APuZ

AUS POLITIK UND ZEITGESCHICHTE

Aus Politik und Zeitgeschichte – Der Podcast

Folge 22: Cybersicherheit | 31.10.2023

Holger Klein: Willkommen zu „Aus Politik und Zeitgeschichte“, einem Podcast der Bundeszentrale für politische Bildung. Ich bin Holger Klein, und wir sprechen heute über Cybersicherheit. Wenn Sie sich nach dem Hören tiefer mit dem Thema befassen wollen, finden Sie die Zeitschrift zum Thema auf bpb.de/apuz.

Musik

Wir haben wahrscheinlich alle schon mal so eine E-Mail bekommen, die „irgendwie komisch“ war. Und wir kennen Schlagzeilen wie diese:

O-Töne: Die Internetseiten mehrerer Sicherheitsbehörden, Ministerien und Politiker sind offenbar durch Hacker angegriffen worden. Ein IT-Dienstleister, der auch für zahlreiche gesetzliche Krankenkassen arbeitet, ist Opfer einer Cyberattacke geworden. Ein mutmaßlicher Hackerangriff auf ein Satellitennetzwerk, welches auch die Ukraine mit Internet versorgt.

Holger Klein: Die Spannweite von Cyberkriminalität ist groß: Das reicht von Computerviren über Phishing Mails bis hin zu Ransomware-Attacken und Wirtschaftsspionage. Solche Angriffe im Netz bedrohen weltweit Unternehmen, Behörden und ganze Infrastrukturen. Und sie spielen auch in politischen Konflikten eine Rolle. Wie ein Cyberangriff überhaupt funktioniert und wie wir uns dagegen besser schützen können, darum geht es in dieser Folge. Ich habe mit der Wissenschaftsjournalistin Eva Wolfangel darüber gesprochen, wie sich Cyberkriminalität entwickelt hat und wie wir uns an unseren Computern davor schützen können.

Eva Wolfangel: Die Schadsoftware wird immer besser, immer professioneller, immer schwerer zu entdecken. Also moderne Cyber-Kriminalität ist top organisiert.

Holger Klein: Und mit Sven Herpig, Experte für Cybersicherheitspolitik, habe ich darüber gesprochen, wie groß die Bedrohung durch Cyberangriffe in Deutschland ist:

Sven Herpig: Wir haben natürlich Cyber-Operationen gegen zum Beispiel den Bundestag gesehen, aber eben auch vor allem im Ausland Cyber-Operationen, die Wahlen beeinflussen wollen. Das ist natürlich ein sehr hohes politisches Risiko.

Musik

O-Töne: Das Justizdepartment hat vergangene Nacht ein internationales Ransomware-Netzwerk ausgehoben, das versucht hat, hunderte Millionen Dollar von Firmen in den USA und in der ganzen Welt zu erpressen. Es handelt sich um die Tätergruppe Hive.

Holger Klein: Das ist der US-amerikanische Justizminister Merrick Garland im Januar 2023. Der Erfolg gegen die Hackergruppe Hive ist der sogenannten Operation Dawnbreaker zu verdanken. Das ist ein internationales Ermittlerteam, das lange versucht hat, den Hackern auf die Spur zu kommen.

Das Hackernetzwerk Hive hat mit Ransomware gearbeitet: „Ransom“ ist das englische Wort für „Lösegeld“ – und genau darum geht es bei Ransomware-Angriffen: Unternehmen oder Privatpersonen werden quasi aus ihrem eigenen Computer ausgesperrt, bis sie ein Lösegeld bezahlen. Die Wissenschaftsjournalistin Eva Wolfangel hat in der APuZ über die Ermittlungen der Operation Dawnbreaker geschrieben, an denen auch eine deutsche Polizeieinheit beteiligt war. Sie hat mir das im Gespräch genauer erklärt:

Eva Wolfangel: Das war eine Gruppe, bei der unter anderem die Polizeidirektion Esslingen-Reutlingen beteiligt war, die eine große Ransomware-Gruppe, na ja, wie soll man sagen, platt gemacht haben oder überführt haben, allerdings nicht die Menschen, aber immerhin haben sie die Infrastruktur übernommen und da war eben das Spannende, nicht nur die Polizeidirektion Esslingen dabei, sondern eben auch die großen, US-Agenturen, das FBI und andere.

