Subject: WG: + Putins Krieg: Nebenschauplatz Cyberraum +
From: Johannes Steger <Johannes.Steger@tagesspiegel.de>
Date: 25/02/2022, 06:06
To: "Reinhold, Thomas" <reinhold@peasec.tu-darmstadt.de>

Lieber Herr Reinhold,

anbei die Ausgabe – und hier der Link:

https://background.tagesspiegel.de/cybersecurity/die-angriffsmethoden-passen-ins-gesamtbild

Noch einmal vielen Dank und herzliche Grüße
Johannes Steger

Von: Tagesspiegel Background Cybersecurity <info@background.tagesspiegel.de>
Gesendet: Freitag, 25. Februar 2022 05:46
An: Johannes Steger <Johannes.Steger@tagesspiegel.de>
Betreff: + Putins Krieg: Nebenschauplatz Cyberraum +

+ Faeser warnt vor Cyberangriffen + Standpunkt: Markus Richter im Podcast + Ungenaues IT-Sicherheitsrecht +

TAGESSPIEGEL
BACKGROUND

Cybersecurity

Ihr politischer Wissensvorsprung für Cybersecurity, 25.02.2022

Sehr geehrter Herr Steger,

es ist **Krieg in Europa** seit auf Geheiß von Wladimir Putin am frühen Donnerstagmorgen russische Truppen die Ukraine angegriffen haben. Ein völkerrechtswidriger Vorgang, den deutsche Politiker:innen in ungewohnter aber angemessener Weise verurteilt haben, und den Aggressor klar benannt haben: „Das ist Putins Krieg“, stellte

Bundeskanzler **Olaf Scholz** (SPD) fest. Außenministerin **Annalena Baerbock** (Grüne) sprach von einem „Tag der Schande“, den die Weltgemeinschaft nicht vergessen wird. Der russische Präsident habe „sich als ein Lügner selbst entlarvt“ sagte am Nachmittag **Bundesfinanzminister Christian Lindner** (FDP). **Verteidigungsministerin Christine Lambrecht** (SPD) warf Putin vor, „seine Großmachtfantasien“ mit einem brutalen Angriffskrieg auszuleben.

Der **Cyberraum** ist im Kontext der tatsächlich in der Ukraine stattfindenden Kämpfe mit konventionellen Waffen und im Kontext von Menschen, die sich vor dem Krieg flüchten müssen, nur ein Nebenschauplatz. Als Fachmedium für Cybersicherheit konzentrieren wir uns dennoch auf dieses Thema – und wissen, dass es in der **Lebenswirklichkeit der Ukrainer:innen** derzeit ganz andere Prioritäten gibt.

Aber zur Realität eines Krieges im 21. Jahrhundert gehört auch, dass die mit konventionellen Mitteln ausgetragene Invasion längst auch von **digitalen Angriffsmaßnahmen flankiert** wird. Was wir über die Dimension des Krieges im Cyberraum wissen und wie gefährlich die neu aufgetauchte Schadsoftware **Hermetic Wiper** ist, hat mein Kollege Jens Ohlig für Sie aufgeschrieben.

Für eine bessere Analyse und Einordnung der russischen Aggressionen im Cyberraum hat mein Kollege Johannes Steger gestern mit **Thomas Reinhold** gesprochen. Reinhold ist Experte für Militarisierung im Cyberspace und forscht an der Technischen Universität Darmstadt. Warum außerdem **Bundesinnenministerin Nancy Faeser** (SPD) gestern ein weiteres Mal vor der Gefahr von Cyberangriffen in Deutschland gewarnt hat, lesen Sie in den Nachrichten.

Das **IT-Sicherheitsgesetz 2.0** ist schon einige Monate in Kraft, doch in der praktischen Umsetzung der neuen Regelungen bleiben viele Fragen offen. Zu vage, wenig praxistauglich und viele bürokratische Pflichten – so das wenig schmeichelhafte Urteil von **Lutz Martin Keppeler**. Wie er zu diesem Fazit kommt, das erklärt der Fachanwalt

für IT-Recht heute im Standpunkt.

Mit „Rohrpost auf die Ohren“ bietet das **Bundesinnenministerium** seit geraumer Zeit einen eigenen Podcast. In einer der vergangenen Folgen sprachen der **Bundes-CIO Markus Richter** und die Informatik-Professorin **Haya Shulman** über die politische Dimension von Cybersicherheit. Meine Kollegin Selina Bettendorf hat die Folge für Sie rezensiert.

