paydirekt die sicherste Bezahlmethode sei. Es kam noch ein zweiter Hinweis, den ich gut fand. Bei dem ging es um Kreditkartenbezahlung: Er oder sie nutzt eine Prepaid-Kreditkarte und verhindert so, dass größere Beträge abgebucht werden, ohne dass die Person, der Karteninhaber, das eigentlich möchte. Vielen Dank für die Zulieferungen! Die haben wir gern aufgenommen, um damit unsere Tipps aus der letzten Folge zu ergänzen.

Lange: Ja, und damit kommen wir zu unserem heutigen Thema. Wir haben wieder einen Gast dabei. Wir haben die Gamescom, die größte Online-Spielemesse der Welt. Die findet in diesem Jahr auch wieder digital statt. Das BSI hat da auch Aktivitäten und wir freuen uns, dass Florian Bierhoff dabei ist. Guten Morgen, Florian! Hallo, grüß dich!

Münz: Schön, dass du dabei bist. Wir freuen uns sehr und sind sehr gespannt auf deine Tipps und Hinweise zum Thema Gaming. Aber bevor wir in das Thema einsteigen, würden wir gern von dir hören: Was machst du im BSI? Wie bist du da hingekommen? Und was war so dein Werdegang?

Bierhoff: Ja, also ich bin 1982 geboren. Das ist zufällig das Jahr, in dem der Commodore 64 auf den Markt gekommen ist und die ersten Leute massenhaft mit Spielen in Kontakt gekommen sind.

Münz: Da gehörte ich auch zu.

Bierhoff: Ich habe mich tatsächlich nachher auch für den C64 interessiert, als ich dann ein bisschen älter war. Ich war mein ganzes Leben lang schon sehr technikinteressiert und auch Computerspiele und Konsolenspiele haben mich immer begeistert und begleitet. Ich habe dann dem folgend 2003 angefangen Angewandte Informatik an der Fachhochschule zu studieren und bin nach meinem ersten Studium direkt zum BSI gewechselt. Ich habe da zunächst in einem Referat für hoheitliche Dokumente gearbeitet. Ich habe mich da mit dem elektronischen Personalausweis und dem elektronischen Reisepass beschäftigt. Ich habe mich dann aber im BSI weiterentwickelt und bin jetzt im Referat DI 22. Das ist das Referat für Cyber-Sicherheit im Smarthome und Smart Cities. Zum Thema Smarthome zählen wir auch das Thema Spielekonsolen, weil die meisten Spielekonsolen online angebunden sind. Sie sind damit irgendwie auch in die Smarthomes integriert. Und weil ich privat an dem Thema auch interessiert bin, habe ich das dann so ein bisschen auch in meinem Beruf integrieren können.

Lange: Wie viele Kollegen und Kolleginnen hast du denn, die sich mit dem Thema beschäftigen?

Bierhoff: Wir sind im Referat insgesamt 10 Leute aktuell. Mit dem Thema Gaming beschäftigen tun sich drei in dem Referat. Aber wir haben natürlich im BSI noch mehr Leute, die an dem Thema dran sind.

Münz: Mit dem Thema Gaming beschäftigen, heißt: Ihr spielt den ganzen Tag und guckt nebenbei nach Sicherheitslücken?

Bierhoff: Nein, tatsächlich ist es eher so, dass wir – klar, haben wir natürlich auch ein Interesse und spielen selbst auch – verfolgen, was es für Angriffe gibt und ob irgendwelche Konten gehackt worden sind. Das ist für uns immer ganz interessant nachzuvollziehen: Was ist bei so einem Angriff passiert? Wie können wir Gamer und Bürger davor schützen, dass so etwas noch einmal passiert?

Münz: Gamer und Bürger, das ist tatsächlich eine große Schnittmenge, wie ich weiß. Über ein Drittel der Bevölkerung in Deutschland spielen in irgendeiner Form, das habe ich noch einmal rausgesucht. Was ich auch interessant fand ist, dass das Durchschnittsalter auf 37 Jahre gestiegen ist – in den vergangenen Jahren von 31 auf 37 Jahre. Das heißt, es spielen auch ganz viele Menschen meines Alters und noch darüber. Die Gamer im Alter von 60 bis 69 Jahren machen schon 10 Prozent der Spielenden aus. Wir sprechen tatsächlich gar nicht von irgendeiner kleinen, eingeschworenen Gemeinde, die sich die Nächte um die Ohren schlägt, sondern jeder von uns hat wahrscheinlich in irgendeiner Form schon einmal gespielt und ein Drittel tun es regelmäßig, auch auf ganz unterschiedlichen Geräten. Das heißt auch, es sind

nicht nur ganz viele Leute betroffen, wenn Sicherheitslücken auftreten, sondern jede dieser Personen kann ein potentielles Opfer sein für unterschiedliche Vorgehensweisen. Dazu kommen wir gleich noch einmal. Jede Person ist – das haben wir auch immer mal wieder festgestellt im Podcast – letztendlich auch ein Einfallstor, falls jemand kriminelle Machenschaften vorhat. Aber dazu kommen wir dann gleich im Einzelnen. Ich wollte es an der Stelle nur noch einmal einordnen.