Holger Klein: Ransomware ist das, wo mein Computer auf einmal nicht mehr funktioniert und irgendjemand sagt, ja wenn du mir jetzt 100 Bitcoin überweist, dann schalte ich deinen Computer wieder frei?

Eva Wolfangel: Genau, im Prinzip so, genau.

Holger Klein: Wie haben die die ausgehoben?

Eva Wolfangel: Also die haben tatsächlich die Angreifer:innen zurückgehackt, sich in deren Server, deren Infrastruktur eingeschlichen und haben ein halbes Jahr lang alle Kommunikationen mitgelesen, genau gesehen, wer die aktuellen Opfer sind,

wen sie gerade planen, anzugreifen, konnten wohl teilweise auch Verschlüsselungs- oder Entschlüsselungsschlüssel abgreifen und eben jede Menge Informationen darüber, wie die arbeiten, wer welche Aufgabe hat und das konnte man wie so oft natürlich sehen, dass es ein perfekt organisiertes Unternehmen ist letztlich.

Holger Klein: Aber weg ist das Problem jetzt nicht, das machen jetzt halt nur andere?

Eva Wolfangel: Also genau, das Problem geht leider nicht weg, auch deswegen natürlich, weil viele Unternehmen das Lösegeld bezahlen. Leider immer noch. Und dadurch sind natürlich die Kriegskassen von solchen kriminellen Banden ganz gut gefüllt. Und das wird nicht weggehen. Die Personen selbst, das glaube ich auch, die da beteiligt waren, werden einen Stand haben, weil natürlich jetzt auch im Untergrund alle wissen, dass da die Polizei ein halbes Jahr mitgelesen hat. Von daher glaube ich, wird es für die persönlich schwierig, aber es gibt natürlich unendlich viele andere Kriminelle, die das gleiche Geschäftsmodell haben.

Holger Klein: Die Unternehmen zahlen das Lösegeld, sagen Sie, sollten die das nicht machen? Was haben die für eine Wahl?

Eva Wolfangel: Also das fragen sich Unternehmen natürlich oft, die dann vor der Entscheidung stehen. Also viele gehen tatsächlich einfach pleite, weil wenn mal alles verschlüsselt ist, kann man nicht weiterarbeiten und so ein Ausfall über mehrere Tage und Wochen hinweg, der ist natürlich extrem teuer. Und es gibt immer wieder Unternehmen, die wirklich vor der Entscheidung stehen: Ich gebe mein Unternehmen auf oder ich zahle das Lösegeld. Soweit sollte man es halt nicht kommen lassen. Weil erstens ist natürlich überhaupt nicht sicher, ob danach alles wieder wunderbar funktioniert. Und das andere ist natürlich, dass sich in Kriminellenkreisen auch rumspricht, dass diese Firma offenbar bereit ist zu zahlen und es gut sein kann, dass sie nochmal angegriffen werden oder dass die Kriminellen sagen, ah, wir haben eure Daten abgezogen, wir erpressen euch einfach nochmal, sobald ihr wieder auf den Beinen steht und veröffentlichen eure Daten, wenn ihr nicht noch mehr bezahlt. Also das ist durchaus eine heikle Sache, aber vor allem, das Hauptproblem ist natürlich, dass es das Geschäftsmodell stärkt und dass wer bezahlt, finanziert den Angriff auf das nächste Unternehmen.

Musik

Holger Klein: Eva Wolfangel beschreibt, dass Cyberkriminelle ein richtiges Geschäftsmodell aus diesen Angriffen entwickelt haben. Und das betrifft tatsächlich viele Unternehmen. Wie viele genau - das ist schwer zu sagen.

Sven Herpig: Also einen Überblick darüber hat keiner wirklich. Wir haben kein vernünftiges umfassendes Lagebild und keine Meldeverpflichtung für den Großteil der Unternehmen in Deutschland.

Holger Klein: Das sagt Sven Herpig. Er leitet den Bereich Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung.

