„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 05, 26.02.2021: Homeschooling – Tipps für Eltern

Moderation: Karin Wilhelm, Maximilian Berndt, BSI
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wilhelm: Hörst du mich?

Berndt: Ja, und du mich?

Wilhelm: Ja, prima Ton. Wir haben es geschafft!

Berndt: Endlich!

Wilhelm: Alle Kabel endlich eingesteckt. Man, das war wieder anstrengend!

Berndt: Das Tablet ist aufgebaut, wir sehen uns! Alles läuft!

Wilhelm: Diese Home-Office-Folgen von „Update verfügbar“! Das sind ganz neue Herausforderungen!

Berndt: Damit hatten wir nicht gerechnet.

Wilhelm: Es ist irgendwie so, dass das ganze Leben jetzt virtuell stattfindet. Das ist gar nicht immer so einfach. Allerdings ist es manchmal auch schön. Es war ja zuletzt Karneval hier bei uns im Rheinland. Da war ich in einem Jeck-Stream. Da gab es Karneval online zu erleben. Das fand ich ziemlich geil!

Berndt: Klingt witzig! Ich habe vor Kurzem mal an einem Escape Room teilgenommen. Die kennt man als Räume, in die man eigentlich physisch reingeht, oder eben auch als Brettspiel mittlerweile. Das war jetzt in dem Fall nicht ganz dasselbe, aber das lief eigentlich ziemlich gut. Man bekam vom Veranstalter PDF-Dateien zugeschickt, man bekam Fotos, man erhielt eine Webseite und musste sich dann irgendwie die Hinweise zusammensuchen und einen Mord aufklären. Ganz cool war dann zum Beispiel, dass man eine Mailbox anrufen musste, auf der eine Nachricht hinterlegt war, oder extra dafür erstellte Instagram Profile durchsuchen musste. Das war eine gute Alternative.

Wilhelm: Das klingt spannend. Aber die wichtigste Frage ist ja: Habt ihr den Mord aufgeklärt?

Berndt: Na klar!

Wilhelm: Gut, da wird nur mit Profis gearbeitet. Aber die Möglichkeit, seine Freizeit zu gestalten, auch virtuell, das ist wirklich der Wahnsinn. Was es da alles gibt! Sportkurse kannst du jetzt online machen, du kannst Tastings – Bier-Tasting, Wein-Tasting, Käse-Tasting – machen. Da kriegst du das zugeschickt. Dann kann man das Zuhause alles mal genießen. Oder Museumsbesuche virtueller Art! Zuhause-Festivals! Also, die Palette ist echt riesig!

Berndt: Zuhause-Festival heißt dann: Man feiert ein bisschen, dass man noch zuhause bleiben darf?!

Wilhelm: Nein, natürlich nicht! Du siehst da ganz tolle Künstler auf deinem Digitalgerät. Nur um das Kaltgetränk musst du dich dann natürlich selbst kümmern. Aber das sind auch ganz tolle Eindrücke, die man da gewinnen kann.

Berndt: Ja, da bieten sich gerade ganz neue Möglichkeiten für die Freizeitgestaltung. Aber es gibt ja auch Bereiche, in denen wir mit der Digitalisierung einfach irgendwie klarkommen müssen, ob wir wollen oder nicht. Ein Beispiel dafür ist neben dem Home-Office auch die Schule für Zuhause, also das digitale Lernen.

Wilhelm: Riesenthema, das du da ansprichst! Was im letzten Jahr da passiert war, war echt krasse Pionierarbeit, weil die Lehrer oder auch die Schulen hatten sich schon in unterschiedlicher Form mit Medienkompetenzen und Medienkonzepten auseinandergesetzt. Aber von heute auf morgen den Unterricht komplett virtuell stattfinden zu lassen, das war noch einmal eine ganz andere Hausnummer. Ich glaube, dass das ganz schön viele auch vor Herausforderungen gestellt hat, die bis heute noch andauern.

