„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 29, 05.04.2023:
Phishing, Smishing, Quishing und Co. –
Das BKA ermittelt

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

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

Michael Münz: Ich bin Michael Münz und auch von mir ein herzliches Willkommen zu dem Podcast, der niemals eure sensiblen Daten abfragen würde. Ihr kennt das, diese Mails, in denen ihr aufgefordert werdet, Kontaktdaten anzugeben, eure Adressen, Bankverbindungen aktualisieren oder irgendwelche solche Aufforderungen. Aber genau darüber wollen wir heute reden, über Phishing.

Ute Lange: Das ist jetzt nicht das neueste Thema. Wir hatten das immer mal wieder in Folgen, manchmal am Rande, manchmal auch mehr im Mittelpunkt. Aber wir haben ja Fragen von euch erhalten, und es gibt auch immer wieder neueste Entwicklungen. Wir müssen das also noch mal vertiefen und mit unserem heutigen Gast auch nochmal eine ganz andere Perspektive beleuchten.

Michael Münz: Bei den neuesten Entwicklungen beziehst du dich auf den BSI-Bericht zum digitalen Verbraucherschutz 2022 vermutlich. Der ist jetzt gerade rausgekommen, und darin ist Phishing ein Fokusthema, weil, und da zitiere ich jetzt mal, sich die technologischen Möglichkeiten und Varianten von Phishing stetig weiterentwickelt haben.

Ute Lange: Genau das hatte ich auch gelesen, und die Kriminellen, so heißt es im Bericht, versuchen ja auf unterschiedlichsten Wegen an unsere und eure Daten zu kommen. Sie bauen auf immer perfideren psychologischen Aspekten und Komponenten. Sie setzen mit ihren Texten und Betreffs in diesen Mails auf aktuelle Themen wie Bereitschaft, zum Beispiel im Zusammenhang mit dem Krieg gegen die Ukraine. Sie spielen mit der Angst vor Inflation oder auch Energieknappheit. Sie suggerieren Zeitdruck und drohen sogar mit Geldstrafen, damit wir auf jeden Fall in diese E-Mail reingucken und dann auch noch, im besten Fall zumindest für die Kriminellen, auf den Link klicken, der da angeboten wird.

Michael Münz: Und ich muss zugeben, die Zeiten, in denen ich Phishing-Mails mit einem Blick erkannt habe, sind offenbar vorbei. Ich hatte letztens eine Mail, da ist mir das wirklich nicht aufgefallen. Da waren die Umlaute richtig, die Ansprache passte, die sah gut aus, und angeblich war das von dem Hoster meiner Webseiten. Weil die Geld haben wollten, habe ich die Mail dann einfach mal liegen lassen und gedacht, ja, ich kümmere mich später drum, und habe wirklich ein paar Tage lang immer in meinem Posteingang auf diese Mail geguckt, bis ich dann irgendwann merkte, dass die Kundennummer gar nicht stimmte. Und da bin ich dann misstrauisch geworden, und tatsächlich, das war ein Phishing Versuch, der mal richtig gut aussah.

Ute Lange: Ja, ich hatte in letzter Zeit auch mehrere Fälle, und zwei davon waren besonders bemerkenswert. Der eine war von der Bank, bei der ich tatsächlich Kundin bin. Die sah täuschend echt aus, klang auch so, das Impressum, alles, wie ich es kenne. Allerdings habe ich mich gewundert, dass die mir eine Mail schicken, weil wir vor kurzem, das war auch ein Angebot der Bank, in unserer Kommunikation auf eine App umgestiegen sind, wo ich ja vorher auch noch mal angeben muss, wo ich sicher sein kann, Zwei-Faktor etc pp. Das haben wir auch öfter hier schon gesagt. Also habe ich die dann einfach elegant ignoriert und gelöscht. Wenn es wichtig ist, kommt es wieder, habe ich mir gedacht. Dann kam man mal ein paar Tage später eine E-Mail von der Bank, bei der ich vor Jahren mein Konto hatte und gedacht habe, das gibt's doch nicht. Ich bin auch gar nicht mehr in deren Verteiler. Aber dass sah so echt aus, wenn ich das nicht sofort gemerkt hätte, dass es die falsche Bank ist, hätte ich gedacht, die ist tatsächlich von meiner. Also es ist schon ganz schön perfide, wie ich bereits gesagt habe, man muss sehr wachsam sein.

Michael Münz: Ja, Phishing-Methoden werden zunehmend professioneller und vielfältiger, denn neben den klassischen Phishing-Mails, über die wir jetzt gesprochen haben, nutzen Cyberkriminelle auch immer häufiger Fake-Webseiten, soziale Medien, SMS oder auch QR-Codes, wir müssen also reden über die Bedrohung Phishing, und dazu haben wir heute jemanden zu Gast, in dessen Namen auch schon mal selbst Phishing Mails verschickt wurden. Herzlich willkommen Carsten Meywirth!

Carsten Meywirth: Hallo zusammen.