Sven Herpig: Wenn man sich allerdings die Einzelnachrichten anguckt und welches Unternehmen gerade wieder betroffen ist, wer gerade wieder Millionen zahlt, um das IT-System in Ordnung zu bringen, glaube ich, kann man ganz gut zusammenpuzzeln, dass es die deutsche Wirtschaft viele, viele, viele Millionen im Jahr kostet.

Holger Klein: Es ist schwierig, den wirtschaftlichen Schaden durch Cyberangriffe genau zu bemessen, weil dafür zu wenig Daten von den Unternehmen selbst vorliegen. Der Branchenverband der deutschen Informations- und Telekommunikationsbranche, BITKOM, versucht seit 2015 trotzdem einen Überblick über die Situation zu bekommen. In einer jährlichen Studie untersucht BITKOM, welche Unternehmen von Cyber-Spionage, Sabotage und Datendiebstahl betroffen sind. In der aktuellen Studie von 2023 kommt BITKOM zu dem Ergebnis, dass der wirtschaftliche Schaden durch Cyberkriminalität bei über 200 Milliarden Euro liegt. Aber nicht nur der wirtschaftliche Schaden ist groß: Wenn Ransomware zum Beispiel die IT-Systeme von Krankenhäusern oder Stromerzeugern blockiert, können die Folgen noch weitreichender sein. Und Cyberkriminalität hat auch eine politische Dimension:

Sven Herpig: Wir haben natürlich in der Vergangenheit auch Cyber-Operationen gegen zum Beispiel den Bundestag gesehen, als eine Spionageoperation, aber eben auch vor allem im Ausland Cyber-Operationen, die die Wahl beeinflussen wollen oder die Wahlen beeinflussen wollen. Das ist natürlich ein sehr hohes politisches Risiko.

Holger Klein: Das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, schreibt in seinem Lagebericht 2022: Die Bedrohungslage in Deutschland sei "so hoch wie nie". Das BSI ist in Deutschland für Cybersicherheit zuständig. Aber es ist nicht die einzige Behörde: Nachrichtendienste und nicht zuletzt die Polizei haben jeweils eigene Abteilungen, die sich mit Cybersicherheit beschäftigen. 2022 hat das Bundeskriminalamt fast 140.000 Cyber-Straftaten in Deutschland erfasst.

Musik

Die Sicherheitsstrukturen gegen Cyberkriminalität müssen sich ständig weiterentwickeln, denn die Kriminellen werden immer professioneller: Wie sich die Cyberkriminalität seit den Anfängen des Internets entwickelt hat, darüber habe ich mit Eva Wolfangel gesprochen.

Eva Wolfangel: Die ersten Anfänge von so Computerwürmern und Viren, das fand ich total interessant, hatten keinen kriminellen Hintergrund, sondern waren mehr so Spielereien oder Neugier von jungen Menschen, die halt früher als der Rest der Welt verstanden haben, wie Computer funktionieren und wie man Schadsoftware verbreiten kann und damals waren das eben eher einfach so kleine Programme, die irgendwas in deren Augen Lustiges gemacht haben, wenn sie auf dem Computer von ihm anders angekommen sind, und dann hat sich daraus natürlich wie immer, wenn Kriminelle sehen, das ist was, womit man Geld machen kann, hat sich daraus über die Zeit eben echte Schadsoftware entwickelt und zum Beispiel die Möglichkeit, Dinge zu verschlüsseln oder natürlich auch Spionage. Das ist das andere, sobald man es schafft, Zugang zu bekommen zum Computer von anderen Menschen und Unternehmen und Staaten kann man natürlich auch wunderbar Spionage betreiben und das ist ja heutzutage auch ganz letztlich, ganz normal tragischerweise.

Holger Klein: Das heißt, moderne Cyber-Kriminalität ist diejenige, die ein Geschäftsmodell im Hintergrund hat?

Eva Wolfangel: Also hätte ich jetzt mal so gesagt, wenn wir das aufteilen wollen zwischen alt und modern, hätte ich gesagt, ja, dass diese Unternehmen und diese Kriminellen immer professioneller werden und die werden immer besser darin, sich zu verstecken. Die Schadsoftware wird immer besser, immer professioneller, immer schwerer zu entdecken. Also das ist vielleicht, wenn man so überlegen will, was ist die Entwicklung aktuell, das, was moderne Cyber-Kriminalität ist: top organisiert.