Paul Dalg

Die wichtigsten Themen im Überblick:

- Wie Russland den Angriff auf die Ukraine mit Cyberangriffen flankiert
- Nachgefragt: „Die Angriffsmethoden passen ins Gesamtbild“
- Standpunkt: Unpräzises IT-Sicherheitsrecht – Daran ändert auch das IT-SiG 2.0 nichts
- Podcast-Rezension: Digitale Rohrpost aus dem BMI
- Bundesinnenministerin warnt erneut vor Cyberangriffen in Deutschland
- Britische Großbank Lloyds: Rechnen mit russischen Cyberattacken
- US-amerikanische Sicherheitsbehörden: Neue Malware aus Russland entdeckt
- IBM-Studie: Fertigungsindustrie ist das Top-Ziel von Ransomware-Kriminellen

Presseschau

Angriff auf Ukraine: US-Geheimdienstschef warnt Satellitenbetreiber | *heise.de*
Ukraine calls on hacker underground to defend against Russia | *reuters.com*
Telekomchef Höttges warnt vor Cyberattacken in der Ukrainekrise: „Die Bedrohung ist da“ | *handelsblatt.com*
Biden has been presented with options for massive cyberattacks against Russia | *nbcnews.com*
Cybersecurity stocks are a bright spot as Russia-Ukraine conflict prompts cyberattack fears | *cnbc.com*
Facebook schaltet Sicherheitstool für Nutzer in der Ukraine frei | *deutschlandfunkkultur.de*
So leicht macht es Facebook einem falschen Elon Musk | *spiegel.de*
EU-Datengesetz: "Großer Wurf", aber auch ein Drahtseilakt | *heise.de*
Pakistan: New cybercrime law threatens to to stifle social media dissent | *dw.com*
Passwort-Manager 1Password setzt auf Krypto-Partnerschaften | *heise.de*
Cybersicherheit in Deutschland: noch viel Luft nach oben | *it-business.de*
War in Ukraine risks scrambling the logic of cyber security | *ft.com*
Datenschutz im Netz variiert stark - auch nach Alter | *deutschlandfunknova.de*
Alternative Videokonferenz-Systeme müssen sich nicht verstecken | *netzpolitik.org*

Analysen & Hintergründe

RUSSLAND-UKRAINE-KONFLIKT

Wie Russland den Angriff auf die Ukraine mit Cyberangriffen flankiert

Russlands Krieg in der Ukraine wird begleitet von DDoS-

Angriffen und Malware-Infektionen, die als Teil der russischen Militärstrategie seit Anfang des Jahres unterstützend eingesetzt werden. Sicherheitsforscher:innen haben die jetzt eingesetzte Schadsoftware „Hermetic Wiper“ analysiert. Eine technische Einordung der Cyberdimension des Kriegs.

Jens Ohlig

Russland hat in der gestrigen Nacht mit der Invasion der Ukraine begonnen. Am frühen Donnerstagmorgen wurde das ukranische Landesgebiet an mehreren Flanken angegriffen. Schon seit längerem bearbeiten Cyberkriminelle die **Flanke im Cyber- und Informationsraum**. Dazu gehört unter anderem die mutmaßlich aus Russland gesteuerte **Defacing-Attacke**, bei der im Januar Internetseiten der ukrainischen Regierung mit „digitalen Graffiti“ verunstaltet wurden (Background berichtete). Kurz danach entdecken IT-Sicherheitsexpert:innen Spuren einer Schadsoftware. In der vergangenen Woche folgten Attacken per Distributed Denial of Service (DDoS) auf ukrainische Ministerien und Banken (Background berichtete).

Als am Donnerstagmorgen Explosionen die ukrainische Hauptstadt Kiew und andere große Städte erschütterten, **hatten neue Cyberattacken schon wieder begonnen**: Die Websites des ukrainischen Verteidigungs-, Außen- und Innenministeriums waren am Donnerstag erneut nach einer Welle von DDoS-Angriffen unerreichbar oder nur sehr langsam zu laden. Zusätzlich entdeckten Cybersecurity-Forscher:innen, dass nicht identifizierte Angreifer **Hunderte von Computern** mit **zerstörerischer Malware** infiziert hatten, einige davon in den Nachbarländern Lettland und Litauen.

Schadsoftware „Hermetic Wiper“ zerstört Computer vollständig

Unter anderem hatten die Sicherheitsfirmen **ESET**, **Symantec** und **SentinelOne** die mittlerweile unter dem Namen „**Hermetic Wiper**“

bekannte Malware beschrieben. Bei einem Wiper handelt es sich um eine **Schadsoftware zur Datenvernichtung**, der unwiederbringlich elektronische Speichermedien löscht. Die Software ist in technischer Hinsicht ähnlich dem Wiper „**WhisperGate**“, der bei einem Angriff im Januar in der Ukraine verwendet wurde.