Berndt: Das hat bei Lehrerinnen und Lehrern viele Fragen aufgeworfen, aber natürlich auch bei Eltern. Der Erfahrungsschatz zuvor mit dem digitalen Lernen war dann doch sehr begrenzt. Insbesondere was die Sicherheit des Lernens online betrifft, wollen wir gerne mit unseren Zuhörerinnen und Zuhörern heute besprechen. Deshalb haben wir vor der Aufzeichnung schon Fragen eingesammelt und den wollen wir uns jetzt während der Folge widmen.

Wilhelm: Genau, und ich bin auch schon ganz gespannt auf die erste Frage. Die kommt nämlich von Melanie aus Leipzig. Ich schlage vor: Wir hören einfach mal rein!

Berndt: Ja, gern.

Elternteil Melanie: Hallo, hier ist Melanie aus Leipzig. Ich melde mich heute bei euch, weil ich tatsächlich auch eine Frage zum Thema digitaler Unterricht habe. Das ist bei uns zuhause ein relativ aktuelles Thema. Ich habe hier zwei Kinder sitzen, die sind zehn und zwölf, und die sind jetzt schon länger im digitalen Unterricht. Ich habe mich gefragt, was eigentlich mit den ganzen Informationen passiert, die sie hier jetzt online mit ihren Lehrern teilen. Werden diese Daten auf dem Schulserver gespeichert oder sind die in einem Cloud-Dienst gesammelt? Wer genau hat überhaupt Zugriff? Wie steht es da um das Thema Sicherheit? Wer darf darauf zugreifen? Was passiert mit diesen Daten? Das würde mich einfach

interessieren und würde mich freuen, falls ihr da eine Antwort für mich und natürlich auch für andere Eltern hättet. Danke euch!

Berndt: Das geht ja direkt mit einer spannenden Frage los. Schauen wir uns aber erst einmal an, was das überhaupt für Daten sind. Stellen wir uns vor: Melanies Kinder schicken ihren Lehrerinnen und Lehrern Aufsätze oder ausgefüllte Arbeitspapiere per E-Mail. Dann würden die Dokumente entweder über eine private E-Mail-Adresse versendet werden – das ist unwahrscheinlich, da die Kinder erst 10 und 12 sind – oder über eine E-Mail-Adresse, die die Schule für die Kinder bereitstellt.

Wilhelm: Manchmal gibt es auch eine andere Möglichkeit, und zwar Lernplattformen. Über viele Lernplattformen kann man auch Arbeitspapiere, Arbeitsblätter, Aufsätze verschicken. Es gibt da einige Plattformen, die bestimmt vielen unserer Zuhörerinnen und Zuhörern auch bekannt sind: Moodle, Logineo, Ilias oder IServ. Es ist nicht so, dass man sich das aussuchen kann. Das wird meistens von der Schule bzw. gar vom Land vorgegeben. Das ist auch nicht die einzige Möglichkeit. Man kann da nicht nur Nachrichten verschicken, sondern da gibt es noch mehr Funktionen: Kurse zur Auswahl anklicken, bei Umfragen mitmachen, Termine koordinieren, lernen oder Lehrmaterial abrufen. Jetzt hat Melanie aber gefragt, wo denn die Daten liegen. Wir haben jetzt zwei Fälle identifiziert: Entweder kann man das per E-Mail schicken oder per Lernplattform. Da kann man sagen, dass für beide gilt: Entweder liegen die Daten bei der Schule oder bei einem Dienstleister, in vielen Fällen auch bei beiden. Das eine ist der Schulserver. Das ist ein Rechner, der auf dem Schulgelände steht, wo ganz viel abgelegt wird. Das funktioniert auch bei den E-Mails so. Oder es gibt einen Dienstleister. Dann steht ein Rechner außerhalb der Schule in irgendeinem Datenzentrum. Das wäre dann für bestimmte Cloud-Dienste der Fall.