Ute Lange: Ja Carsten, schön, dass du da bist. Du bist Leiter der Abteilung Cybercrime im Bundeskriminalamt. Viele von uns kennen das BKA, als magst du dich mal ganz kurz vorstellen und erzählen, wie du zu dieser Position gekommen bist. Also ich habe gelesen, du warst tatsächlich ganz klassisch Polizist.

Carsten Meywirth: Ja, richtig, also, mein Name ist Carsten Meywirth, und ich leite die Abteilung Cybercrime Bundeskriminalamt. Ich bin seit 1984 Polizeibeamter, habe angefangen bei der Schutzpolizei im Land Niedersachsen und bin dann drei Jahre später 1987 ins Bundeskriminalamt gewechselt, habe das nie bereut und bin dann irgendwann mal mit Cybercrime in Berührung gekommen, war vorher lange Jahre in

der Abteilung Informationstechnik im Bundeskriminalamt. Das war eine ganz gute Ausbildung, ganz gute Vorbildung für das, was einem dann in so einer Abteilung erwartet, und da kommt natürlich dann auch noch mal polizeiliche Aufgaben hinzu, also eine unwahrscheinlich spannende und interessante Tätigkeit.

Michael Münz: Ich hab es gerade schon mal erwähnt. Von dir waren auch schon mal Mails im Umlauf, die gar nicht von dir waren. Wie war das für dich, als du dann erfahren hast, dass Phishing Versuche in deinem Namen unterwegs sind?

Carsten Meywirth: Das war zunächst mal total überraschend, damit hatte ich gar nicht gerechnet. Aber auf der anderen Seite, das ist klar, diejenigen, die Kriminalität begehen, die Akteure auf der anderen Seite, die lesen halt auch mit, die beobachten das Geschehen sehr genau, und die suchen ständig nach neuen Narrativen, wie sie Legenden bilden können, wie sie vermeintlich sichere Ansprachen wählen können, und ja, dann haben wir natürlich sofort reagiert und entsprechend gewarnt.

Ute Lange: Ja, bevor wir jetzt noch tiefer in das ganze Thema einsteigen und tatsächlich mal mit eurer polizeilichen Brille auf dieses Thema Cybercrime schauen, können wir euch, glaube ich, auch erstmal gratulieren. Ihr werdet jetzt im April drei Jahre alt als Abteilung, also noch relativ jung, zumindest in dieser Form einer Abteilung. Magst du mal kurz einordnen, warum eure Abteilung gegründet wurde und was eure Zuständigkeiten sind, vielleicht auch in Abgrenzung zu anderen Behörden, wie zum Beispiel dem BSI, für das wir ja heute hier auch gemeinsam vor dem Mikro stehen.

Carsten Meywirth: Ja, also, das Bundeskriminalamt bekämpft natürlich schon länger Cybercrime, als es die Abteilung gibt. Wir sind mal gestartet als ein kleines Team, dann ist es ein Referat geworden, und 2013 war es dann eine Gruppe Cybercrime Bekämpfung in der Abteilung schwere und organisierte Kriminalität. Die habe ich damals auch schon geleitet. Drei Jahre lang und 2020 haben wir uns dann entschieden, einen Schwerpunkt zu bilden, also eine feste Prioritätensetzung vorgenommen und haben eine Abteilung daraus gemacht. Wir sind jetzt eine von elf Abteilungen im Bundeskriminalamt, und damit sind natürlich auch entsprechende finanzielle und personelle Ressourcensteigerung verbunden, das heißt, Ausdruck einer starken Schwerpunktsetzung bei der Kriminalitätsbekämpfung. Wir als Abteilung Cybercrime im Bundeskriminalamt stehen so auf zwei Säulen. Wir sind Zentralstelle der deutschen Cybercrime Bekämpfung, das heißt, wir erstellen Lagebilder, wir unterstützen die Bundesländer bei der Durchführung ihrer Ermittlungsverfahren, wir versorgen die mit entsprechender Beratung mit Informationen, und wir sind auch selbst Ermittlungsbehörde, und unsere Ermittlungszuständigkeiten richten sich nach dem Bundeskriminalamtsgesetz, und da sind wir zuständig bei Cyberangriffen auf kritische Infrastrukturen in Deutschland oder auf Bundesbehörden oder Bundeseinrichtung.

Michael Münz: Das heißt, ihr seid in erster Linie dafür da, die Kriminellen dann zu verfolgen, wenn es zu Straftaten kommt, die sie einrichten.

Carsten Meywirth: Ja, genau, Strafverfolgung ist unsere Mission.

Michael Münz: Wie wichtig eure Arbeit ist, zeigen auch ein paar Zahlen, die wir rausgesucht haben. Cybercrime gehört weiter zu den Phänomenbereichen, habe ich gelesen, mit dem höchsten Schadenspotenzial in Deutschland. Kannst du vielleicht an der Stelle einmal kurz erzählen, was Phänomenbereiche sind, weil das ein Wort war, über das ich gestolpert bin.

Carsten Meywirth: Ja, Erscheinungsform der Kriminalität. Wir unterscheiden ganz grob den Bereich Terrorismusbekämpfung, die organisierte Kriminalität, die Cybercrime, und Staatsschutzdelikte.