Lange: Was mich interessiert oder vielleicht auch unsere Hörer und Hörerinnen: Florian, was fällt denn unter diesen großen Begriff Gaming? Welche Arten von Onlinespielen oder Tätigkeiten gibt es? Welche davon sind besonders im Blick eurer Arbeit?

Bierhoff: Wie Michael es schon ein wenig angedeutet hat: Das hat sich über die Jahre ein bisschen verändert. Mittlerweile ist es so, dass wir eine hohe Gaming-Durchdringung haben. Wir haben Gaming auf ganz vielen Devices: Wir haben Spielekonsolen, die viele Leute zuhause haben und die auch vielleicht als Medienspieler benutzen. Wir haben Mobiltelefone, Handys, auf denen Spiele laufen. Wir haben auch noch das klassische PC-Gaming, was früher hauptsächlich den Markt dominiert hat. Aber auch Smart-TVs kann man für kleine, meistens portierte Handyspiele nutzen. Das zeigt einfach, dass dieses Thema unheimlich relevant ist. Dadurch, dass so viele Leute Gaming und Spiele nutzen, steigt auch die Attraktivität für Angreifer. Ich habe dann meistens auch digitale Güter, die irgendwie damit vernetzt sind. Meine Accounts sind mittlerweile häufig richtig etwas wert, wenn ich mir mit In-Game-Bezahlvorgängen wichtige Items gekauft habe, die man vielleicht sogar auf einem Marktplatz oder so handeln kann. Das ist die eine Sache, dass digitale Güter einfach interessant sind für Angreifer. Darüber hinaus sind aber auch persönliche Daten extrem interessant für Angreifer, weil die weiterverkauft werden oder auch für weitere Angriffe genutzt werden können. Häufig ist es bei Hackern ein beliebtes Vorgehen, dass man sich von Ziel zu Ziel hangelt, um quasi möglichst viel zu kompromittieren, um möglichst viel mitzunehmen. Dementsprechend sind auch häufig die privaten Daten im Fokus. Das hat man auch vor zehn Jahren gesehen bei einem der bekanntesten Hacks, der in der Gamingszene überhaupt stattgefunden hat. Da wurde das Playstation Network ziemlich umfassend gehackt. Da sind tatsächlich insgesamt 77 Millionen Kundendatensätze in falsche Hände geraten. Da war wirklich alles bei. Ein paar Datenteile waren dabei verschlüsselt. Zum Beispiel Kreditkartendaten sind nicht direkt online gegangen. Aber trotzdem: Auch meine E-Mail-Adresse ist ein hohes Gut.

Münz: Wenn solche Hacks passieren und Daten veröffentlicht werden, was passiert dann mit denen? Es ist natürlich schlimm genug, dass meine persönlichen Daten dann irgendwo im Netz rumliegen. Aber was kann man dann damit machen? Was sind die üblichen Vorgehensweisen, wenn solche Daten erst einmal im Netz auftauchen?

Bierhoff: Meistens ist das so ein bisschen wie in der freien Wirtschaft. Da macht jeder das, was er am besten kann. Die Leute treffen sich auf dem freien Markt und so ist das im Prinzip bei diesen kriminellen Machenschaften auch. Es gibt Leute, die extrahieren gern Daten und beschaffen die, aber meistens machen die selbst gar nichts mit den Daten, außer dass sie die

weitergeben, zum Beispiel in Hackerforen zum Verkauf anbieten. Mittlerweile ist es auch eine relativ beliebte Masche, dass man erst einmal das Unternehmen selbst versucht zu erpressen mit dem Leak der Daten. So ist es zum Beispiel den Entwicklern von Cyberpunk ergangen. Das ist ein ganz aktueller Fall aus diesem Jahr.

Münz: Cyberpunk ist ein Spiel?

Bierhoff: Genau, Cyberpunk 2077 heißt das komplett. Das ist ein ziemlich populäres Spiel, bei dem der Quellcode von Hackern quasi geklaut wurde. Die haben dann erst einmal versucht, eine Erpressung durchzuführen.

Lange: Lass uns doch einmal gucken, was man dagegen machen kann. Michael hat ja schon gesagt, dass wir alle betroffen sein können in unterschiedlichen Aspekten. Wir können selbst das Datenrisiko sein, weil wir unsere Daten nicht absichern. Wir können aber auch Betroffene sein, wenn andere – entweder eine Firma oder andere Nutzer – das nicht tun. Du hast anfangs schon erwähnt, dass du selbst spielst. Lass uns doch mal anhand deiner Erfahrungen beim Spielen durchgehen, wie du dich absicherst. Ich meine, du arbeitest beim BSI: Deswegen gehe ich davon aus, dass du das vorbildlich machst und wir alle davon lernen können, wie wir es in Zukunft auch so machen können wie du. Du hast schon einmal gesagt, dass Accounts, die Konten und deren Sicherheit, ein ganz großes Thema sind. Erzähl doch mal, was du alles an Konten hast – nicht alle Daten und natürlich keine Passwörter! Aber welche Kategorien gibt es? Wie kann ich meine Sicherheit gewährleisten, wenn ich jetzt zum Beispiel anfangen sollte, online zu spielen? Ich tue das bisher selten, habe ich festgestellt, aber ich finde es total spannend, nachdem ich mich jetzt ein bisschen damit beschäftigt habe. Ich könnte dein Versuchskaninchen sein. Wie mache ich es jetzt richtig, wenn ich damit anfange?