Bei „Hermetic Wiper“ werden notwendige Daten für den Systemstart des Computers im Master Boot Record (MBR) der Festplatte überschrieben. Dadurch wird der Computer **vollständig unbenutzbar**. Wiper überschreiben den Speicherbereich bis zu 35-fach, wodurch selbst mit einem Magnetkraftmikroskop keine physikalischen Spuren der ursprünglichen Daten mehr rekonstruierbar sind. Laut einer Analyse von SentinelOne wird dabei ein **signierter Treiber** verwendet, um Windows-Geräte und Schattenkopien zu löschen und den MBR nach einem Neustart zu manipulieren. ESET Research meldete am Mittwochabend auf Twitter, dass der Zeitstempel für die Erstellung der Software auf den 28. Dezember 2021 zeige, was darauf hindeute, dass der Angriff **möglicherweise seit fast zwei Monaten vorbereitet** worden sei.

Juan-Andres Guerrero-Saade, leitender Sicherheitsforscher bei SentinelOne, schätzt gegenüber dem Portal Cyberscoop „Hermetic Wiper“ gefährlicher als die im Januar entdeckte Malware ein. Demnach verwendeten die Angreifer **mehrere redundante Methoden**, um die Systeme zu zerstören. „Das ist **viel konzertierter** als WhisperGate oder andere Wiper, die wir in letzter Zeit gesehen haben“, so der SentinelOne-Forscher.

Cyberattacken als Teil der Angriffsstrategie

Die Kombination aus DDoS-Angriffen und Malware-Infektionen entspricht nach Ansicht von Sicherheitsanalysten Russlands Strategie, Cyberoperationen mit realer Aggression zu verbinden. „**Sie werden den Krieg [mit Cyberangriffen] nicht gewinnen, aber sie könnten ihn auf jeden Fall erleichtern**", sagte **Aaron Brantly**, Professor für Politikwissenschaft mit Schwerpunkt Cybersicherheit an der staatlichen Hochschule **Virginia Tech** in den USA gegenüber der

Washington Post. „Das ganze Ziel ist es, ein günstigeres Umfeld für kinetische Konflikte zu schaffen."

Spillover-Effekte durch den Krieg befürchtet

Dass der Krieg Russlands in der Ukraine zu gezielten russischen Cyberangriffen auf die Infrastruktur in westlichen Ländern führt, ist zwar nicht auszuschließen, aber nach Meinung von Expert:innen derzeit kein realistisches Szenario. Viel wahrscheinlicher sind nach Ansicht von **Ciaran Martin**, ehemaliger Leiter des **National Cyber Security Centre** in London, sogenannte **Spillover-Effekte**, bei denen es zu Kollateralschäden durch Vernetzung kommt: „**Ein offensichtliches Risiko besteht darin, dass westliche Netzwerke ungewollt von russischen Angriffen auf die Ukraine betroffen sind.** Dies geschah bekanntermaßen im **Juni 2017**, als Unternehmen im ganzen Westen von **NotPetya** betroffen waren und dadurch große wirtschaftliche Verluste erlitten".

Deutlich ist aber auch, dass der derzeitige **russische Angriff mit Truppen, Luftangriffen und Raketen** die Lebenswirklichkeit der Menschen in der Ukraine **unmittelbarer betrifft als flankierende Cyberangriffe**. Auf die Frage der Nachrichtenagentur AP, ob die Denial-of-Service-Angriffe auch am Donnerstagmorgen noch andauerten, antwortete der hochrangige ukrainische Cyberverteidungsbeamte **Victor Zhora** zunächst nicht und meldete sich dann per SMS: „Ist das Ihr Ernst?", schrieb er. „Es gibt hier ballistische Raketen".

Nachgefragt

RUSSLAND-UKRAINE-KONFLIKT

„Die Angriffsmethoden passen ins

Gesamtbild“

Thomas Reinhold, Wissenschaftlicher Mitarbeiter am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der TU Darmstadt, forscht zur Militarisierung im Cyberspace und Fragen der Abrüstung und Rüstung in dieser Domäne. Im Interview erklärt er die Hintergründe zur russischen Aggression im Cyberraum.

Thomas Reinhold

In den vergangenen Wochen hat es immer wieder Attacken auf die ukrainische digitale Infrastruktur gegeben. Welche Rolle haben die zuletzt erfolgten DDoS-Angriffe im Vorfeld der russischen Invasion gespielt?

Zum einen muss festgehalten werden, dass ein Schutz vor DDoS-Angriffen aufgrund der technischen Beschaffenheit schwer großflächig umzusetzen ist. Man kann mit bestimmten Technologien einzelne kritische Systeme absichern, aber nicht etwa die gesamte kritische Infrastruktur eines Landes. Es ist also leider relativ leicht – quasi wie bei digitalem Vandalismus – irgendwelche Systeme per DDoS lahmzulegen, da Angreifer fast in jedem Fall verwundbare Ziele finden werden. In diesem Sinne sind die DDoS-Angriffe, die wir beobachten konnten, leider ein sehr wirksames Mittel, um zum einen Verunsicherung und Unruhe zu stiften. Gerade angesichts des Informationsbedarfes der Menschen in der Ukraine wurde Ihnen gleichzeitig aber auch ein wichtiger Informationszugang genommen, indem wichtige Webseiten nicht erreichbar waren. Denkbar ist außerdem, dass mit Hilfe des Chaos, die solche DDoS-Attacken auslösen und der Ressourcen, die sie binden, auch andere Cyberoperationen verdeckt werden sollen, die sich gezielt gegen relevante militärische oder zivile Systeme gerichtet haben.