Berndt: Das heißt, die E-Mails liegen bei privaten E-Mail-Anbietern, weil man da zuvor schon eine E-Mail-Adresse hat und die Schule keine E-Mail-Adressen bereitstellt, oder die Schule liefert die E-Mail-Adressen zu. Dann liegen die E-Mails dort auf den Servern ab. Unabhängig davon, was Lehrer und Schüler miteinander austauschen, gibt es Informationen – Noten, Geburtsdatum, Adressen, aber auch Telefonnummern von Eltern oder Großeltern, Infos über Allergien der Kinder, über chronische Krankheiten, über die die Schule einfach Bescheid wissen muss. Das kann auch auf diesen Servern zu finden sein. Das sind Informationen, die hatte man früher einfach im klassischen Klassenbuch, und die waren da jederzeit für die Lehrerinnen und Lehrer verfügbar. Heute läuft es aber häufig digital und dann sind die Infos auf Schulservern hinterlegt. Das kann auch bei Dienstleistern liegen und muss nicht lokal auf dem Schulgelände auf irgendeinem Rechner gespeichert sein.

Wilhelm: Spätestens jetzt wird klar: Wir haben ganz, ganz viele Möglichkeiten und die kannst du auch noch miteinander kombinieren. Das scheint ein bisschen so, als würde es hier unübersichtlich werden. Nicht zuletzt, wenn sich Eltern mal austauschen mit Eltern aus anderen Bundesländern: Da ist es nochmal anders. Jede Schule trifft Entscheidungen. Wie verlieren wir denn da nicht den Überblick?

Berndt: Ja, das ist sehr schwierig im Moment. Es stimmt, die Lage ist unübersichtlich und deutschlandweit gibt es verschiedenste Systeme. Wie du schon gesagt hast: Die Länder machen ihr eigenes Ding und teilweise gibt es auch noch Schulen, die ihr eigenes Ding machen. Aus dem Grund können wir keine pauschale Empfehlung geben. Alle Tools, die von den Schulen und Ländern genutzt werden, haben ihre Vor- und ihre Nachteile. Da ist keines besonders schlecht und keines herausragend gut. Es kommt noch hinzu, dass die Tools teilweise untereinander kombiniert werden. Die sind häufig modular aufgebaut. Man nimmt beispielsweise nur den E-Mail-Versand oder die Organisations-Tools, die der Dienstleister bereitstellt, und macht die Videokonferenzen wieder über ein anderes Programm.

Wilhelm: Ja, aber was die meisten Eltern jetzt interessiert: Sind die Daten ihrer Kinder und vielleicht auch der Eltern bei den Schulen denn nun gut aufgehoben oder nicht?

Berndt: Da kann ich ein ganz klares „Jein“ beisteuern. Das können wir eben nicht mit einem „Ja“ beantworten, denn es ist eigentlich egal, ob die Schulen eigene Server betreiben, ob sie einen Dienstleister nutzen, ob sie eine der bekannten Lernplattformen nutzen. Es gibt am Ende ganz viele Faktoren, die bestimmen, ob die IT sicher betrieben ist. Manche dieser Faktoren liegen bei den Dienstleistern oder bei den Betreibern der Server, andere bei den Nutzern. Dazu gehört, dass individuelle Passwörter vergeben wurden, und dass die einzelnen Netzwerke, die entstehen können, voneinander getrennt und jeweils gesichert sind. Aber es kommt eben oft auch auf die IT-Kenntnisse der Lehrerinnen und Lehrer an und wie sie ihre Schüler darauf vorbereiten, mit der neuen Technik umzugehen. Da können Eltern leider oft recht wenig tun, außer kritisch bei der Schule nachzufragen und gegebenenfalls auf offensichtlich bestehende Mängel hinzuweisen.

Wilhelm: Wir wollen auch kein schlechtes Bild zeichnen. Viele Dinge, die du gerade jetzt genannt hast, sind den Schulen, den Verantwortlichen sehr wohl bekannt. Es ist aber wichtig, das im Blick zu behalten. Dazu passt auch ein bisschen die nächste Frage eines Vaters aus Berlin, der sich fragt, was denn überhaupt passieren kann. Ich glaube, da sollten wir auch mal reinhören.

Elternteil Christian: Hallo, ich bin Christian aus Berlin und ich habe eine Frage zu Videokonferenzen bzw. zu Videokonferenzsystemen. Ich habe eine schulpflichtige Tochter zuhause, die gerade über Videokonferenzsysteme Homeschooling macht. Ich wollte fragen: Welche Erfahrungen haben Schulen da gesammelt? Was kann ich tun oder was kann ich ihr zeigen, damit sie sicher von zuhause aus diese digitalen Tools nutzen kann? Vielen Dank!