Bierhoff: In Kategorien kann man das ziemlich gut einteilen. Ich habe im Wesentlichen drei Kategorien von Accounts, die ich selbst verwalten und sichern muss. Das eine sind Spiele-Verkaufsplattformen, auf denen ich einen Account habe. Mittlerweile werden über die Hälfte der Spiele rein digital verkauft. Das ist die erste Kategorie. Die zweite Kategorie sind Spiele-Plattformen, die direkt mit einem Spiel verbunden sind. Das sind dann meistens Onlinespiele, wo ich irgendwie einen Marktplatz habe oder wo ich Social-Funktionen habe. Das ist es bei mir meistens. Ich bin relativ aktiv in der Gaming-Community und habe teilweise auch Community-Management-Funktionen, die entsprechend geschützt werden müssen. Die dritte Kategorie, die bei mir noch ziemlich relevant ist, sind tatsächlich Messenger. Es ist so, dass zum Gaming meistens eigene Messenger-Plattformen genutzt werden, die einen sehr starken Fokus auf Anonymität legen, weil ich nur mit meinem Gamertag nach außen auftreten möchte. Dadurch, dass ich auch in den Communities aktiver war und auch weil ich Leitungsfunktionen hatte, war das für mich auch wichtig, um mit den Leuten in Kontakt zu sein. Bei Social Gaming ist das ein großer Aspekt. Das sind so die drei Kategorien: Spiele-Verkaufsplattform, Plattform für Spiele selbst und Messenger-Dienste.

Münz: Bei allen dreien gilt dann natürlich: sicheres Passwort benutzen und nie dasselbe. Und es gelten die Tipps, die wir hier auch immer wieder mal geben.

Bierhoff: Genau, ein sicheres Passwort ist ein ganz wichtiger Stichpunkt und vor allem unterschiedliche Passwörter. Das ist ganz wichtig. Weil ich habe es ja schon angesprochen: Dieses Durchhangeln durch Accounts ist irre beliebt bei den Hackern, weil es meistens auch funktioniert. Die Leute tendieren irgendwie dazu, ähnliche oder das gleiche Passwort zu nutzen. Das heißt, ich benutze am besten gute Passwörter und unterschiedliche Passwörter für jeden Dienst. Ute, du hast es gerade auch angesprochen: Zwei-Faktor-Authentisierung ist eigentlich das beste Mittel. Da habe ich echt eine gute Nachricht aus der Gaming-Welt. Da sind wirklich die meisten Plattformen vorbildlich. Ich bin ja selbst an dem Thema sehr interessiert und verfolge auch, wer als erstes Zwei-Faktor-Authentisierung einführt. Glücklicherweise waren das tatsächlich Gaming-Plattformen, die das wirklich in einem sehr großen Maße angeboten haben. Mittlerweile sind das wirklich alle Plattformen, die Zwei-Faktor-Authentisierung anbieten. Egal, ob das jetzt kleine Indie-Spiele-Verkaufsplattformen sind oder die großen Plattformen, alle setzen mittlerweile auf Zwei-Faktor-Authentisierung.

Lange: Dann muss man sie aber auch nutzen! Vielleicht für euch Hörer und Hörerinnen der Tipp: Wenn die Plattform sie anbietet, dann richtet sie ein. Es ist vielleicht einmal so ein kleines „Nerv, jetzt muss ich das auch noch machen“, aber für die Zukunft ist, glaube ich, viel Schaden von euch abgehalten, richtig?

Bierhoff: Genau, das ist ein super Stichpunkt! Einmal mache ich mir diese Mühe und richte das ein, aber ich kann damit viele, viele Probleme im Nachhinein quasi vermeiden. Ich selbst habe die Erfahrung gemacht in einer Community, die ich gemanagt habe: Die ist nicht direkt gehackt worden. Da hat tatsächlich jemand Rechte erlangt, dass er auch Mitgliederverwaltung machen konnte. Er hat dann bei Nacht – auch extra die Uhrzeit – gegen drei Uhr morgens – und wir haben hauptsächlich europäische Mitglieder – die komplette Community leergefegt. Alle anderen Administratoren guckten dann morgens in die Röhre, als sie das gesehen haben. Das war eine Community von ungefähr 2000 Leuten, die sich über einen langen Zeitraum kennengelernt haben und auch die Community geschätzt haben. Das war schon ein herber Schlag. So etwas kann man verhindern, wenn man entsprechend die Accounts und die damit verbundenen Berechtigungen schützt.

Münz: Bevor wir zum nächsten Thema kommen, was im Bereich Gaming auch eine große Rolle spielt, lassen wir Felix Rick vom Magazin Gameswelt zu Wort kommen. Felix moderiert für Gameswelt den Videochannel „Insert Coin“ und berichtet uns hier von einem seiner Arbeitskollegen, dessen Konto beim Spiel Grand Theft Auto gehackt wurde.