Verschiedene IT-Sicherheitsunternehmen haben Malware-Aktivität in der Ukraine beobachtet. Wie schätzen Sie diese

Analysen ein?

Ich halte diese Analyse für glaubhaft und stichhaltig, auch wenn bei es Cyberattacken natürlich immer einer umfangreichen und zeitlich aufwendigen Analyse bedarf, um die Herkunft der Schadsoftware zu attribuieren. In jedem Fall kann man davon ausgehen, dass die Hintertüren, die für die Infektion der betroffenen Systeme und die Aktivierung der Malware benutzt wurden schon seit längerem vorbereitet worden sind. Der für die Angriffe eingesetzte Wiper ist leider ein sehr effektives Mittel, um Computersysteme schnell zu zerstören und eine rasche Reaktivierung zu unterbinden. Es ist allerdings auch kein besonders subtiles Mittel, sondern sozusagen der Holzhammer.

Sehen Sie einen Zusammenhang zwischen der Entdeckung der Malware und den DDoS-Attacken etwa am Mittwoch?

Davon ist auszugehen. Beide Angriffsmethoden passen gut ins Gesamtbild. Mit Hilfe der Malware-Angriffe wurden Systeme lahmgelegt, von denen man ausgehen musste, dass sie gut geschützt waren und DDoS-Angriffen vielleicht sogar standgehalten hätten. Diese Systeme wurden höchstwahrscheinlich lange im Vorfeld infiltriert und die „digitale Bomben“ nun aktiviert. Die DDoS-Attacken, die technisch relativ simpel umzusetzen sind, wurden für die großflächigen Schäden, die schnelle und effektive Unterdrückung der Informationslage und möglicherweise sogar den militärischen zeitlichen Vorteil eingesetzt.

Erwarten Sie, dass der Konflikt auch die europäische und deutsche Wirtschaft im Cyberraum treffen wird, wie etwa im Fall von NotPetya im Jahr 2017?

Ich gehe davon aus, dass es im aktuellen offenen Krieg keine direkten Cyberangriffe durch offizielle russische Akteure wie Nachrichtendienste oder Militärs gegen die europäische beziehungsweise deutsche Wirtschaft geben wird. Dies könnte ganz am Ende auch dazu führen, dass Artikel 5 der NATO-Charta ausgelöst wird. Gleichwohl könnten sich angesichts der Narrative, die Putin aktuell verbreitet, „patriotische

Hacker“ dazu berufen fühlen, hier zu agieren. Und selbstverständlich beinhalten Malware-Angriffe immer auch die Gefahr, dass sich die Schadsoftware versehentlich ausbreitet. Mittelfristig betrachtet sollte es uns aber auch Sorgen machen, dass Cyberattacken zunehmend als probates Mittel für die Durchsetzung politischer Interessen eingesetzt werden. Bisher hatten wir dies vorwiegend auf der Ebene der nachrichtendienstlichen Informationsgewinnung beobachtet, die alle Staaten mehr oder minder dulden. Aber mit einem staatlichen Akteur, der seine Missachtung internationaler Regeln gerade dermaßen demonstriert, könnte sich auch hier die scheinbare Gewissheit, dass der Cyberspace ein ziviler Raum ist, den es im Interesse aller Menschen zu schützen gilt, in Luft auflösen.

Die Fragen stellte Johannes Steger

Standpunkt

IT-SICHERHEITSGESETZ 2.0

IT-Sicherheitsrecht nach IT-SiG 2.0-Novelle: Immer noch unpräzise

Lutz Martin Keppeler, Fachanwalt für IT-Recht bei Heuking Kühn Lüer Wojtek

Zu vage, wenig praxistauglich und viele bürokratische Pflichten, die dann doch eine politische Lösung erforderlich machen: Auch nach der IT-Sig 2.0-Novelle gibt es noch zahlreiche regulative Baustellen im deutschen IT-Sicherheitsrecht, sagt Fachanwalt Lutz Martin Keppeler.

Stellt man sich einen Rechtshistoriker vor, der in einigen Jahrzehnten auf das aktuelle IT-Sicherheitsrecht zurückschaut, wird er vermutlich zu dem Schluss gelangen, dass die IT-Sicherheit im Jahr 2021/22 noch kein „rechtliches“ Thema war.