Berndt: Erst einmal sind diese ganzen digitalen Tools und die Videokonferenzsysteme superpraktische Lösungen, um sich wenigstens hin und wieder zu sehen. Das kennen die meisten auch von ihrer Arbeit aus dem Home-Office. Wenn man sich vorstellt, wie das vor 20 Jahren ausgesehen hätte: Da wären wir wohl ziemlich aufgeschmissen gewesen. Das ist eben auch eine Möglichkeit für Lehrerinnen und Lehrer, mit ihren Schülern in Kontakt zu bleiben. Aber betrachten wir das mal durch unsere Sicherheitsbrille. Da gibt es eigentlich zwei größere Probleme, die hin und wieder auftreten. Das sind einmal die sogenannten

DDoS-Angriffe und zum anderen ist es die Störung des Unterrichts durch Leute, die im Unterricht nichts verloren haben.

Wilhelm: Ja, da fangen wir doch direkt mit den DDoS-Angriffen an. Vielleicht erklärst du uns erst einmal: Was ist das überhaupt genau?

Berndt: Ja, das ist nicht ganz selbsterklärend, da hast du Recht. Also, DDoS ist eine Abkürzung aus dem Englischen und heißt so viel wie „außer Betrieb setzen“. Das kann man sich so vorstellen, als würde man zum Beispiel zur Post gehen und der Frau hinter dem Schalter so viele Anfragen stellen, dass kein anderer Kunde mehr bedient werden kann. Bei DDoS-Attacken stellt man natürlich keine mündlichen Anfragen. Man ruft nirgendwo an oder steht an keinem Schalter. Stattdessen sind es Tausende oder gar Millionen von Rechnern, die Anfragen an einem Dienst stellen, indem sie zum Beispiel eine Webseite aufrufen bis es da zu einer Überlastung kommt. Dann kann der Dienst nicht mehr arbeiten oder steht nur noch sehr stark eingeschränkt zur Verfügung. Da fragt man sich natürlich: Warum machen das diese Millionen von Rechnern plötzlich? Die sind tatsächlich mit Schadsoftware infiziert. Das kann auch passieren, ohne dass die Besitzer das mitbekommen. Das muss auch gar nicht der eigene PC oder der eigene Laptop sein, sondern das sind häufig auch so kleine elektronische vernetzte Geräte, zum Beispiel im Smart-Home. Das kann der intelligente Fernseher sein, das kann die Rollladen-Steuerung sein. Das ist eigentlich relativ egal. Hauptsache, das Gerät hat in irgendeiner Weise eine Internet-Anbindung und ist aus Sicht der Hacker bestenfalls auch noch leicht zu übernehmen. Die Täter nutzen eine Schadsoftware, um die Geräte so zu übernehmen und dazu zu bringen, einen bestimmten Server anzuwählen. Sie bombardieren ihn also mit Anfragen und wenn der Angreifer es beispielsweise auf einen Schulserver abgesehen hat, der in der Regel nur wenige hundert Anfragen gleichzeitig bearbeiten muss und vielleicht maximal mit 10.000 Anfragen gleichzeitig klarkommt, und jetzt mit einer Million Anfragen bombardiert wird, dann schmiert er ab. Der ist dann außer Betrieb gesetzt.

Wilhelm: Das Faszinierende an dieser Angriffsart finde ich immer – stellen wir uns vor: Während wir beide jetzt hier diesen Podcast aufnehmen, könnten theoretisch unsere Geräte auch genauso so einen DDoS-Angriff starten. Gehen wir davon aus, dass wir nicht immer ordentlich Updates machen würden und nicht ganz einwandfreie Technik hier hätten. Aber das wäre möglich, wenn wir mit einem Schadprogramm infiziert werden, ohne dass wir eigentlich davon was mitkriegen würden, oder?

Berndt: Ja, genau. Das könnte parallel zu unserer Aufnahme gerade stattfinden und schlimmstenfalls würden wir es gar nicht merken.