Holger Klein: Ist dem überhaupt was entgegenzusetzen?

Eva Wolfangel: Ja, man kann die Hürde hochsetzen und das hält wirklich viele Angriffe ab. Weil neben diesen toporganisierten Ransomwarebanden, die vielleicht wirklich mit sehr, sehr viel Aufwand hoch ausgefeilter Schadsoftware irgendwo eindringen, gibt es natürlich jede Menge Abstufungen bis hin zu Kleinkriminellen, die keine ausgefeilten Schwachstellen verwenden, die einfach Sicherheitslücken ausnutzen, die schon länger existieren, also die quasi ausnutzen, dass Menschen eben mit ihrer Cyberhygiene, wie manche sagen, nicht so aufm Topstand sind und die dann mit wenig Aufwand kleinere Summen erbeuten, aber das ist natürlich auch nervig und kann eben einzelne auch teuer zu stehen kommen.

Holger Klein: Sie haben eben gesagt, die Würmer, Viren, was ist eigentlich der Unterschied? Was ist ein Wurm? Was ist ein Virus? Und was gibt es da noch? Was ist ein Botnetz? Botnetz ist so das große Ding, was man zuletzt immer hört. Was ist das alles?

Eva Wolfangel: Also allenthalben gelten Viren oft so als Überbegriff oder Schadsoftware im Prinzip, das wird oft synonym mit Viren verwendet. Würmer sind Schadsoftware, die sich selbst verbreitet, also die, wo nicht quasi jemand im Hintergrund alles selbst von Hand steuern muss. Und Botnetze sind infizierte Computer, also das habe ich auch gesehen im Darknet. Es gibt quasi Angebote, da kann man Zugang zu Millionen infizierter Computer kaufen. Das sind dann so wie ja vielleicht Ihrer und meiner, also, ich hoffe es natürlich nicht, aber Computer, wo Menschen nicht so viel Wert drauf gelegt haben vielleicht oder nicht so hinterher waren, Updates einzuspielen, die irgendwie angreifbar waren. Also es gibt ganze eigene Zweige in diesem kriminellen Unternehmertum, die nur solche Zugänge suchen, die mit automatisierten Scans gucken, wo ist noch welche Sicherheitslücke offen und in diese Computer eindringen, sich dann da, ja, eine Hintertür einbauen und dann diesen Zugang verkaufen, dass Kriminelle, was auch immer damit machen können, zum Beispiel diese dann ausnutzen, um sogenannte Ddos-Attacken zu fahren, also konzertiert von sehr, sehr vielen dieser infizierten Computer eine Website aufzurufen oder eine Infrastruktur, die dann überfordert ist und in die Knie geht.

Holger Klein: Und die Betreiber dieser Bot-Netze sind immer die Russen. Steht jedenfalls in der Zeitung. Inwieweit sind russische Hacker vielleicht auch mit dem russischen Geheimdienst an solchen Dingen beteiligt?

Eva Wolfangel: Also ich würde eigentlich sagen, dass es nicht immer nur die Russen sind. Andererseits ist es schon so, dass der russische Staat, seine Cyberkriminellen gewähren lässt. Es gibt immer diese Geschichte, die mir viele Sicherheitsforscher erzählt haben, deswegen glaube ich, dass die wahr ist, dass wenn man in Russland als Cyberkrimineller eine Schadsoftware entwickelt, dann muss man dafür sorgen, dass man keine russischen Bürger und Unternehmen angreift, weil sonst wird man durchaus verfolgt und die machen das in der Art, dass ihre Schadsoftware erst mal guckt, wenn sie auf einem Computer ankommt, was für eine Tastatur benutzt denn dieser Computer. Wenn es eine russische Tastatur ist, dann machen die einfach nichts. Und ja, wenn man das macht, so heißt es zumindest, dann ist man Russland völlig unbehelligt und kann von da aus durchaus den

Rest der Welt angreifen und das ist aktuell insbesondere, natürlich auch im Interesse des russischen Staates.