Der Grund ist simpel: **Der Gesetzgeber hat es sich zu einfach gemacht.** Es mangelt an konkreten Angaben, an detaillierten Vorgaben. Gerichte mussten sich bislang kaum mit der Materie befassen und konnten die **vagen Regelungen** des Gesetzgebers nicht in praxistaugliche konkrete Fallgruppen fassen. Gerade Betreiber von kritischer Infrastruktur, die sich täglich mit dem BSIG und dem neuen IT-Sicherheitsgesetz 2.0 („IT-Sig 2.0)“ befassen, sehen sich mit losen Formulierungen konfrontiert, die viel Interpretationsspielraum übriglassen.

Nun liegt die Untätigkeit nicht an kollektiver Unlust im zuständigen Innenministerium. Der Hintergrund ist komplexer: Die Informationstechnik und alle mit ihr eng verknüpften Bereiche befinden sich im stetigen Wandel, sodass die Gesetzgebung fürchtet, mit aktuellen Regelungen kaum hinterherzukommen. Die **Notlösung**: Man hofft auf die Rechtsprechung, die dann Präzedenzfälle schaffen soll – doch dazu ist es bisher nicht gekommen. Man hofft auch auf branchenspezifische Sicherheitskataloge, die jedoch in vielen Fällen auf einen Verweis auf ein ISMS nach **ISO 27001** hinauslaufen.

Kleine Schritte nach vorne

Gut ist, dass der Gesetzgeber sich im IT-Sicherheitsgesetz 2.0 zumindest ein paar kleine Schritte hervorgewagt hat und die Regelungen etwas konkretisiert hat. Nun heißt es nicht mehr nur, dass Systembetreiber für „angemessene Sicherheit“ sorgen müssen, sondern dass es **„Systeme zur Angriffserkennung“** geben muss. Das ist – im Vergleich zu vorher – eine erhebliche Präzisierung.

Detaillierter wird es im Gesetzestext allerdings nicht. Es stellt sich daher nach wie vor die Frage, wieso nicht weitere Vorgaben mit ähnlichem Abstraktheitsgrad in den Gesetzestext aufgenommen

wurden. Der Gesetzgeber könnte etwa regeln, dass **Systeme der kritischen Infrastruktur segmentiert und abgeschlossen von anderen Systemen** sein müssen. Ferner ließe sich auch detailliert regeln, wie abgeschottet das System sein muss und welche (Mindest-)Voraussetzungen für Systeme zur Angriffserkennung gelten. Ähnliche Beispiele würden sich noch viele finden lassen.

Die Bürokratie der Meldepflicht für kritische Komponenten

Ein weiterer Punkt, der irritiert, ist die **politische Entscheidung zur Meldung kritischer Komponenten**. Nach dem neuen Gesetz müssen Betreiber kritischer Infrastruktur dem Innenministerium darlegen, welche Komponenten, die kritisch sind, sie in ihren **5G-Systemen** verwenden. Der Hintergrund dieser Regelung ist klar: Die Politik möchte einen Überblick darüber haben, an welchen Stellen Komponenten des chinesischen Herstellers **Huawei** verbaut sind.

Unabhängig von der politischen Entscheidung, es Huawei (und vergleichbaren Anbietern) schwer zu machen, ist die Art und Weise, wie die Politik an diese Überlegung herantritt, fragwürdig. Ein Beispiel: Der Betreiber eines **Campusnetzwerks**, sei es universitär oder unternehmerisch, muss nun eine Vielzahl an Komponenten an das Innenministerium melden, bei denen die Sicherheitsforschung keinerlei Bedenken hat.

Zugleich muss eine **Garantieerklärung** vorliegen, aus der hervorgeht, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Missbrauchsmöglichkeiten zum Zwecke von **Sabotage, Spionage oder Terrorismus** verfügt. Dies muss der Betreiber nun bei allen möglichen Herstellern nachfragen, dessen Komponenten im Campus verbaut sind – auch wenn man schon seit Jahrzehnten Kunde ist und es nie zu Problemen gekommen ist.

Nun kann das Innenministerium untersagen, mit Herstellern bestimmter Komponenten Geschäfte zu machen, wenn das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) ein Problem darin sieht: Hier kommt es wieder zur politischen

Entscheidung. Unterm Strich werden also zahlreiche Sachverhalte gesammelt und große Mengen an Bestandteilen im gesamten System gemeldet, damit am Ende doch Politiker im Ministerium über die Verwendung entscheiden können. Man kann sagen: Es ist ein **reines Herauszögern der Entscheidung**, ob man nun Huawei-Komponenten in die Systeme einbinden darf, oder nicht.

Starke Eingriffsrechte durch legales Hacking

Ein weiterer Kritikpunkt am neuen BSI-Gesetz, sind die Paragrafen 7b und 7c. Sie behandeln die „Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden“ sowie „Anordnungen des Bundesamtes gegenüber Diensteanbietern“. Das BSI erhält **neue, weitreichendere Kompetenzen** bei der Untersuchung von Netzwerken und Systeme.