Michael Münz: Dann lege ich da jetzt mal konkrete Zahlen hinter, damit wir auch mal was haben, über das wir dann konkret sprechen können. 2021 verzeichnete die Polizeiliche Kriminalstatistik knapp 150000 Cybercrime Delikte, und durch den Branchenverband Bitkom wurde mal gerechnet, was diese Cybercrime-Schäden so insgesamt ausmachen, und da beliefen sich in Deutschland 2021 die Schäden auf 223 Milliarden Euro jährlich und sind damit mehr als doppelt so hoch wie noch 2019. Also, da schließen sich dann gleich zwei Fragen an, nämlich, wie erklärt ihr euch diesen Anstieg, und was sind das eigentlich alles für Straftaten, die dann diese Schäden zur Folge haben?

Carsten Meywirth: Darunter befinden sich viele Betrugsdelikte, wenn also jemand mit Kreditkartendaten eines anderen im Internet einkaufen geht. Darunter befinden sich aber auch schwere Straftaten wie die Kompromittierung des Online-Bankings mit nachgelagerten Betrugsstraftaten dann oder aber auch schweren Cyberangriffen. Angriffen, wie Ransomware. Wir sehen seit vielen Jahren Steigerungsraten. Das ist genau richtig beobachtet. So, seit 2015 bis 2020 haben sich die Fallzahlen in der polizeilichen Kriminalstatistik verdoppelt, und auch danach hat es wieder Steigerungen gegeben. Warum ist das so? Nun, die Digitalisierung ist ein ziemlich großer Trend. Immer mehr Lebens- und Arbeitsprozesse finden digital statt, und Straftäter nutzen das aus. Cybercrime ist eine Straftat, die ich von jedem Ort der Welt begehen kann. Ich brauche nur Strom und einen Internetanschluss, und dann kann ich loslegen. Und es ist auch deshalb so einfach, weil sich die kriminellen Akteure, so man kann sagen, ab 2015 besser organisiert haben. Seit 2015 beobachten wir eine hochprofessionell nach Arbeitsteilung funktionierende Underground Economy. Das ist eine kriminelle Dienstleistungsgesellschaft. Wir nennen das Crime Service, wo verschiedene kriminelle Akteure ihre inkriminierten Dienstleistungen anbieten. Die einen vermieten Server Bullet Proof, also sicher vor polizeilichen Maßnahmen, andere bieten Schadsoftware an. Und Dritte, die sorgen dafür, dass diese Schadsoftware nicht von den gängigen Antivirus Systemen erkannt werden können. Und dann gibt es

weitere Dienste wie die Geldwäsche oder das Verwerten der illegalen Gelder, so dass sich die Spur der Polizei verliert. Und dieser kriminelle Kosmos, der hat sehr stark dazu beigetragen, dass Cybercrime Straftaten sehr einfach geworden sind, weil ich mir alle Dienstleistungen zusammenkaufen kann.

Ute Lange: Also, da würde ich jetzt gerne nochmal ein bisschen näher einsteigen, weil wir haben ja gesagt, wir kriegen heute mal eine ganz andere Perspektive geboten. Das klingt auf eine gewisse Art und Weise spannend, also zumindest, wenn ich es im Fernsehen gucken würde. Aber du sprichst ja über die Realität, also habe ich das richtig verstanden? Cybercrime Service bedeutet, ich gehe in so einen, ich sag jetzt mal, Online-Shop für solche Angebote und Klick mir zusammen, was ich gerne hätte. Oder geht meine Fantasie jetzt gerade mit mir da weg?

Carsten Meywirth: Ich will natürlich keine Insider Tipps verraten hier in diesem Podcast, aber es ist in der Tat relativ einfach. Beispielsweise gibt es entsprechende Marktplätze im Internet, im Darknet, wo du entsprechende digitale Identitäten kaufen kannst. Das heißt, da werden Zugangsdaten auch gehandelt, Passwörter, Usernames, Zugang für bestimmte Accounts, aber auch für Banking-Accounts, beispielsweise Kreditkartendaten, und wenn du dir Kreditkartendaten holst, dann gehst du damit im Internet ein bisschen shoppen auf die Kosten eines anderen.

Michael Münz: Fangen wir mal bei den Daten an, von denen du gerade sprachst. Also ich gehe mal davon aus, dass Phishing eine Methode ist, wo kriminelle Daten sammeln, um die dann anzubieten. Wie kommen die denn sonst noch an unsere Daten ran? Also das, was dort angeboten wird, das muss ja irgendwo herkommen, und das liegt ja jetzt nicht auf der Straße rum. Also wie landen solche Daten dann bei diesen Verkäufern?

Carsten Meywirth: Es gibt beispielsweise eine sehr spezielle Tätigkeit, einen sehr speziellen Dienstleister in dieser Underground Ökonomie. Das sind die sogenannten Initial Access Broker. Die machen eigentlich nichts anderes, als Systeme zu kompromittieren und entsprechende Zugangsdaten abzuziehen, und die verwerten die nicht, indem sie beispielsweise dann selbst Betrugsstraftaten begehen oder Ransomware auf das System aufspielen, sondern die verkaufen diese Zugangsdaten ganz einfach an diejenigen, die dann ihr kriminelles Geschäft mit diesen Zugangsdaten betreiben.