Holger Klein: Das heißt, Russland führt im Netz einen Krieg gegen den Westen?

Eva Wolfangel: Das auf jeden Fall, genau und eben durchaus Hand in Hand mit den Kriminellen. Also ich habe auch bei meiner Buchrecherche gesehen, dass es einen sehr schlauen Kriminellen gibt, Yewgeni Bukatschew heißt der, der einen der bekanntesten und auch „besten" Banking-Trojaner entwickelt hat, also eine Schadsoftware, die dazu hilft, dass man Bankkunden infiltriert oder deren Computer und dann ihnen das Geld klaut, der sitzt in Russland und wird vom FBI gesucht, seit auch vielen, vielen Jahren mit der höchsten Summe, die man auf Cyber-Kriminelle hier ausgesetzt hat und ja, also offenbar hat auch das FBI keine Chance ihn zu finden.

Holger Klein: Lässt sich denn überhaupt mit Sicherheit sagen, dass irgendwelche Schadsoftware russischen Ursprungs ist? Also es ist immer so leicht, mit dem Finger drauf zu zeigen. Und es passt ja auch gerade sehr gut und es passt auch in die große Erzählung unserer Zeit, aber…

Eva Wolfangel: Also ich habe immer wieder Sicherheitsforscherinnen begleitet, wenn sie versucht haben so was rauszukriegen oder auch mir sehr genau erklären lassen, warum sie ziemlich sicher sind, dass eine Schadsoftware zum Beispiel aus Russland kommt, ein Angriff aus Russland kommt und da gibt es natürlich schon Indizien oder deutliche Zeichen, also eben angefangen von dieser Sache mit der Tastatur, über IP-Adressen, die kann man natürlich auch fälschen, bis hin zu wann sind die aktiv, in welcher Zeitzone sind die aktiv. Und ich habe beobachtet, dass immer dann, wenn sich quasi fast alle großen IT-Sicherheitsunternehmen einig sind, dass ein Angriff aus Russland kommt, dann denke ich, kann man davon ausgehen, dass das richtig ist. Selbst Kaspersky, was ja ein Unternehmen ist, was aus Russland selbst kommt, selbst die haben einfach sehr viele Angriffe dem russischen Geheimdienst zugeordnet, da denke ich muss man nicht mehr allzu viel zweifeln.

Musik

Holger Klein: Es gibt noch andere Länder neben Russland, in denen Cyberkriminelle ziemlich ungestört arbeiten können, erklärt Sven Herpig. Zum Beispiel Nordkorea und China:

Sven Herpig: In Nordkorea werden die Kriminellen noch genutzt zum strategischen Ziel des Landes, das heißt eben, Geld, finanzielle Werte nach Nordkorea transferieren, damit diese Werte umgemünzt werden können in zum Beispiel die Entwicklung von Nuklearwaffen oder so. In der Tat ist es so, dass die Vereinten Nationen Berichte rausgegeben haben, in denen sie versucht haben nachzuverfolgen, wie viel Geld durch Cyberkriminelle dem nordkoreanischen Staat jedes Jahr zugetragen wird, damit er eben seiner Aufrüstung, unter anderem so eine nukleare, fortsetzen kann. Und bei China ist es ein bisschen anders. Bei China ist es so, dass es oftmals Mitarbeiterinnen und Mitarbeiter des Staates sind, die tagsüber für zum Beispiel Cybersicherheitsbehörde arbeiten, und nachts sich ein Zubrot verdienen wollen, das nennt man Moonlighting, und dann eben kriminell aktiv werden.

Musik

Holger Klein: Maßnahmen zur IT-Sicherheit sollten natürlich nicht nur auf staatlicher Ebene oder in Unternehmen ergriffen werden. Ich habe mit Eva Wolfangel auch darüber geredet, welche Rolle jede und jeder einzelne dabei spielt:

Eva Wolfangel: Ich finde schon, dass IT-Sicherheit oft sehr viel technischer ist, als viele Unternehmen sich eingestehen, weil ich beobachte, dass gerade immer wieder gesagt wird: Der Mensch ist das Problem, der Mitarbeiter ist das Problem, die sind so doof und klicken auf irgendwelche Phishing-E-Mails. Ich habe jetzt eben auch schon einige sehr, sehr gut gemachte Phishing-E-Mails gesehen oder auch Test-Phishing-E-Mails sind ja auch viel im Umlauf, viele