Insbesondere kann das BSI nun zur „Detektion von Angriffsmethoden“ auch aktive Verfahren nutzen: Man täuscht einem Cyberangreifer vor, dass der Angriff erfolgreich war, um ihn besser untersuchen zu können – in der Fachsprache spricht man vom „Honeypot“, dem Honigtopf. Auch darf das BSI nun die Systeme mit sogenannten **Portscans** nach unsicheren Passwörtern durchsuchen – was eigentlich eine Hacking-Straftat ist. Auch das offensive Hacking in Form von Honeypots ist ein Verstoß gegen das Fernmeldegesetz – und damit eigentlich grundgesetzwidrig.

IT-Sicherheitssiegel für smarte Produkte

Positiv zu beurteilen ist die Einführung des **IT-Sicherheitskennzeichens** in Deutschland. Die Idee dahinter ist, dass ein Unternehmen mit dem Kennzeichen seinen Kunden ein Versprechen gibt; etwa, dass ein Produkt fünf Jahre lang regelmäßige Updates bekommt oder dass ein vollautomatisches System mitprogrammiert wurde, das Angriffe auf das Produkt erkennt. Das BSI vergibt nach Prüfung dieses Siegel, welches Unternehmen für alle denkbaren „smarten“ Produkte beantragen können, seien es intelligente Rasenmäher, Kühlschränke mit WLAN-Funktion oder

Autos. In der Praxis lässt sich an diesem Kennzeichen vom Verbraucher mittels eines QR-Codes überprüfen, welche Versprechen das Unternehmen anbietet und ob sie noch aktuell sind.

Für Unternehmen ist das eine große Chance: Sie können sich mit aktuell gehaltenen und sinnvoll gestalteten Siegeln gegenüber Wettbewerbern, die auf das Siegel verzichten, einen Vorteil erarbeiten. In der Praxis lässt sich ein solches Siegel zukünftig werbewirksam platzieren – wie man es bereits von vielen anderen Siegeln, zum Beispiel in der Lebensmittelbranche, kennt.

Allerdings sollten Unternehmen zwingend darauf achten, ihre Siegel aktuell zu halten, da ein Siegel mit falschen oder veralteten Informationen schnell zum Ausschlusskriterium für den Produktkauf wird. Da aufgrund einer Gesetzesänderung im BGB ohnehin für **jedes digitale Consumer-Produkt** eine Aktualisierungspflicht besteht (die auch Sicherheitsupdates erfasst) müssen im Übrigen ab 01.01.2022 ohnehin Sicherheitsupdates bereitgestellt werden: Warum dann nicht „zwei Fliegen mit einer Klappe schlagen“ und die notwendig zu erfüllende Pflicht nach außen mit einem IT-Sicherheitskennzeichens garnieren.

Lutz Martin Keppeler ist Fachanwalt für IT-Recht und Salaried Partner bei der Sozietät Heuking Kühn Lüer Wojtek. Er ist außerdem Mitautor von „Die Weiterentwicklung des IT-Sicherheitsgesetzes – Kommentar zum IT-Sicherheitsgesetz 2.0“.

Abgehört – die Serie

PODCAST

Digitale Rohrpost aus dem BMI

Es gibt viele Podcasts, die sich mit Cybersicherheit beschäftigen. Aber welche sind gut? Welche nicht? Welche sind unterhaltsam

und bei welchen lernt man viel? Wir haben für Sie reingehört. Folge 2 unser Serie über Podcasts: Digitale Rohrpost aus dem BMI.

Selina Bettendorf

Der Podcast-Boom macht auch vor dem Innenministerium nicht Halt. Seit 2020 hat **Staatssekretär Markus Richter** mit der „Rohrpost“ seinen eigenen Podcast, in dem er jeden Monat über aktuelle Nachrichten rund um die Digitalisierung des Staates informiert. Richter ist als Beauftragter der Bundesregierung für Informationstechnik (**Bundes-CIO**) auch für das Thema Cybersicherheit zuständig.

Der Cybersicherheit ist eine eigene Folge gewidmet. In Folge acht interviewt ein Moderator des BMI Markus Richter und die renommierte **israelische IT-Sicherheitsforscherin Haya Shulman**. Sie philosophieren darüber, ob man Kriminelle mit kriminellen Methoden bekämpfen darf und wie die Meinungen zu Hackbacks und offenen Sicherheitslücken sind. Shulman kritisiert, dass die Wissenschaft nicht genug in den Cybersicherheitsrat eingebunden sei und es auch beim Entwurf der Cybersicherheitsstrategie nicht gewesen sei. Überhaupt **die Cybersicherheitsstrategie**. Die enthalte eigentlich alle wichtigen Themen und Deutschland sei gut aufgestellt, sagt Shulman. Aber Länder wie die USA, Frankreich und Israel würden in der Cyberintelligence zeigen, was man noch besser machen könne.

Klarheit schaffen durch Verfassungsänderung?