Ute Lange: Also ganz arbeitsteilig wie in vielen anderen Bereichen, wo man halt eine Lieferkette hat, ja bis man dann zu seinem Endprodukt kommt.

Carsten Meywirth: Genau das ist so. Es gibt entsprechende Foren, wo man sich trifft. Das kannst du dir vorstellen, wie das Örtliche früher analog. Ja nur, dass das jetzt entweder im Clear Web oder im Darknet ist, und da trifft man sich, da werden die entsprechenden Dienstleistungen beworben, und dann setzt man die Gespräche mit

persönlichen Nachrichten fort und kommt dann zu entsprechenden Käufen und Verkäufen von Dienstleistungen.

Michael Münz: Stellen wir uns mal vor, ich wäre jetzt im Darknet unterwegs und hätte so einen Datensatz mit E-Mail-Adressen gekauft. Kann man ungefähr beziffern, wie viel ich dafür ausgegeben hätte? Gibt's Marktpreise?

Carsten Meywirth: Gibt schon Marktpreise. Ich glaube, E-Mail-Adressen sind relativ günstig. Auch Kreditkartendaten sind unterschiedlich bepreist, je nach Wertigkeit. Also das richtet sich dann danach, ob die Prüfkennziffer dabei ist, wie lange diese Kreditkarte noch ihre Validität hat, und du kannst sogar auch Schadsoftware kaufen oder aber auch natürlich Server mieten. All das hat seinen Preis. Für eine Schadsoftware bezahlt man auch schnell 1000 €. Ein Server ist da schon etwas günstiger anzumieten, und es gibt auch entsprechende Crypto-Dienste, die also prüfen, ob die Schadsoftware von den entsprechenden Antivirensystemen erkannt werden kann. Die kriegt man auch schon für 50 € im Monat.

Ute Lange: Okay, ich setze mich jetzt mal auf die andere Seite derjenigen, die sich in dem kriminellen Kosmos eben auch wirtschaftlich betätigen. Das klingt jetzt im ersten Moment noch nicht so, als wäre das so wahnsinnig lukrativ, aber offensichtlich ist es das, sonst würden die Zahlen ja nicht so steigen. Dann wieder zu euch zurück. Warum sollte jemand seine Fähigkeiten in diesem Bereich lieber bei euch einsetzen, also für die gute Seite? Und wie wird man dann auf eurer Seite Cyberkriminalist statt selber Krimineller?

Carsten Meywirth: Ja, die Antwort ist eigentlich relativ einfach. Unser Leitmotiv ist ja das richtige Tun im Bundeskriminalamt, das heißt, wir werben dafür. Wir suchen Menschen, die einen Sinn in dem erkennen, was sie tun, und Kriminalität bekämpfen, die Gesellschaft ein Stück weit gerechter machen. Das ist natürlich ein ganz wichtiges Motiv, und wir suchen Menschen, auch IT-Fachkräfte hier bei uns in der Abteilung. Wir haben so eine gute Mischung aus Vollzugsbeamten, die wir selbst ausbilden im Bundeskriminalamt, und IT-Fachkräften, die wir einstellen, die wir extern gewinnen. Und wenn du als Fachkraft zu uns kommst, dann kannst du bei uns als Analyst eingesetzt werden. Das heißt, du arbeitest sofort im Team mit einem Polizeikollegen zusammen an einem Schreibtisch, an einem Ermittlungsverfahren oder an einer Auswertung, oder aber du möchtest selber Cyber-Kriminalist werden, und dann kommst du zu uns als IT-Fachkraft, und wir schicken dich in eine verkürzte Laufbahnausbildung, also Polizeiausbildung, und wenn du die bestanden hast, dann arbeitest du als Cyber-Kriminalist und hast beide Kompetenzen, die der Polizei und die im Bereich der Informationstechnik.

Michael Münz: Okay, ich weiß jetzt also, dass ihr da seid, und bei einer Straftat auf der Straße zum Beispiel wüsste ich ja, ich rufe jetzt also per Telefon die Polizei an oder winke mir Polizisten hinzu, wenn mir auf der Straße etwas passiert oder ein Einbruch

ist. Aber wie komme ich denn an euch ran, wenn mir etwas passiert ist und etwas ja auch oft sehr Abstraktes, also wie kann ich euch das beschreiben? Wie finde ich euch da an der Stelle? Wann hole ich euch dazu?

Carsten Meywirth: Wir haben bei der Cybercrime-Bekämpfung in Deutschland ein Netzwerk von zentralen Ansprechstellen, die befinden sich in den Bundesländern, bei den Landeskriminalämtern und beim Bund, hier auch beim Bundeskriminalamt, und diese Ansprechstellen, die sind spezialisiert auf Cybercrime Delikte. Das heißt, die verstehen, was dir passiert ist, die können das einordnen, und die haben dann auch den direkten Rat natürlich zu den Ermittlungskollegen, und da ist dann Hilfe sehr schnell und sehr kompetent möglich.