Rick: Hallo, mein Name ist Felix Rick von Gameswelt. Ein guter Kumpel von mir war lange bei GTA-Online aktiv, hatte über Jahre hinweg gespielt und seinen Charakter aufgebaut. Er hat da auch echt Geld reingesteckt, also für diverse Dinge online mit echtem Geld bezahlt. Und dann war‘s auf einmal so, dass er eine E-Mail von Rockstar bekommen hat, dem Entwickler des Spiels, die ihm sagten, dass sie sein Konto gesperrt haben. Also mit seiner Spielfigur hatte er dann keinen Zugriff mehr. Er hat es dann versucht, das zu überprüfen und hat festgestellt, dass der Name geändert wurde und diverse andere Daten und hat dann Kontakt mit dem Kundensupport von Rockstar aufgenommen. Er hat denen die Situation

erklärt, dass sein Konto eben gehackt wurde. Und die haben das dann auch gesehen. Ja, das hätte wohl jemand aus Russland gemacht. Die Konsequenz daraus war dann, dass diese Personen aus Russland all seine Sachen gestohlen, online mit dieser Figur Schabernack getrieben hat und dieses Konto gesperrt wurde. Und der ganze Fortschritt, den er sich über die Jahre erarbeitet und das Geld was er da reingesteckt hat, das war dann halt in dem Sinne einfach futsch. Und Rockstar hat es dann leider auch nicht mehr geschafft, dieses Konto, obwohl sie gesehen haben, dass es alles ja aus dem Ruder lief und nicht die richtige Person war, wieder so umzustellen, dass er seine Sachen zurückbekommen hat.

Münz: Vielen Dank für diesen Erfahrungsbericht, der auch zeigt, dass man selbst als Gaming-Experte Opfer werden kann von kriminellen Machenschaften oder Hackerangriffen oder so etwas. Damit solche Erfahrungen nicht zu schlimm werden, gehen wir zum nächsten Thema, was man berücksichtigen sollte, Ute!

Lange: Ganz vielen herzlichen Dank an Felix für diesen Bericht. Das zeigt uns, wie wichtig das ist, was wir ja gerade auch mit Florian besprochen haben, und worauf wir immer wieder hinweisen im Podcast: Datensparsamkeit und sorgfältig überlegen, mit wem man was teilt. Das nächste Thema ist eines, das wir schon einmal hatten. Aber dieses Mal geht es um Bezahlung beim Online-Gaming. Da gibt es auch eine ganze Menge zu berücksichtigen.

Bierhoff: Ja genau! Schon allein da fängt es an: Was kauft man? Weiß ich, was ich kaufe? Das ist eigentlich die viel größere Frage. Es gibt viele Spiele, bei denen das sehr gut geregelt ist. Meistens ist es so, dass ich zunächst mein richtiges Geld wechseln muss in eine Online-Währung. Das ist quasi der erste Schritt. Dann kann ich mit dieser Online-Währung entweder direkt irgendwelche Güter kaufen, die ich auswählen kann. Außerdem gibt es noch das große Thema der sogenannten Lootboxen, wo ich quasi vorher nicht genau weiß, was ich kaufe und auch ein gewisses Risiko habe, wenn ich eine Lootboxen öffne.

Münz: Da wollte ich kurz einhaken, weil mir das schon drei Schritte zu weit ist an dieser Stelle. Ich wollte noch einmal zurück an den Anfang, nämlich an die Stelle, wo du sagtest: „Dann wechsele ich von der echten in eine digitale Währung und zwar sofort“. Für mich im Hinterkopf spielen sich ganz viele Einrichtungsfragen ab: Wie funktioniert das? Muss ich irgendwo meine Kreditkartendaten hinterlegen oder gibt es andere Bezahlmöglichkeiten? Wie sicher sind die? Wie viel Aufwand macht es am Anfang? Und wie kann ich mich absichern oder muss ich das gar nicht?

Bierhoff: Es gibt eine ziemlich große Bandbreite! Wenn man ganz sicher gehen möchte, dann kann man zum Beispiel mit Guthabenkarten arbeiten. Das ist insbesondere so für Mobile Gaming Shops ein probates Mittel. Da kann ich mir an der Kasse im Einzelhandel eine Guthabenkarte kaufen und die einlösen. Dann haben wir eben noch das Nutzer-Feedback von eurer letzten Podcastfolge gehabt: Das passt da auch sehr gut zu. Prepaid-Kreditkarten sind natürlich auch ein super Mittel. Wenn ich die Kreditkarte hinterlegt habe als Bezahlmethode, wenn ich mich dazu entscheide, dann ist trotzdem gedeckelt, dass nicht beliebig viel Geld abgehoben werden kann. Klar, ich habe auch dann ein gewisses Risiko, dass das Guthaben, was ich darauf geladen habe, futsch ist. Aber ich kann nicht irgendwie richtig

in finanzielle Schieflage dadurch geraten und mich mit höheren Rückforderungen vom Kreditkartenbetreiber konfrontiert sehen. Deswegen macht es einfach Sinn, Guthabenkarten und Prepaid-Kreditkarten zu nutzen!