Wilhelm: Darum ist es so sauwichtig, immer Updates zu machen – mindestens – und gute Antivirenprogramme zu haben, dass man so etwas auch finden kann. Solche DDoS-Angriffe sind tatsächlich gar nicht so eine Seltenheit. Das passiert immer wieder in ganz unterschiedlichen Bundesländern. Zuletzt war das in Thüringen passiert. Da war ein Lernportal für mehrere Stunden nicht mehr erreichbar. Was bedeutet das? Etwa 10.000 Schüler konnten einfach nicht mehr am Unterricht teilnehmen, was ja dann schon ganz

schön hart ist. Die hatten sowas wie Hitzefrei, nur die digitale Version davon. Was da besonders kurios ist, wenn man sich den Angriff genauer anschaut: Der kam wohl über einen Server aus Singapur. Das klingt jetzt erst einmal ganz schön seltsam. Das muss man aber einordnen. Denn wer sich genau dahinter verbirgt, das werden wir vielleicht nie erfahren. Cyberkriminelle haben es meistens ganz gut drauf, ihre Spuren zu verschleiern. Das heißt, es müssen nicht Menschen in Singapur gewesen sein. Das kann von überall auf der Welt stattgefunden haben.

Berndt: Ja, das ist in jedem Fall superärgerlich, wenn die ganze IT ausfällt. Aber das ist eben ein technisches Problem, das im Moment hin und wieder vorkommt. Es gibt aber auch Probleme, die während des Unterrichts auftreten. Ich habe eben schon von Störungen gesprochen, bei denen Externe, die nichts im Unterricht verloren haben, dazustoßen. So kommt es im Moment immer wieder zu Einzelfällen, in denen völlig Fremde oder vielleicht auch Freunde der Schüler einfach in den digitalen Unterricht platzen, und dann in ihren Augen lustige Dinge tun oder im schlimmsten Fall die Schüler sogar belästigen. Das kann sogar so weit gehen, dass die Eindringlinge die Lehrer herausschmeißen. Dann können sie ungestört mit den Kindern sprechen, ihnen unangemessene Inhalte zeigen und sie in schlimmen Fällen auch belästigen. Vor Kurzem gab es einen Fall, da fand es ein YouTuber wohl ziemlich witzig und hat auf diese Weise Unterrichtsstunden gestört, um im Nachgang seinen Gag medienwirksam zu veröffentlichen. Er ist an Schüler herangetreten und hat um die Zugangsdaten der Unterrichtsstunden gebeten. Die sind dann wohl irgendwann eingeknickt, haben ihm die Daten gegeben und er hat sich daraus einen Spaß gemacht, der jetzt aber wohl auch juristische Folgen haben könnte. Den Link zu diesem Vorfall findet ihr wie immer in den Shownotes.

Wilhelm: Das ist ja fast schon eine Horrorvorstellung, wenn man sich überlegt: Der physische Klassenraum war immer ein ganz gesicherter Raum, wo einfach nichts Fremdes reinkam. Im Virtuellen sieht es jetzt plötzlich ganz anders aus. Es gibt jedoch ein paar Tricks, die es den ganzen Witzbolden und lustigen Menschen und schlechten Menschen schwieriger machen, so eine Videokonferenz zu kapern. Zum Beispiel sollte man immer darauf achten, dass es einen individuellen Raumnamen gibt. Das kann man auch nachvollziehen: Zum Beispiel gibt es viele Raumnamen bei verschiedenen Anbietern, die „Test“ heißen. Wenn die nicht passwortgeschützt sind, dann ist es super einfach, dass da mal ein Fremder aus Versehen reinstolpert, der nur in einen anderen Testraum wollte. Übertragen wir das mal auf das Schulthema: So ein Raum kann ja auch „Klasse 3“ heißen – in ganz vielen Bundesländern, in ganz vielen Orten und Städten, weil es natürlich viele Klassen 3 gibt. Wenn das Passwort recht einfach erratbar ist – vielleicht „Hallo“ oder so, dann ist es natürlich sehr einfach, da reinzukommen.