Ute Lange: Jetzt würde ich gerne nochmal auf das Thema Phishing kommen, weil das ist ja in dem vorhin schon genannten Bericht zum digitalen Verbraucherschutz von WSI als Evergreen krimineller Methoden bezeichnet. Evergreen ist ja immer, das gibt es offensichtlich schon länger, das können wir in höherem Alter dann schon mitsingen. Offensichtlich ist das jetzt nicht das neueste, aber es gibt immer wieder neue Tricks und Vorgehensweise. Warum hat es eine solche Relevanz, dass ihr euch auch so darum kümmert?

Carsten Meywirth: Phishing ist eine ganz wichtige Art, um weitere schwere Straftaten vorzubereiten. Deswegen gibt es das auch schon so lange. Das gibt es so lange, wie es digitale Daten gibt. Es ist ganz wichtig, wir bezeichnen diese Credentials oder die persönlichen Daten, die die Täter abfischen, als Rohstoff für die Cyberkriminellen. Das heißt, die brauchen diese Daten, um weitere Straftaten zu begehen. Diese Daten, das sind Zugangsdaten wie Username oder Passwort für bestimmte Accounts, und die braucht man, um dann entsprechende Verwertungstaten zu begehen, beispielsweise beim Kompromittieren des Online-Bankings oder aber auch, um Systeme zu infiltrieren, und dann Ransomware Straftaten zu begehen.

Ute Lange: Das heißt, um das nochmal auf die analoge Welt zu übertragen, das ist im Grunde genommen der Schlüssel für meine Wohnungstür. Wenn die Kriminelle haben, können sie sich ja frei bewegen und müssen sich nicht mehr besonders anstrengen, da reinzukommen.

Carsten Meywirth: Ja, genau das ist eine Vorbereitungstat, wenn man so will, die allerdings auch schon eine Straftat ist, wenn die Kriminellen in Systeme eindringen und sich dort mit Daten versorgen, aber eine ganz wichtige Vortat für weitere Verwertungstaten wie Online-Banking kompromittieren oder Ransomware verteilen.

Michael Münz: Richten sich denn so Cyberkriminelle also an alle bei uns in der Gesellschaft? Oder könnt ihr auch sehen, dass es da einen Fokus gibt, dass die zum Beispiel versuchen, Unternehmen lahm zu legen? Oder wir hatten auch schon oft das

Beispiel öffentlicher Bereich, dass Städte lahm gelegt worden sind, also suchen sie gezielt nach lukrativen Angeboten, oder sind wir erst mal alle potenziell Opfer?

Carsten Meywirth: Ich glaube, potenziell sind wir alle Opfer gerade bei Betrugsstraftaten. Die finden auch gegen private Nutzer statt. Wir sehen allerdings bei den schweren Straftaten den Fokus eindeutig auf Unternehmen. Wir bezeichnen das als Big Game Hunting, was die Cyberkriminellen da machen. Das heißt, die versuchen natürlich, wenn sie schwere Straftaten wie beispielsweise Ransomware-Straftaten begehen, nach Möglichkeit ein Opfer zu finden, das in der Lage ist, ein möglichst hohes Lösegeld zu bezahlen, und dann priorisieren die ganz einfach auch bei sich, so wie wir unsere Tätigkeiten priorisieren, und dann nimmt man natürlich lieber ein Unternehmen mit hohem Umsatz, das in der Lage ist, ein hohes Lösegeld zu zahlen, als irgendein Privatmann oder eine -frau, die gar nicht in der Lage wäre, so viel Lösegeld zu zahlen.

Ute Lange: Und auch da wieder die Analogie. Der Name Big Game kommt ja tatsächlich vom Jagen, wenn man Großwild jagt. Also da habe ich dann auch wieder gleich ein Bild in der analogen Welt, wobei das ja nicht immer kriminell ist, aber manchmal auch. Ich würde jetzt nochmal gerne gucken auf so besondere Fälle, die wir auch schon hier hatten. Vielleicht kannst du uns da noch mal Einblicke geben. Immer wieder haben wir hier Emotet gehabt, und 2021 gelang euch, ich glaube in Kombination mit anderen Ermittlungsbehörden, ein großer Schlag. Also es hieß dann auch, Emotet ist jetzt erst mal weg vom Markt. Jetzt haben wir gelesen, das seit Anfang des Monats Cyberkriminelle wieder auf Opfersuche gehen. Genau mit dieser Software, das ist eine Ransomware. Kannst du vielleicht nochmal genauer erklären, wer steckt denn jetzt dahinter, und wie gehen sie diesmal vor?