Angestellte müssen ja grad zum Cyber-Sicherheitstraining, wo dann so Test-Phishing-E-Mails kommen. Und es zeigt sich immer wieder, selbst wenn die nicht auf einen persönlich zugeschnitten sind, da die massenhaft verschickt werden, trifft eine von diesen E-Mails immer wieder auf eine Situation, in der man selbst denkt, ja klar, total legitim, plausibel. Ich habe ja auf die E-Mail gewartet. Ist doch mein Kollege, der schreibt hier ja auch, es geht um das Thema, was wir gemeinsam bearbeiten. Natürlich klicke ich die an. Und das ist das Problem, dass irgendwann so eine E-Mail so gut passt, dass man einfach in dem Moment nicht nachdenkt und das kritische Denken nicht aktiv einschaltet, weil unser Gehirn eben so gestrickt ist, dass wir in so Situationen, in denen wir zum Beispiel unter Druck sind, die sind ja oft verbunden mit Zeitdruck diese Phishing-Mails. „Klicken Sie, das müssen Sie noch gleich machen, das geht nämlich dann nicht mehr“ oder „Achtung, wir haben was ganz Schlimmes auf Ihrem Bankkonto entdeckt“ und also so, solche Maschen führen dazu, dass das kritische Denken aussetzt. Und deswegen ist es gar nicht so einfach, das bewusst anders zu machen, weil wir in dem Moment in einer anderen, ja, unser Gehirn in einer anderen Phase ist. Und deswegen ist mein Reden eigentlich gerade immer: Natürlich ist es wichtig, skeptisch zu sein und vorsichtig zu sein mit E-Mails, auf jeden Fall. Ich bin es auch, bin sehr vorsichtig mit Anhängen. Aber Unternehmen dürfen sich damit nicht rausreden, dass sie sagen, wir haben doch hier so ein Awareness-Training gemacht. Niemand kann jetzt ja hier so blöd sein und auf eine Phishing-E-Mail klicken, sondern sie müssen für technische Sicherheit sorgen. Also wenn jemand einen Account übernimmt, dass man damit zum Beispiel nicht so viel anfangen kann, also so technische Sperren einbauen in die eigenen Systeme. E-Mails sortieren, also dass solche E-Mails gar nicht mehr ankommen, weil das ist auch technisch überhaupt nicht schwierig, zu gucken, kommt die E-Mail wirklich von da, wo sie vorgibt herzukommen und so weiter. Also solche technischen Maßnahmen, die gibt es, die werden bei weitem nicht ausgeschöpft von den meisten Unternehmen und das ist, finde ich, auf jeden Fall wichtig, damit anzufangen.

Musik

Holger Klein: Die Ziele sind klar: Bessere IT-Sicherheitssysteme, weniger Lücken, mehr Schutz. Die Ermittlungsgruppe Dawnbreaker, von der Eva Wolfangel vorhin erzählt hat, hat ein halbes Jahr lang die Kommunikation innerhalb einer Hackergruppe verfolgt. Der effektive Kampf gegen Cyberkriminalität braucht Zeit und Ressourcen. Und für den Ausbau der Sicherheitsstrukturen braucht es vor allem eins: Personal.

Sven Herpig: Wir haben davon nicht genug. Ich bin auch der Meinung, dass es wahrscheinlich vielleicht mit Ausnahme von Israel kein Land auf der Welt gibt, was genug IT-Sicherheitsfachkräfte hat. Wir haben in den letzten Jahren uns in Deutschland bei der Fachkräfteausbildung oder Bekämpfung des Fachkräftemangels im IT-Sicherheitsbereich darauf konzentriert, vorrangig Bachelor- und Masterstudiengänge zu schaffen. Das ist zwar ganz nett, aber was wir brauchen, sind keine Personen, die irgendwie formale Nachweise in irgendwelchen Kryptotechniken liefern können, sondern wir brauchen Leute, die Firewalls konfigurieren, Vorfälle aufklären und so weiter. Das heißt, wir brauchen hier Umschulungen, Ausbildung, Weiterbildung, etwas, was unter drei Jahren möglich sein muss, um möglichst viele Personen in den Bereich zu bekommen. Ein zweiter Punkt, der daran anknüpft, ist, diese Personen müssen dann auch, wenn sie in den Behördendienst eintreten, ein vernünftiges Auskommen haben und dürfen dann nicht im irgendwie mittleren oder gehobenen Dienst anfangen, nur weil sie kein Studium haben, aber mehr können als jemand, der irgendwie fünf Jahre lang studiert hat.