Berndt: Genau, und da gibt es aber noch einen Tipp. Wenn die Software das zulässt, dann sollte man nämlich immer auch einen Warteraum einrichten. Warteraum bedeutet, dass die Administratoren, also die Lehrkräfte, im besten Fall in Ruhe prüfen können, wer sich gerade

in diesem Warteraum befindet, und dann jedem einzelnen Zutritt zum Unterricht gewähren können. So haben Externe gar nicht erst die Möglichkeit, in so einen Videochat einzudringen.

Wilhelm: Natürlich kann es da auch immer wieder sein, dass diese Witzbolde sich einen Namen geben, der vielleicht plausibel klingt. „Stefan Müller“ oder so, was einfach möglich sein kann. So könnte ja ein Schüler heißen. Dann ist es ganz wichtig, nachdem er den freigegeben hat, den auch wieder zu entfernen, als Lehrer. Vor allem ist es wichtig, dass nur die Moderatoren dieser Videokonferenz die Möglichkeit haben, andere zu entfernen. Dieses Recht sollte nicht jedem zustehen, denn sonst wird der Lehrer plötzlich herausgeschmissen.

Berndt: Außerdem schadet es auch nie, mit den eigenen Kindern einmal über dieses Thema zu sprechen und ihnen zu erklären, wofür so ein Passwort gut ist und was schlimmstenfalls alles passieren kann, wenn sie das Passwort einfach weitergeben.

Wilhelm: Es ist wahnsinnig wichtig, sich einmal mit seinem Kind auseinanderzusetzen, welche Bedeutung, welche Rolle so ein Passwort hat. Das wird im späteren Leben auch immer wieder ein Thema sein. Allerdings muss man dazusagen: Betrüger sind sehr trickreich. Gerade in sozialen Medien werden vereinzelte Schüler ein bisschen in die Mangel genommen. Da wird so Druck aufgebaut, bis dann der- oder diejenige das Kennwort vielleicht herausgibt, um einen schlechten Scherz zu starten. Da muss man mit seinem Kind am besten reden und sagen: „Hör mal, wenn dir irgendetwas komisch vorkommt, rede erst mit mir und gib keine Passwörter heraus“. Das sollte jedes Kind verstehen.

Berndt: Zusätzlich gibt es noch Tipps, die weniger auf die IT-Sicherheit oder die Sicherheit der Daten abzielen: Man sollte außerdem darauf achten, dass die Kinder vor einem neutralen Hintergrund sitzen. Bestenfalls sind sie entweder nicht in ihrem Kinderzimmer oder geben möglichst wenig über den Raum hinter sich preis. Das kann man im Moment häufig auch mit virtuellen Hintergründen einrichten. Das macht man, damit die Kinder keine Hinweise auf Passwörter geben, weil im Hintergrund das Poster der Lieblingsband hängt oder so etwas. Sie verraten eben nichts über ihre Lebensumstände und schützen ihre Privatsphäre. Deshalb möglichst wenig, zum Beispiel vom Kinderzimmer oder vom Büro der Eltern, zeigen!

Wilhelm: Absolut! Da ist also auch einiges möglich, was man selbst seinem Kind zeigen kann, worüber man mit seinem Kind reden kann. Wenngleich natürlich auch eine große Verantwortung bei den Lehrerinnen und Lehrern liegt. Ein Punkt, auf den wir auch noch zu sprechen kommen wollten: Womit gehen denn eigentlich die Schülerinnen und Schüler ins Netz? Also, mit welchen Geräten? Gerade im letzten Jahr hat man gemerkt, wie unterschiedlich das ist. Beispielsweise Familien mit sehr vielen Kindern haben einfach nicht die nötige Ausstattung, mussten vielleicht auch etwas Neues ankaufen. Man nutzt vielleicht einen PC gemeinsam. Da gibt es auch ein paar Tipps, auf die wir gleich eingehen wollen. Aber erst einmal hören wir uns an, welche Frage Marie aus Göttingen dazu hat.

Elternteil Marie: Hallo, hier ist Marie aus Göttingen. Ich habe eine zwölfjährige Tochter und meine Frage lautet: Welche Geräte sind sicher und worauf soll ich beim Kauf achten? Dankeschön, Tschüss!