Carsten Meywirth: Ja, Emotet war in der Tat ein Riesenerfolg von uns. Der Präsident des BSI hat irgendwann mal Emotet als den König der Schadsoftware bezeichnet, und wir haben dann erkannt, Emotet richtet enormen Schaden an. Viele Angriffe richteten sich auf deutsche Ziele, viele Unternehmen waren betroffen, Behörden sind betroffen gewesen, und dann habe wir den entsprechenden Schwerpunkt gesetzt. Bei uns hier, auch im Bundeskriminalamt, haben wir ein Ermittlungsverfahren eröffnet, haben zweieinhalb Jahre ermittelt im Rahmen einer internationalen Allianz. Wir waren mit den Amerikanern zusammen, mit den Briten, mit den Franzosen, mit den Esten, mit den Niederländern und haben uns immer weiter vorgearbeitet in dieser Allianz. Konnten immer mehr der kriminellen Infrastruktur aufklären, die die Täter hinter Emotet benutzt haben. Die hatten mehrere 100 Server weltweit angemietet und betrieben, die hatten ein riesiges Botnetz, und wir haben dann einen Plan zusammengeschmiedet, wie wir diese Infrastruktur runternehmen können, wie wir den Takedown durchführen können, und das haben wir getan in einer Art und Weise, die vorher keiner vor uns getan hat. Wir waren in der Lage, diese Infrastruktur, die die Täter benutzt haben, komplett aufzuklären, und konnten auch den Administrator

dieser Infrastruktur identifizieren und konnten ihn, über ein Rechtshilfeersuchen an die ukrainischen Behörden, auch festnehmen lassen und auch vernehmen lassen. Der war kooperativ, der hat uns auch Zugänge zur Infrastruktur noch ermöglicht, und wir haben dann diese Schadsoftware nochmal versandt und haben ihr aber freundliche IPs mitgegeben, sodass die gesamten Bots, das heißt die Opferrechner, nicht mehr zur Täter-Infrastruktur, zu den feindlichen Servern zurückfunken, sondern zu unserer. Das heißt, wir haben den Tätern die Opfer weggenommen und haben gleichzeitig die Server, die sie benutzt haben, um diese Straftaten zu organisieren, also beispielsweise die Schadsoftware weiterzuentwickeln, das Spamming durchzuführen von E-Mails, die haben wir zerstört und haben ihnen insofern die gesamte Infrastruktur weggenommen. Das war sehr effektiv, sehr nachhaltig. Wir haben dann auch zehn Monate lang nichts von Emotet gehört. Dann kam ein kleines Lebenszeichen, ein Tech-Dienstleister, der sagt hier, das ist wieder Emotet, wir erkennen das, und sie sind langsam wieder zurückgekommen. Aber sie haben längst nicht die Gefährlichkeit, die sie hatten, bevor wir hier zugeschlagen haben. Vielleicht noch ein Wort zu der Art und Weise, wie Emotet vorgegangen ist und was das Geschäftsmodell davon gewesen ist. Selbst haben die gar nicht mehr die Ransomware verteilt, sondern es ist ein sogenannter Dropper Dienst gewesen. Das heißt, das ist auch einer der speziellen Dienste in der Underground Economy, in diesem Bereich der Dienstleistungsindustrie, die einen Zugang zu verschiedenen Opfer-Systemen vorhalten und dann anbieten. Und wenn dann eine Ransomware Gruppierung wie beispielsweise Conti LockBit diese Dropper nutzt, um sich mit ihrer Schadsoftware Zugang zu verschaffen, und dann ist das für die ein einfaches, Systeme zu kompromittieren und ihre Ransomware quasi auf die Systeme zu verteilen und auch die Straftat dann erfolgreich durchzusetzen.

Michael Münz: Jetzt stelle ich es mir total deprimierend vor, dass man wirklich jahrelang hinter jemanden hinterher war oder nach einer Struktur, die dann erschlagen hat, und dann kommt das einfach wieder. Ist es nicht total demotivierend?

Carsten Meywirth: In diesem Fall war es gar nicht demotivierend, sondern es war ein Riesenerfolg, weil wir zehn Monate nichts gehört haben. Ja, dann kam etwas zurück, aber das, was zurückkam, ist längst nicht so stark, längst nicht so gefährlich und kann längst nicht so viel Schaden verursachen wie vorher. Das heißt, wir haben ja einen erheblichen Wirkungstreffer erzielt.

Ute Lange: Michael hat ja gerade von demotiviert gesprochen. Ich würde jetzt nochmal auf die Motivation bei euch im BKA vor allen Dinge in eurer Abteilung zu sprechen kommen. Was motiviert Euch? Du hast ja schon gesagt, das Motto ist das richtige tun. Aber was sind da noch für Faktoren drin? Also ich finde, es klingt jetzt auch so ein bisschen wie ein Krimi. Also ich könnte mir vorstellen, wir könnten jetzt noch stundenlang weitersprechen, und du würdest wahrscheinlich gar nicht alles sagen dürfen, was wir wissen wollen, weil natürlich auch nicht da draußen bekannt

geben wollen, wie ihr vorgeht. Aber was sind so die Motivationsfaktoren, sich bei euch zu engagieren, dass wir alle am Ende sicherer sind?