Münz: Dann habe ich das einmal hinterlegt. Wenn ich in dem Spiel der Auffassung bin, ich brauche ein Haustier, ein Lichtschwert, ein Raumschiff, dann wird das mit der Währung in dem Spiel bezahlt, mit dem, was ich vorher an Geld oder Währung angesammelt habe. Gleichzeitig läuft aber im Hintergrund eine Abrechnung oder eine Umrechnung ab, dass mir das Geld dann in echt abgebucht wird.

Bierhoff: Ja genau, da gibt es verschiedene Modelle. Gerade beim Mobile Gaming ist diese Anbindung häufig ziemlich direkt. Das kann ich auch über die Mobilfunkrechnung abrechnen lassen. Bei vielen anderen Spielen ist es auch so, dass ich von dem Spiele-Anbieter selbst Guthabenkarten kaufen muss. Da habe ich noch einmal einen Zwischenschritt, dass ich nicht direkt auf echtes Geld zugreife. Wobei man natürlich ein bisschen aufpassen muss: Das hat natürlich den Vorteil, dass dieser Zugriff nicht passiert. Es hat aber auch für mich persönlich den Nachteil, dass mit jedem Schritt, der dazwischen ist, sich natürlich ein bisschen verwässert, wie viel Geld ich da gekauft habe. Wie viel Geld habe ich in das Spiel bisher investiert? Das ist auch ein bisschen Taktik, sage ich mal, dass man die wahren Kosten zumindest undurchsichtiger macht.

Lange: Und dann hast du ja diese Lootboxen erwähnt. Also für mich sind das so Wundertüten, wo ich gar nicht weiß, was darin ist. Aber sie werden wohl häufig angeboten. Was verbirgt sich dahinter für diejenigen, die jetzt vielleicht nicht so vertraut damit sind? Worauf gilt es da zu achten?

Bierhoff: Lootboxen, das ist tatsächlich ein Begriff, der rein aus der Gaming-Welt kommt! Looten ist einfach das Einsammeln von Gütern. Die Lootbox ist dann quasi das, wo die Güter hineingepackt werden. Das ist im Prinzip auch genau die Beschreibung des Problems. Die Güter sind erst einmal in der Box sind, die meistens nicht durchsichtig ist. Ich weiß vorher nicht, was ich am Ende herausbekomme. Manche Länder haben das tatsächlich schon als Glücksspiel eingestuft. Das muss dann entsprechend gekennzeichnet werden. Es müssen entsprechend Jugendliche davor geschützt werden, weil das natürlich auch einen sehr hohen Reiz hat, dass man es weiter probiert. Es ist so ähnlich wie beim Glücksspiel: Wenn ich zehn Lootboxen geöffnet habe und es war immer noch nicht das darin, was ich unbedingt haben will, dann ist natürlich der Anreiz hoch, dass es dann beim elften Mal klappen muss.

Münz: Ich versuche gerade zu verstehen, warum man etwas kauft, von dem man gar nicht weiß, was es ist. Das ist ein bisschen wie bei den Sammelheften, wo du einfach hoffst, noch den einen Stürmer mit dabei zu haben. Oder es ist wie beim Greifen in den Loseimer: die Hoffnung, den großen Teddybären, der schon seit Wochen an diesem LKW hängt und mich an der Kirmes lockt, zu gewinnen. Also so ähnlich ist es dann auch.

Bierhoff: Richtig! Im Endeffekt läuft das, glaube ich, auf Statussymbole hinaus, die sich in der Gaming-Welt irre gut abbilden lassen. Das hat sich einfach gezeigt. Auch die großen Online-

Brands machen ihre Umsätze nicht mehr durch den Verkauf des Spiels selbst. Das läuft mittlerweile alles über Bezahlkarten. Damit wird der Großteil der Umsätze generiert.

Münz: Das ist so ein bisschen wie früher bei den Lampen: Lampen verschenken und verkaufen.

Bierhoff: Ja, genau, oder wie bei Druckern!

Lange: Florian, gibt es denn irgendwelche Tipps, dass man nicht in Kostenfallen oder ähnliches tappt? Oder gilt da dasselbe wie beim generellen Bezahlen im Onlinespiel-Bereich?

Bierhoff: Im Prinzip gilt da das Generelle, das ich das entsprechend absichern muss und ich muss es im Auge behalten. Man muss gucken, was man wirklich braucht. Was ich noch als Tipp geben kann: Es gibt relativ viele Spiele, bei denen Lootboxen nicht nur mit Geld, sondern auch mit Spielepunkten geöffnet werden können. Da muss ich vielleicht gucken, dass ich eher den Fokus auf das Spielen als auf das Bezahlen lege, einfach um nicht in finanziellen Druck zu geraten.

Münz: Das heißt, eher den schwereren Weg gehen im Spiel, anstatt über einen Kauf zwei Level weiter zu springen und dann irgendetwas zu erreichen.