Holger Klein: Gerade wegen der erhöhten Gefährdung in Deutschland sind auch Gesetzesänderungen im Gespräch. Dann könnten die Sicherheitsbehörden besser gegen Cyberangriffe vorgehen, das ist die Hoffnung der Bundesregierung. Um welche Berechtigungen es dabei genau gehen würde, ist aber bisher unklar. Dass es auch in Zukunft erfolgreiche Cyber-Angriffe geben wird, darüber sind sich alle einig. Auch Sven Herpig sagt deshalb: Wir brauchen mehr Cyberresilienz.

Sven Herpig: Resilienz bedeutet einfach, zu sagen, okay, wir können nicht mehr unsere IT-Systeme und Netzwerke nur absichern und dann kommt keiner rein, sondern irgendwann wird irgendwer reinkommen. Und für diesen Fall müssen wir aufgestellt sein und da kommt die Resilienz ins Spiel. Das heißt, im einfachsten Modus vorhersehen, was passieren kann, den Schadensfall eingrenzen, wenn er eintritt, den operativen Betrieb wieder ins Laufen bringen, und dann natürlich die Schwachstelle schließen, über die die Kriminellen oder wer auch immer reingekommen ist.

Musik

Holger Klein: Cyberkriminalität wird uns weiter beschäftigen und stellt uns vor viele Schwierigkeiten. Aber es gibt auch Veränderungen zum Positiven, findet Eva Wolfangel. Ihr APuZ-Artikel zum Thema Cybersicherheit hat ein Happy End. Sie haben vorhin auch gesagt, Gegenmaßnahmen sind durchaus möglich. Heißt das, es wird alles ein bisschen besser?

Eva Wolfangel: Also was ich sehe ist, dass es eben mehr technische Möglichkeiten gibt sich zu schützen. Also es gibt ja mindestens zwei Seiten, die IT-Sicherheitsbranche, die furchtbar ungeduldig ist und mit normalen Menschen, die sagen, boah, ich kann mir einfach kein langes, komplexes Passwort merken und dann noch ein eigenes für jeden Dienst. Da kommt oft so eine Ungeduld. Und da sehe ich eine kleine Veränderung, dass es zumindest eine Bewegung gibt innerhalb dieser Community. Die sagt: Wir müssen Dinge so bauen, dass Menschen sie auch wirklich umsetzen können. Weil das ist natürlich was, was ganz, ganz oft vorkommt und da gibt es inzwischen auch einen eigenen Forschungszweig, der eben schaut, welche Kosten verursachen solche Sicherheitsmaßnahmen und quasi die Kosten-Nutzen-Wirkung eigentlich, funktioniert die eigentlich und wenn man merkt, nee, die dann auch anzupassen, sodass sie funktionieren für die Menschen und für die Sicherheit, also da sehe ich ein paar ermutigende Bewegungen und Diskussionen. Und auf der anderen Seite sehe ich, dass verbreiteter ist, zum Beispiel dass man Zwei-Faktor-Authentifizierung inzwischen fast überall machen kann.

Holger Klein: Was wären so zum Schluss die drei wichtigsten, praktischen IT-Sicherheitstipps, die Sie unseren Zuhörer:innen mit auf den Weg geben können?