Carsten Meywirth: Ich glaube, dass eine ist, dass wir natürlich eine unwahrscheinlich interessante und spannende Aufgabe haben, die nicht jeder hat: die Kriminalität zu bekämpfen, gegen kriminelle Akteure vorzugehen. Das ist natürlich eine unheimlich spannende Aufgabe, und dann versuchen wir natürlich hier gerade bei uns in der Abteilung Cybercrime über ein modernes Führungs-Management und auch über moderne Strukturen wie beispielsweise Kommunikationsstrukturen, flache Hierarchien und entsprechende Kompetenz, Bildung und Teambildungsmaßnahmen ja so eine Einheit zu werden und einen ganz besonderen Spirit zu leben.

Michael Münz: Letzte Frage noch, die mich interessiert. Wenn ich das nächste Mal so eine Phishing-Mail bekomme, lösche ich die und denk so, ah, ich kriege die nicht, oder sage ich irgendwem Bescheid, dass da wieder was unterwegs ist.

Carsten Meywirth: Grundsätzlich ist es so, dass wir immer empfehlen, polizeiliche Anzeige zu erstatten. Wenn eine Cybercrime-Straftat nicht angezeigt wird, der Polizei nicht zur Kenntnis gerät, dann findet sie quasi für unseren Ressourcengeber, für die Politik, die Regierung, nicht statt, und insofern ist es wichtig, dass eine Straftat angezeigt wird, dass wir die Möglichkeit bekommen, Täter zu ermitteln, die Straftat aufklären zu können, dass sie aber auch zur Kenntnis genommen wird, dass es hier ein sehr starkes Straftatenaufkommen gibt und dass man die Bekämpfung in diesem Bereich stärken muss.

Ute Lange: Ich hab da auch noch einen Tipp für unsere Hörer und Hörerinnen. Ich habe in der Recherche entdeckt, dass die Verbraucherzentrale, ich glaube, es ist NRW, die haben eine Facebook-Seite, einen Twitter-Account und ihre eigene Webseite, wo die jeden Morgen den neuesten Phishing-Trend melden. Also, statt morgens in die Zeitung zu gucken oder sich Kaffee zu kochen, sollte man heute offensichtlich das als erstes tun, damit man tagsüber nicht über irgendwas stolpert, was dann hinterher großen Schaden anrichtet. Würde ebenso zustimmen. Was macht ihr denn morgens als allererstes?

Carsten Meywirth: Ja, bei mir ist es so. Ich lese als allererstes natürlich die Aufbereitung der Medien und unsere tägliche Lage. Also was ist am Vortag passiert? Welche Straftaten sind passiert? Was sind die neuesten Meldungen? Auch damit werde ich hier versorgt von den Kolleginnen und Kollegen von meinem Team. Das ist ganz wichtig. Das kann natürlich auch als Privatmann nicht schaden, wenn man sich entsprechend informiert, weil gerade als privater Nutzer muss man dann auch entsprechend sensibilisiert sein.

Michael Münz: Das nehmen wir gerne mit, und ich werde auch noch mal genauer hinschauen, das nächste Mal, wenn so Mails kommen, die eigentlich aussehen, als

seien sie echt, damit mir nicht noch mal so ein Fehler passiert oder ich womöglich noch draufklicke. Casten, vielen Dank, dass du dir die Zeit genommen hast, uns einen Einblick in eure Arbeit zu geben, zu wissen, dass da jemand ist, der den Leuten hinterherrennt, die uns mit Phishing-Mails, mit den Versuchen überhäufen, unsere Daten Preis zu geben. Gut, dass ihr da seid, und vielen Dank, dass du dir die Zeit genommen hast.

Carsten Meywirth: Sehr gerne, herzlichen Dank für diese Möglichkeit an euch!

Ute Lange: Ja, danke auch von mir. Wir haben ja vorhin so ein bisschen über Onlineshoppen gesprochen, aber in einem etwas anderen Kontext, nämlich in einem kriminellen Kosmos, den Casten beschrieben hat. Es gibt aber auch noch einen anderen Anlass, darüber zu sprechen, weil unsere Daten ja nicht nur über Phishing ins Netz kommen, also nicht nur, weil andere sie abgreifen, sondern vor allen Dingen beim Onlineshop sind wir selber sehr großzügig damit, und wir haben jetzt eine Studie vom BSI auf dem Markt und haben uns die auch mal so ein bisschen angeguckt. Die haben nämlich Softwareprodukte für Onlineshops auf Schwachstellen untersucht, und ehrlich gesagt, finde ich dieses Ergebnis relativ ernüchternd und kann euch nur empfehlen, mal in die Studie und Ergebnisse zu schauen, und vielleicht werden wir dann alle auch beim Vergnügen oder eben manchmal auch Missvergnügen online bisschen sparsamer mit den Daten, die wir da freiwillig in das große weite Internet verstreuen.

Michael Münz: Genau und wie in der vergangenen Folge auch, wollen wir euch zum Abschied auch noch eine Frage beantworten, die ihr uns geschickt habt. Wir gucken ja immer, was so aus der Community bei uns landet, was ihr von uns wissen wollt, und da gab es eine Frage, die wir euch in dieser Folge beantworten wollen, nämlich wie hilfreich ist der Einsatz einer VPN-Verschlüsselung, und die Antwort darauf ist, das kommt ganz darauf an, was ihr eigentlich vorhabt.