Wilhelm: Die schlechte Nachricht! Das eine sichere Gerät gibt es leider nicht! Diesen Tipp würden wir supergern geben, aber dafür ist einfach zu viel in Bewegung in der Digitalisierung. Natürlich haben wir auch eine gute Nachricht dabei. Wir haben gleich ein paar Tipps, was zu einem guten Basisschutz gehört. Zum einen hat Marie gefragt, worauf sie beim Kauf achten soll. Da ist es zum Beispiel sehr wichtig, dass die Geräte, die man kauft, immer noch Updates zur Verfügung stellen. Jetzt denkt man vielleicht: „Updates werden doch sowieso immer mitgeliefert!“ Das stimmt nicht. Es wurden beispielsweise schon Smartphones verkauft, wo keine Updates mehr zur Verfügung standen oder nur noch binnen eines halben Jahres. Da muss man tatsächlich auf das Kleingedruckte achten! Das lohnt sich dann zum Beispiel!

Berndt: Wenn man ein neues Gerät kauft, einen Neukauf plant, dann ist es, glaube ich, eine ganz gute Idee, bei der Schule nachzuhaken, ob die bestimmte Anforderungen haben. Wenn alle Mitschüler ein bestimmtes Betriebssystem nutzen und das eigene Kind nutzt ein anderes, ist das nicht so hilfreich. Manchmal sind besondere Features nötig. Manchmal muss eine bestimmte Webcam verbaut sein. Da einfach mal nachhaken und die Schule fragen, was empfehlenswert ist! Wenn die Kinder mit dem eigenen Familienlaptop ans Werk gehen sollen, auf dem vielleicht auch noch Home-Office betrieben wird, dann ist es ganz klug, ein eigenes Benutzerkonto für das Kind zu errichten, in dem der Unterricht stattfindet. So verhindert man, dass das Kind aus Versehen die digitalen Kontoauszüge an die Schule schickt, oder dass Dateien heruntergeladen werden, die in irgendeiner Art und Weise schädlich sein können. Das passiert dann immer nur innerhalb des Benutzerkontos des Kindes. So sind Schulangelegenheiten von Arbeitsangelegenheiten oder privaten Dingen getrennt.

Wilhelm: Es gibt auch Schulen, die ihren Schülerinnen und Schülern zum Beispiel kleine Tablet-Computer zur Verfügung stellen. Da ist es als Elternteil sehr wichtig, dass man sich die Grundeinstellungen anschaut. Ein Punkt, den man auf jeden Fall beachten sollte, ist, ein sicheres WLAN einzurichten, denn meistens will man mit einem Tablet-Computer ja auch ins Internet, will vielleicht recherchieren oder Daten versenden.

Berndt: Genau! Bei den Einstellungen kommt es auch wieder darauf an, wie das jeweilige Land oder die jeweilige Schule damit umgeht, welche Plattform genutzt wird. Da können wir hier leider keine pauschalen Infos zu geben. Aber um auf Karins Hinweis mit dem sicheren WLAN zurückzukommen: Da sollte man erst einmal hingehen und sich den eigenen Router anschauen. Hat man ein möglichst langes und vor allem individuelles Passwort eingerichtet, um einerseits auf den Router zugreifen zu können? Aber auch ein möglichst langes und individuelles Passwort, damit die einzelnen Geräte, die man zuhause hat, sich sicher ins WLAN einwählen können? Braucht der Router vielleicht ein Update? Das kann man im Menü