Eva Wolfangel: Das eine habe ich ja gerade schon gesagt, Zwei-Faktor-Authentifizierung ist wirklich was, was hilft. Ich weiß, es ist nervig, mich nervt es auch jedes Mal, weil es natürlich Extrazeit kostet und Extraklicks. Aber das ist vom Kosten-Nutzenaufwand nach meiner Analyse wirklich eins der besten Mittel, also wirklich das zu verhindern, dass Kriminelle sich einloggen können in ihre Accounts, nur weil sie Passwörter erraten und das wendet man mit Zwei-Faktor-Authentifizierung relativ zuverlässig. Und dann Updates, also tatsächlich, wenn es ein Update gibt für den Computer oder fürs Handy, das nicht rauszögern, sondern updaten, weil da sind oft Sicherheitslücken, die quasi geschlossen werden mit so einem Update und da sind die Kriminellen hinterher. Die kriegen das ja auch mit und die sehen dann „Aha. Hier ist die Lücke!“ und dann suchen die automatisiert, welche Rechner haben das, haben die Lücke noch nicht gestopft und wie kommen wir da rein. Ja, und das letzte ist kritisches Denken und wie gesagt, das ist ein bisschen mit Vorsicht zu genießen, weil man natürlich diese Angriffe, diese sogenannten Social-Engineering-Angriffe, dazu gehören eben Phishing-Emails auch, also Angriffe, die auf uns Menschen abzielen, natürlich genauso gebaut sind, dass sie dieses kritische Denken aushebeln und versuchen uns dazu zu bringen, das nicht zu erreichen. Aber man kann sich ein bisschen drauf trainieren und das ist wirklich Training, weil das Gehirn ist plastisch, wissen wir ja, und verändert sich, einfach kritisch zu sein, vorsichtig zu sein. Anhänge nicht leichtfertig öffnen, wenn man auf einen Link klickt, also erstens gucken, ob man wirklich denkt, dass der Link legitim ist. Und man hat aber meistens eine zweite Chance, nämlich dann, wenn man gebeten wird, seine Zugangsdaten einzugeben. Da besonders vorsichtig sein, wenn irgendjemand mich bittet, meinen Zugangsdaten auf einer Website einzugeben, wirklich überlegen, hat das Hand und Fuß? Ist es die richtige Website? Sieht die aus wie immer und wenn man auch nur einen kleinen Zweifel hat, lieber einmal zu viel das Unternehmen anrufen und fragen,

ist das richtig? Und wenn man sich jetzt mal nur diese drei Sachen vornimmt, ist es doch schon viel überschaubarer, als wenn man einen Ratgeber liest und 100 Sachen bekommt, von denen man die Hälfte nicht versteht.

Holger Klein: Eva Wolfangel, vielen Dank.

Musik

Was wir also mitnehmen können:

1. Die Bedrohung durch Cyberkriminalität ist real: Das betrifft Unternehmen, Infrastruktur, Privatpersonen und politische Prozesse.

2. Um uns gegen Cyberkriminalität zu schützen, braucht es mehr Organisation und Investitionen in diesem Bereich. Ohne genügend Fachkräfte können wir uns nicht absichern.

3. Es braucht gute technische Lösungen im großen Stil, denn Menschen können nicht jeden Cybertrick durchschauen, aber jede und jeder einzelne kann auch zuhause den eigenen Computer ein bisschen sicherer machen.

Musik

Das war „Aus Politik und Zeitgeschichte“. In der APuZ zum Thema „Cybersicherheit“ finden Sie Beiträge von Eva Wolfangel, Lennart Maschmeyer, Matthias Schulze und Christian Stöcker, sowie Interviews mit Sven Herpig und Gerhard Schabhüser. Den Link zum Heft finden Sie in den Shownotes. Wir freuen uns natürlich über Feedback zu diesem Podcast. Fragen, Lob, aber auch Kritik können Sie uns schicken an apuz@bpb.de. In vier Wochen erscheint die nächste Folge, dann sprechen wir über die Rolle der Kirchen in Deutschland. Ich bin Holger Klein, und danke für die Aufmerksamkeit.

Musik

Der Podcast „Aus Politik und Zeitgeschichte“ wird von der APuZ-Redaktion in Zusammenarbeit mit hauseins produziert. Redaktion für diese Folge: Gina Enslin, Julia Günther und Lorenz Abu Ayyash. Schnitt: Oliver Kraus. Musik: Joscha Grunewald. Produktion: hauseins. Am Mikrofon war Holger Klein.