Lange: Privatsphäre ist ja auch in dem Bereich ein Thema. Du hast schon gesagt und erzählt, dass du in Communities tätig bist. Man hat so Gamertags, also praktisch Namen, die man sich gibt, wenn man in den Spielen unterwegs ist. Das heißt, ich weiß ja erst einmal gar nicht, mit wem ich da spiele und ob das jemand ist, der oder die in guter Absicht sich mit mir in Kontakt setzt. Wie kann ich mich und meine Daten oder meine Privatsphäre schützen, wenn ich in so einer Community bin? Was gibt es für Anregungen, die du hast, oder auch Erfahrungen, die du teilen kannst?

Bierhoff: Was ich auf jeden Fall sagen kann: Die meisten Communities haben ziemlich gute Privatsphäre-Einstellungen mittlerweile. Da muss ich echt sagen, dass es ähnlich ist wie bei der Zwei-Faktor-Authentisierung. Die Spielehersteller und die Spiele-Plattformbetreiber haben ziemlich früh erkannt, dass Privatsphäre ein sensibler Punkt. Da fängt es im Prinzip an, dass ich zum Beispiel einstelle, dass mich unbekannte Leute nicht anschreiben können. Das wäre so ein Tipp, den ich dir geben würde. Man kann das auch fein granular einstellen: Wenn ich zum Beispiel Mitglied einer bestimmten Community bin, können mich dann Leute aus dieser Community ansprechen. Dann habe ich wenigstens einen gewissen Filter, dass es eine Verbindung gibt zu den Leuten und mich da nicht völlig Fremde anschreiben können. Ich würde den Leuten raten, vorher genau zu gucken, wie meine Privatsphäre-Einstellungen sind und was ich von mir preisgeben möchte. Auch gibt es häufig mehrstufige Freigaben für den eigenen Account. Ich bin zum Beispiel für unbekannte Personen nur unter meinem Gamertag verfügbar. Aber für Leute, die mit mir befreundet sind, kann ich auch einen Klarnamen angeben. Damit wäre ich, ehrlich gesagt, auch ein bisschen vorsichtig, weil es ist schon so – das hab ich in den Communities wirklich viel mitbekommen, dass die Leute ziemlich kreativ sind und auch sehr viel Arbeit darein stecken, um anderen zu schaden, um

sich Vertrauen zu erschleichen. Da habe ich echt viel Sachen mitbekommen, wo wir dann auch Leute melden mussten bei den Plattformenbetreibern, weil irgendwie unangebrachte Bilder verschickt wurden und so. Da muss man wirklich ein bisschen aufpassen

Münz: Hilft das Bewusstsein, das man hat? Also dieses Thema Datensparsamkeit: sich immer bewusst zu sein, dass die Daten, die ich eingebe, irgendwann auch mal frei im Netz stehen können.

Bierhoff: Ja, auf jeden Fall. Das ist ein sehr guter Tipp. Das man einfach sagt: Poste quasi nur online, was du auch später über dich, wir haben früher gesagt, in der Bildzeitung lesen möchtest. Aber genau wie sagtest: Poste nur das, was man auch mal online von sich sehen möchte.

Münz: Es gibt auf der anderen Seite das Interesse der Betreiber, der Hersteller, möglichst viele Daten von mir als Kunden zu bekommen – angefangen von meiner E-Mail-Adresse bis Kreditkarteninformationen und so weiter und so fort. Aber da dann den Spagat herzustellen zwischen dem, was nötig ist, um das machen zu können, was ich gerne möchte, und dem, was eben nicht mehr nötig ist, um das Spiel spielen zu können.

Bierhoff: Aber da muss ich auch sagen, dass zumindest der Großteil der Gaming-Community wirklich super vorbildlich ist. Es ist absolut Gang und Gäbe, dass man sich nur mit seinem Gamertag unterhält, auch über wirklich interessante Themen, viele Diskussionen führt und unabhängig von Alter, Geschlecht, Sexualität und so. Man kann da wirklich auch Freundschaften finden. Deswegen, glaube ich, sollte man sich nicht verleiten lassen, weil man irgendwie mehr von sich preisgeben möchte, ein besonders umfangreiches Profil anzulegen. Ich würde da eher durch Inhalte überzeugen.

Lange: Ich habe jetzt eine Frage für die jüngere Zielgruppe. Wir haben ja gelernt – Michael hatte das ja anfangs schon gesagt, dass es die breite Bevölkerung ist, die sich online spielend trifft und austauscht. Aber es gibt ja eine Gruppe, die vielleicht noch ein bisschen mehr Schutz braucht: Jugendliche, Kinder. Was habt ihr für Tipps als BSI? Wenn ich jetzt Eltern bin oder meine Patentochter zum Beispiel spielt, sind die Eltern immer ein bisschen besorgt. Da konnte ich jetzt etwas beruhigend einwirken und sagen: „Guck mal, hier gibt es Informationen und die sind auch teilweise schon sehr fit“. Aber gibt es noch etwas Besonderes, was zu berücksichtigen ist bei denen, die noch nicht volljährig sind und vielleicht auch manche Sachen noch nicht so einschätzen können, was Datensicherheit angeht?