Richter weist darauf hin, dass viele der in Cybersicherheitsstrategie formulierten Ziele erst jetzt in der neuen Legislaturperiode mit neuen Maßnahmenkatalogen umgesetzt werden können. Natürlich auch mit Einbindung der Wissenschaft. **Für die Umsetzung der Strategie sei es auch legitim, die Verfassung zu ändern.** „Wir wollen Klarheit schaffen“, sagt er. So soll damit die Kompetenz auf Bundesebene zur Gefahrenabwehr gegeben und die Zentralstellenfunktion des BSI gestärkt werden.

Der Podcast des BMI ist schwer zu vergleichen mit Studioproduktionen wie „Der Mann in Merkels Rechner“. **Es fehlen Einblendungen, Musik, Spannungsaufbau, kritische Nachfragen des Moderators**. Was bleibt, ist aber ein informatives Gespräch zwischen **hochrangigen Expert:innen** über die politische Dimension von Cybersicherheit. Mit einem Verhältnis von 1:3 ist die Frauenquote auch besser, als sie sonst im Cybersicherheitsbereich ist.

Zielgruppe: Von 👱 bis 👱🎓

Spannung: 🔥

Lernfaktor: 🧠🧠

Beste Stelle: „Die Schwelle für Angriffe im Internet ist niedriger, als in der realen Welt. Es ist nicht das gleiche, ob man digital oder physisch in eine Organisation einbricht. Für Cyberangriffe braucht man keine Sprengstoffe oder physische Werkzeuge, man muss auch nicht weit fahren. Man braucht nicht mehr als Expertise oder Geld, um jemanden im Darknet für Angriffe zu beauftragen.“ (Shulman bei etwa 3:48)

Länge: 43:40 Minuten

Link zum Podcast

Nachrichten

Faeser warnt erneut vor Cyberangriffen

Bundesinnenministerin **Nancy Faeser** (SPD) hat abermals vor einer erhöhten Gefahr von Cyberangriffen in Deutschland gewarnt. „Wir wissen, dass Cyberangriffe mittlerweile **ein häufiges Mittel in Konfliktsituationen** sind, wir gehen daher auch für deutsche Stellen von einer erhöhten Gefahr für Cyberangriffe aus“, sagte sie am

gestrigen Nachmittag. **Konkrete Hinweise auf Cyberangriffe gegen deutsche Stellen** lägen allerdings noch nicht vor. Ein für den Nachmittag angesetzter Termin beim **Bundesamt für Sicherheit in der Informationstechnik** (BSI) war gestern aufgrund der russischen Invasion in der Ukraine kurzfristig abgesagt worden. Alle Beobachtungen liefen derzeit im Nationalen Cyberabwehrzentrum zusammen, erklärte Faeser. Dort werde die weitere Entwicklung „sehr eng verfolgt".

Auch die russischen Aktivitäten in den sozialen Medien beobachtet das Innenministerium derzeit mit Sorge. Man nehme war, „dass die **russische Propaganda und Desinformation** im Zuge des Ukraine-Konfliktes deutlich zunimmt", erklärte Faeser. Dies werde in nächster Zeit voraussichtlich noch zunehmen. Die Bundesinnenministerin bat insbesondere **Betreiber Kritischer Infrastrukturen**, „ihre IT-Sicherheitsmaßnahmen hochzufahren". Dies gelte auch für **Unternehmen mit Bezug zur Ukraine**, sagte sie.

Laut dem IT-Branchenverband **Bitkom** unterhalten viele Unternehmen der Tech-Branche Beziehungen in die Ukraine und beschäftigen ukrainische IT-Freelancer. Laut dem Verband importieren vier Prozent der deutschen IT-Unternehmen Güter aus Russland – vorrangig Software-Produkte. **27 Prozent der deutschen Unternehmen exportieren digitale Technologien oder Leistungen nach Russland**, so der Verband in einer Unternehmensbefragung aus dem Jahr 2021. Deutschland, die EU sowie die G7-Staaten haben am gestrigen Abend bereits umfangreiche Wirtschaftssanktionen angekündigt, zu denen auch **Exportbeschränkungen von High-Tech-Produkten** zählen sollen. *prd*

Lloyds rechnet mit russischen Cyberattacken

Die britische Großbank **Lloyds** bereitet sich auf mögliche russische Cyberattacken als Vergeltung für Sanktionen im Finanzsektor vor. Das sagte **Lloyds-Chef Charlie Nunn** am Donnerstag bei der Vorstellung der Jahreszahlen des Kreditinstituts. Es habe Gespräche des Bankensektors mit der Regierung über mögliche Angriffe durch russische Hacker:innen gegeben, so Nunn. Seine Bank habe in den vergangenen fünf Jahren erheblich in die Cybersicherheit investiert. Angesichts des **russischen Einmarschs in die Ukraine** wird mit deutlichen britischen Sanktionen auch im Finanzsektor gegen Moskau gerechnet. *dpa*

USA warnt vor neuer Malware aus Russland

US-amerikanische und britische Behörden haben in einem am Mittwoch veröffentlichten Bericht vor einer neuen **Malware-Variante** gewarnt, die seit 2019 eingesetzt wird.