des Routers erkennen. Da muss man mal in das Handbuch schauen, wie man sich am besten in dieses Menü einwählt. Das ist je nach Hersteller sehr unterschiedlich. Da wird einem dann angezeigt, ob der Router auf dem neuesten Stand ist. Welche Verschlüsselung hat das Gerät? Da hat sich vor Kurzem auch etwas geändert. Da ist man vom sogenannten WPA2-Standard auf den WPA3-Standard gewechselt. Vorausgesetzt natürlich, man hat ein relativ aktuelles Gerät. Da vielleicht einmal nachhaken! Sollte da noch WPA1 ausgewählt sein, empfiehlt es sich zu schauen, ob man per Update die neueren Varianten einstellen kann oder ob man vielleicht über die Neuanschaffung eines Geräts nachdenkt. Wenn man diese Hinweise beachtet, wird es für Außenstehende schon recht schwierig, ins heimische Netzwerk einzudringen und Daten abzufangen. Insgesamt gilt aber für alle Geräte, egal ob Tablet, Router oder Laptop, immer Software-Updates installieren, wenn sie bereitstehen. Dazu bestenfalls die automatischen Updates überall aktivieren! Dann ist es auch kein großes Ding im Alltag mehr und die Geräte erledigen das für einen. Dann lange und möglichst sichere Passwörter verwenden! Dazu haben wir auf unserer Webseite auch Tipps, wie man das bestenfalls einrichtet. Hinzu kommt noch: Wenn dann viele E-Mails verschickt werden, egal ob beruflich oder im Schul-Kontext, bitte nie auf Links klicken, in E-Mails, die man nicht erwartet hat.

Wilhelm: Das sind doch schon sehr gute Tipps für einen Basisschutz. Jetzt stellt sich das ein oder andere Elternteil vielleicht die Frage: „Ja, gut, was kann ich denn nun konkret tun?“ Bestimmte Sachen, wie bei der Videokonferenz den Raumnamen vergeben, sind ja nicht unbedingt die Aufgabe der Eltern. Es ist einfach wichtig, aufmerksam zu sein. Eltern sollten ihr Kind begleiten und zuhören: Wo gibt es Probleme? Auch aufmerksam sein, wenn einem vielleicht etwas „Spanisch“ vorkommt und dann auch mit dem Kind reden. Es geht auch darum, Themen anzusprechen, wie zum Beispiel Passwort. Wofür ist das gut? Wofür brauche ich das? Beides wird auch später im Leben noch sehr, sehr wichtig sein. Da eine Sensibilität herzustellen und zu sagen: „Ja, mein Kind hat schon verstanden, dass man ein Passwort nicht einem Fremden erzählt“. Das ist vielleicht auch so, wie ich nicht jedem Fremden meine Telefonnummer gebe. Und zuletzt: Wer ein ungutes Gefühl hat, der sollte auch Dinge ansprechen, und zwar nicht nur bei seinem Kind, sondern sich gern auch an die Lehrerinnen und Lehrer wenden, wenn vielleicht in der Schule etwas vorgefallen ist. Es wurde einfach eine App heruntergeladen auf einem Privatgerät. Da sollte man ruhig ansprechen, dass man das in puncto Sicherheit nicht sehr gut findet. Oder wenn man sich unsicher ist, wie man vielleicht ein Gerät von der Schule richtig einrichtet: Sprechen Sie die Lehrerinnen und Lehrer an. Die werden vielleicht sehr dankbar sein, weil wir momentan noch in einem Lernprozess sind. Da ist Feedback vielleicht genau das Richtige.

Berndt: Ich hoffe, wir konnten auf alle offenen Punkte und auf alle Fragen eingehen. Wir haben uns zumindest bemüht. Falls jetzt noch Fragen bestehen, sind wir bei Facebook, bei Twitter oder bei YouTube zu finden. Wie immer gilt: Wir freuen uns sehr über Vorschläge für nächste Episoden und ganz besonders natürlich auch über Feedback und über viele schöne Bewertungen.

Wilhelm: Genau! In den Shownotes werden wir noch ein paar Informationen, Empfehlungen, Tipps und Links zusammenstellen, damit jeder, der Interesse hat, sich noch ein bisschen weiter mit dem Thema befassen kann. Und jetzt kann man sagen: „Wir haben Glück gehabt, es hat sich kein YouTuber in unsere Konferenz gehackt“. Nun bleibt uns eigentlich nur noch, auf Wiedersehen zu sagen.

Berndt: Tschüss!

Wilhelm: Bis zum nächsten Mal!

Besuchen Sie uns auch auf:

https://www.bsi-fuer-buerger.de
https://www.facebook.com/bsi.fuer.buerger
https://twitter.com/BSI_Bund
https://www.instagram.com/bsi_bund/

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