Bierhoff: Da kann man auf jeden Fall etwas machen. Was ich immer empfehlen würde: Wenn es die Möglichkeit gibt, einen Unter-Account oder einen Kinder-Account im Familien-Account anzulegen, sollte diese auf jeden Fall genutzt werden. Dann habe ich einfach als Elternteil zumindest einen Hebel, um zu gucken, welchen Gefahren ich meinem Kind aussetzen möchte. Das kann man nach und nach dann weiter öffnen, wenn das Kind älter wird und man merkt, dass das Kind reifer ist und auch selbst darüber entscheiden kann, ob es das Taschengeld zum Beispiel für einen In-Game-Kauf nutzt. Wenn man das merkt, kann man das freischalten. Das andere ganz Wichtige ist, mit den Kindern zu reden, den Kindern

auch zu erklären, was Online-Gaming ist, und was es bedeutet, wenn einen jemand anschreibt; zu erklären, dass man das auch einfach löschen oder blockieren und ignorieren können. Diese Taktik wird häufig gemacht. Kinder werden überrumpelt und die Kinder sind dann erst einmal noch unsicher. Vielleicht spielen sie auch, ohne dass die Eltern es wissen, und haben Angst, zu den Eltern zu gehen. Es ist wichtig, mit den Kindern zu reden und dafür zu sorgen, dass man da ein bisschen am Ball bleibt und die Kinder schützt.

Münz: Es gibt auch den umgekehrten Fall. Bei mir was es so, dass mir die Kinder erklärt haben, wie bestimmte Spiele funktionieren. Bei mir sind die Nächte, wo ich am C64 Elite gespielt habe, schon längst vorbei und ich spiele, wenn Spiele, auf Mobiltelefonen: in der Supermarktschlange stehen, im Zug irgendwie Zeit verbringen, schnell mal das Telefon herausholen. Ich finde „Stadt, Land, Fluss“ zum Beispiel einen super Zeitvertreib, um einfach mal zu gucken, wie es funktioniert und wie schnell ich noch gedanklich bin. Aber ich frage mich, ob beim Thema mobiles Gaming auf dem Telefon noch weitere, bestimmte Punkte zu beachten sind. Gibt es noch zwei, drei Punkte in deiner Tipps-Lootbox, die du uns mitgebracht hast?

Bierhoff: Im Prinzip gilt das gleiche wie bei den klassischen Gaming-Plattformen. Das ist schon so. Ich kann dennoch achten, dass ich zum Beispiel beim Bezahlen dieses Abrechnen über den Mobilfunkanbieter einschränke. Da ist schon viel gewonnen, weil das viele per Default aktiviert haben – aus Bequemlichkeit meistens. Das ist aber etwas, was eigentlich selten wirklich legitim benutzt wird. Das ist eher etwas, was im Hintergrund läuft. Klar, es gibt es natürlich auch, dass das legitim benutzt wird. Ich möchte nicht, dass das ins falsche Ohr kommt. Aber häufig wird es auch missbraucht. Bei den Apps sollte ich darauf achten, welche Berechtigungen die wollen. Wieso braucht zum Beispiel eine Quiz-App den Zugriff auf mein Kontaktbuch? Darauf sollte ich ein Auge haben.

Münz: Was ist mit Schadsoftware? Kann ich mir die über so ein Spiel einfangen?

Bierhoff: Die offiziellen App-Store, muss man sagen, filtern da ziemlich gut. Die haben zumindest schon einen Basisschutz. Es ist eher selten, dass wirklich mit Schadsoftware belastete Spiele da durchkommen. Wenn ich mir aus irgendwelchen unbekannten Quellen die Spiele hole, dann habe ich da ein deutlich größeres Risiko. Werbesoftware-Bestandteile, die dann da integriert sind, sind eher ein Punkt; weil sich diese Free-to-Play-Spiele meistens auch finanzieren müssen.

Lange: Was kostenlos ist, kann mich hinterher viel kosten. Den Tipp hatten wir an anderer Stelle auch schon öfter. Mir rauschte gerade ein bisschen der Kopf, weil du so viele praktische und hilfreiche Tipps gegeben hast. Vielleicht versuchen wir das, Michael, zum Abschluss zusammenzufassen. Gerade aus deiner letzten Beschreibung oder Erklärung, Florian, nehme ich mit: Es ist wichtig, sich zu versichern, dass der Anbieter, bei dem ich mir etwas herunterlade oder kaufe, seriös ist, und dass ich den auch überprüft habe. Wir hatten auch schon eine Folge über Fakeshops. Die scheint es auch bei Onlinespielen zu geben, dass das vielleicht gefälschte Spiele sind, und dass ich mir da andere Sachen einhandele als das, was ich eigentlich damit machen möchte. Das ist ein Tipp. Meine Lieblings-Zwei-Faktor-

Authentisierung hast du schon mehrfach erwähnt. Das Thema Passwörter – sichere und vor allen Dingen unterschiedliche – haben wir auch schon gehabt. Was hast du noch mitgenommen?