Das britische **Nationale Zentrum für Cybersicherheit** (NCSC), die US-amerikanische **Agentur für Cybersicherheit und Infrastruktursicherheit** (CISA), die **Agentur für Nationale Sicherheit** (NSA) und die Bundespolizei (FBI) haben festgestellt, dass der als **Sandworm** oder Voodoo Bear bekannte Akteur eine neue Malware verwendet, die in der entsprechenden Mitteilung als Cyclops Blink bezeichnen. Die Behörden hatten Sandworm in der Vergangenheit dem Leitungsorgan des **russischen Militärnachrichtendienstes** (GRU) zugeschrieben.

Laut Erkenntnissen der Behörden soll Sandworm etwa für die Störung des ukrainischen Stromnetzes im Jahr 2015, **NotPetya** 2017 oder Angriffe auf die Olympischen Winterspiele und Paralympics im Jahr 2018 verantwortlich sein. Die Behörden gehen davon aus, dass die neue Malware entwickelt wurde, um ein früheres Botnetz zu ersetzen. *jos*

Fertigungsindustrie Top-Ziel von Ransomware

Die **Fertigungsindustrie** gehört mit weltweit 23 Prozent aller Angriffe zu den am stärksten betroffenen Branchen, die von Cyberkriminellen angegriffen werden. Das ist das Ergebnis des jährlichen „X-Force Threat Intelligence Index“, den IBM Security in dieser Woche veröffentlichte. Bisher war die **Finanzdienstleistungs- und Versicherungsindustrie** das Top-Ziel von Ransomewareattacken, für das Jahr 2021 fällt sie auf den zweiten Platz.

Der 59-seitige Report fasst Trends und Angriffsmuster zusammen, die IBM Security beobachtet und analysiert hat. Laut IBM setzten Angreifer darauf, dass Störungen bei Fertigungsunternehmen auf ihre **nachgelagerten Lieferketten** einen stark wirtschaftsschädlichen Dominoeffekt haben, um Firmen zur Zahlung des Lösegelds zu zwingen. **Charles Henderson**, Leiter von IBM X-Force, weist in diesem Zusammenhang auf die Wichtigkeit von Sicherheitskonzepten bei Unternehmen hin: „Die Angriffsfläche wird immer größer. Anstatt also davon auszugehen, dass alle Schwachstellen in ihrer Umgebung gepatcht sind, sollten Unternehmen davon ausgehen, dass sie kompromittiert sind, und ihr Schwachstellenmanagement mit einer Zero-Trust-Strategie verbessern.“

In dem Report bemerkt IBM X-Force weiterhin, dass **einer von vier Angriffen**, die sie 2021 weltweit beobachteten, **in Asien** stattfand. Damit gab es dort im vergangenen Jahr **mehr Cyberangriffe als in jeder anderen Region**. Als neuen Trend macht der Report das sogenannte **Vishing** (Voice Phishing), also den durch Telefonanrufe unterstützten Phishing-Angriff aus: Bei den Penetrationstests **verdreifachte sich die Klickrate in den Phishing-Kampagnen**, wenn diese mit Telefonanrufen kombiniert wurde. *johl*

Fotohinweise
(Lutz Martin Keppeler)

Der Tagesspiegel Background Cybersecurity erscheint täglich als E-Mail-Briefing um 6 Uhr. Alle Artikel und weitere Entscheider-Briefings finden Sie auf unserem Portal unter background.tagesspiegel.de.
- IMPRESSUM -
Verlag Der Tagesspiegel GmbH, Askanischer Platz 3, 10963 Berlin
Geschäftsführer: Gabriel Grabner, Ulrike Teschke
Chefredakteure, v.i.S. von § 18 Abs. 2 MStV: Lorenz Maroldt, Christian Tretbar
AG Charlottenburg HRB 43850, UID: DE 151725755, Fax: (030) 29021-599
Redaktion: Selina Bettendorf, Paul Dalg, Jens Ohlig, Johannes Steger (Leitung)
Fragen zu redaktionellen Inhalten, zum Datenschutz & technischen Problemen: background.cybersecurity@tagesspiegel.de
Fragen zu Anzeigen: anzeigen@tagesspiegel.de
Fragen zum Abonnement: background.service@tagesspiegel.de
DATENSCHUTZ | KONTAKT | IMPRESSUM

Verlag Der Tagesspiegel GmbH
Askanischer Platz 3, 10963 Berlin
Geschäftsführung: Gabriel Grabner, Ulrike Teschke
Amtsgericht Charlottenburg HRB 43850 B