Ute Lange: Sehr unbefriedigende Antwort, aber wir möchten da gerne auch noch ein paar Erläuterungen geben, damit ihr wisst, warum das mal so und mal so zu betrachten ist. Das hilft ja auch beim Handel. Also VPN, Virtual Privat Network, wird für zwei Dinge sehr geschätzt: Zum einen ändert es die IP-Adresse, also praktisch die Anschrift deines Rechners, mit der du oder ich oder wir alle im Internet surfen, und zum anderen schickt es Daten verschlüsselt zu dem Empfänger am anderen Ende, wenn du etwas rausgeben willst.

Michael Münz: Genau, und den letzten Fall, den kennen wir ja spätestens seit der Pandemie alle aus dem Homeoffice. Wir verbinden uns mit einem VPN, das uns wie ein Tunnel von allen anderen abgeschirmt, in das Netzwerk unserer Firma bringt und zwischen dem Gerät und dem VPN Server alle übertragenen Daten durch Verschlüsselung vom restlichen Internet abschirmt.

Ute Lange: Diese Verschlüsselung gräbt quasi einen abhörsicheren Tunnel durch das ungeschützte Internet, das ja seine Gefahren birgt, wie wir auch heute wieder gehört habe. Wie diese Tunnelleitung, lassen sich schutzwürdige Daten von jedem beliebigen Ort aus, also in andere Länder, andere Kontinente, auf gesicherte Art und Weise mit einem lokalen Netzwerk austauschen, und das hat schon für viele Menschen in anderen Ländern eine große Relevanz. Weil ihnen dort oft der Zugang zum Internet verwehrt ist. Per VPN kommen sie an Daten ran zum Beispiel Nachrichten, die wir als selbstverständlich empfinden. Wie auch gerade gesagt hat, kriegt er jeden Morgen diese, dass es in vielen Ländern auf dieser Welt nicht so selbstverständlich, und da werden auch oft VPN Verbindungen genutzt.

Michael Münz: Damit noch mal wieder zurück zu der, wie du sagst, unbefriedigenden Antwort, also für den digitalen Alltag, für das, was wir so normalerweise im Internet machen: Webseiten aufrufen, sozialen Netzwerken folgen, auch Nachrichten lesen, dafür ist VPN eigentlich ein bisschen übertrieben. Also dafür müssen wir jetzt hier uns weder verstecken oder unsere Identität verschleiern, noch einen Tunnel graben, um unsere Nachrichtenseiten aufzurufen.

Ute Lange: Na ja, wenn wir aber zum Beispiel unterwegs sind und dann eventuell Bankgeschäfte machen möchten oder andere Dinge, wo unsere Daten wieder besser geschützt sein sollten, dann kann es durchaus von Vorteil sein, darauf wieder zurückzugreifen und nicht beispielsweise auf einer Zugfahrt einfach mal eine Überweisung tätigen. Das ist vielleicht nicht unbedingt die beste Idee.

Michael Münz: Vielleicht noch ein kleiner Hinweis und damit auch der Bogen zurück zu den Cyberkriminellen, über die wir jetzt auch schon viel gesprochen haben in dieser Folge. Wie jede Technik hat VPN ja auch eine andere Seite, sprich, für Kriminelle ist es natürlich auch so reizvoll, die Identität zu verschleiern. Also auch da ist dann VPN vielleicht ein Mittel der Wahl. Mehr Informationen zu dem Thema haben wir euch in die Shownotes gepackt, und dann schauen wir mal, was ihr für die nächste folgende für Frage habt.

Ute Lange: Genau, weil wir wollen uns in der kommenden Folge noch mehr mit euren Fragen beschäftigen. Wenn ihr noch eine stellen möchtet, dann schreibt uns doch, kontaktiert uns gerne über die BSI-Kanäle auf Facebook, Instagram, Twitter sowie YouTube oder schickt uns eine E-Mail an die Adresse. Heute versuche ich es selber mal, und vielleicht auch stolperfrei. Podcast@bsi.bund.de. Geschafft! Wir freuen uns auf eure Post.

Michael Münz: Ja, und nicht nur auf eure Post, sondern auf eure Meinung. Wir haben nämlich einen kleinen Link noch in den Shownotes, wo ihr uns per Umfrage sagen könnt, was ihr an dem Podcast vielleicht noch ändern wollt, welche Wünsche ihr habt oder Verbesserungsvorschläge. Also auch da sind wir in dieser Frage ganz kundenorientiert. Also ihr könnt uns schreiben, ihr könnt uns per Link Antworten. Wir

sind auf jeden Fall daran interessiert, von euch zu hören und sagen schon mal, vielen Dank fürs Mitmachen.

Ute Lange: Ja, und bis wir uns Wiederhören in der nächsten Folge, folgt doch dem Podcast Update verfügbar auf euren präferierten Podcast-Plattform, denn so verpasst ihr keine Folge und könnt auch vorherige nochmal nachhören. Bis wir uns dann tatsächlich Wiederhören, mit neuen Infos, sagen wir wie immer tschüss, und bis bald!

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