Münz: Ich habe vor allen Dingen mitgenommen, dass das Thema Gaming im Prinzip das zusammenführt, worüber wir in den vergangenen Folgen gesprochen haben. Es fing bei Account-Sicherheit an. Das fängt damit an, eine Spielekonsole, die im Netz ist, auch mitzudenken – Thema Smarthome, was Florian ganz am Anfang gesagt hat. Wir hatten das Thema bezahlen, was wir beim letzten Mal hatten. Da kommt echt ganz schön viel zusammen! Für mich ist das eine fortgeschrittene Stufe von Datensicherheit, die ich irgendwie mitbedenken muss. Da kommt echt richtig viel zusammen, auch wenn es nur so ein, ich sage jetzt mal, popeliges Spiel ist, was ich mal eben 30 Sekunden in einer Supermarktschlange spielen möchte. Da ist echt viel zu bedenken. Aber ich glaube, wir haben auch viele Tipps dabei gehabt heute von Florian, sodass man ein gutes Gefühl hat, wenn man spielt und weiß, wo man sicher sein kann. Ein Thema, was wir auch hatten und was ich nur ganz kurz ansprechen möchte, ist Updates. Ich vermute: Wenn ich ein Spiel habe, gibt es wahrscheinlich auch Spiele-Updates. Wenn ein Update verfügbar ist, sollte ich das gefälligst dann auch installieren.

Bierhoff: Ja, das bietet sich auf jeden Fall an. Das soll ich man machen. Bei Spielen haben Updates auch viel Sicherheitsrelevanz. Das muss man auch sagen. Häufig werden da Lücken gepatcht. Noch viel wichtiger ist es aber auch bei den Plattformen, auf denen ich spiele, dass ich meinen PC, den ich zuhause stehen habe, regelmäßig update, damit einfach die Betriebsumgebung des Spiels sicher ist und ich nicht aus dem Spiel heraus irgendwelchen Unfug treiben kann.

Lange: Du hast ja gesagt, dass ihr euch im BSI in deinem Referat damit beschäftigt und ich habe gesehen, dass es auf der Webseite ganz viele Tipps gibt, wo ihr, liebe Hörer und Hörerinnen, noch einmal alles nachlesen und auch immer wieder darauf zurückgreifen könnt, wenn ihr euch jetzt nicht alles im ersten Durchlauf gemerkt habt. Ihr könnt die Folge natürlich auch gern öfter hören, wenn ihr möchtet. Ich habe noch eine Frage für dich, Florian. Du bist ja nicht nur beruflich mit Gaming beschäftigt, sondern auch privat ein großer Fan und sehr aktiv. Jetzt steht aktuell die Gamescom an. Auf was freust du dich am meisten?

Bierhoff: Ich bin einfach gespannt auf neue Spiele. Ich habe im Moment tatsächlich keinen großen Brenner, auf den ich mich besonders freue. Letztes Jahr war es Cyberpunk. Tatsächlich haben wir heute auch darüber gesprochen. Dieses Jahr bin ich einfach offen und freue mich auf die vielen neuen Sachen, die es sicherlich geben wird.

Münz: Fehlt einem bei der digitalen Gamescom nicht das stundenlange Schlange stehen?

Bierhoff: Ja, schon so ein bisschen. Also, ich muss sagen, ich bin jetzt kein Fan von Schlangestehen an sich. Aber ich habe in den Schlangen extrem viele nette Leute kennengelernt. Das, finde ich, ist auch so ein Qualitätsmerkmal. Vielleicht übertrieben, aber das ist so eine Eigenschaft von Gamern, die ich kennen und schätzen gelernt habe, dass man

sehr offen ist und schnell ins Gespräch kommt. Ich meine, man kann natürlich auch ein gemeinsames Thema sehr schnell finden, wenn man gerade für seinen Stil einsteht.

Lange: Ja, wir haben auch sehr angeregt gesprochen. Ich glaube, wir könnten auch noch weitersprechen. Aber ich denke, wir kommen zum Abschluss und freuen uns, dass du da warst. Florian, ganz herzlichen Dank! Es hat sehr viel Spaß gemacht!

Münz: Ja, war super! Vielen Dank!

Bierhoff: Ja, vielen Dank! Danke für die Einladung!

Lange: Wir freuen uns, wenn ihr auch beim nächsten Mal wieder dabei seid. Wenn es heißt: Update verfügbar. Bis dahin könnt ihr uns abonnieren auf euren Podcast-Plattformen. So verpasst ihr keine Folge. Und weil wir noch nach Anregungen für weitere Folgen suchen. Wir haben zwar ein paar Ideen zu Themen, mit denen wir uns beschäftigen möchten. Hier noch einmal die Einladung: Schickt uns doch gerne Anregungen, Ideen, Fragen, die euch schon immer beschäftigt haben, wenn es um Datensicherheit geht. Wie ihr uns erreicht, Michael, das weißt du genau.

Münz: Über die Kanäle Facebook, Instagram, Twitter oder auch YouTube! Da ist das BSI vertreten. Es gibt auch eine E-Mail-Adresse, die auch bei uns landet, wenn es um Themen, Anregungen geht. Die lautet bsi@bsi.bund.de. Wir freuen uns auf Post für Themenvorschläge für die nächsten Folgen! Wir sind sehr gespannt und nehmen die Anregungen, die dann auf den Wegen kommen, gern in den neuen Folgen auf!

Lange: Ja, bis zum Wiederhören alles Gute und Tschüss!

Bierhoff: 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