73. Jahrgang, 22–24/2023, 30. Mai 2023

bpb:

AUS POLITIK UND ZEITGESCHICHTE

Cybersicherheit

Eva Wolfangel
HASE UND IGEL IM DARKNET

Gerhard Schabhüser
„DIE GEFÄHRDUNGSLAGE IST SO HOCH WIE NIE ZUVOR"

Sven Herpig
„WIR BRAUCHEN EINEN NOTFALLPLAN"

Lennart Maschmeyer
WUNDERWAFFEN UND WIRKLICHKEIT

Matthias Schulze
SICHERHEITSLOGIK DER CYBERDOMÄNE

Christian Stöcker
KLEINE GESCHICHTE DER HACKERKULTUR

APuZ
ZEITSCHRIFT DER BUNDESZENTRALE FÜR POLITISCHE BILDUNG
Beilage zur Wochenzeitung Das **Parlament**

Der APuZ-Podcast
bpb.de/apuz-podcast

Cybersicherheit
APuZ 22–24/2023

EVA WOLFANGEL
HASE UND IGEL IM DARKNET
Moderne Cybercrime-Banden sind gut organisiert. Ein Blick in die Geschichte der Viren und Würmer zeigt eine logische Entwicklung und Eskalation krimineller Aktivitäten im Netz – und auch, wieso Behörden oft das Nachsehen hatten. Doch eventuell ändert sich gerade etwas.
Seite 04–09

GERHARD SCHABHÜSER
„DIE GEFÄHRDUNGSLAGE IST SO HOCH WIE NIE ZUVOR"
Wie lässt sich die IT-Sicherheit in Deutschland verbessern? Ein Gespräch mit dem Vizepräsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die aktuelle Cybersicherheitslage, Künstliche Intelligenz und den IT-Fachkräftemangel.
Seite 10–13

SVEN HERPIG
„WIR BRAUCHEN EINEN NOTFALLPLAN"
Entspricht die deutsche Cybersicherheitsarchitektur noch den heutigen Anforderungen? Ein Gespräch mit dem Leiter für Cybersicherheitspolitik und Resilienz der Stiftung Neue Verantwortung (SNV) über deutsche Cybersicherheitspolitik.
Seite 14–17

LENNART MASCHMEYER
WUNDERWAFFEN UND WIRKLICHKEIT
Seit 2014 ist die Ukraine Angriffsziel russischer hybrider Kriegsführung einschließlich Cyberoperationen. Das Land gilt als Testlabor für Russlands Cyberwaffen. Schaut man sich die Operationen jedoch genauer an, offenbart sich ihre begrenzte strategische Wirkung.
Seite 18–22

MATTHIAS SCHULZE
SICHERHEITSLOGIK DER CYBERDOMÄNE
Der globale Cyberraum stellt eine völlig neue strategische Umwelt zwischenstaatlicher Machtausübung dar, in der die alten Paradigmen der konventionellen Domäne nicht mehr gelten. Die Charakteristika des Cyberspace erfordern ein neues strategisches Denken.
Seite 23–29

CHRISTIAN STÖCKER
KLEINE GESCHICHTE DER HACKERKULTUR
Ende der 1950er Jahre entstand am Massachusetts Institute of Technology eine neue Form der Auseinandersetzung mit digitaler Technik: spielerisch, meritokratisch, gelegentlich anarchisch und auf radikale Transparenz bedacht. Diese Hackerkultur ist bis heute lebendig.
Seite 30–37

EDITORIAL

Schulen, Krankenhäuser, Unternehmen, Behörden – kaum ein Bereich ist vor Cyberangriffen wie Datendiebstahl, Erpressung und Wirtschaftsspionage sicher. Auch IT-Dienstleister, die eigentlich gegen solche Angriffe gewappnet sein sollten, werden zu Opfern. Das Problembewusstsein in Politik und Gesellschaft ist zwar geschärft, aber noch immer gibt es zu viele Schwachstellen in den Systemen. So bezeichnet das Bundesamt für Sicherheit in der Informationstechnik in seinem Lagebericht 2022 die Bedrohungslage in Deutschland als „so hoch wie nie". Dies hänge auch mit dem russischen Angriffskrieg gegen die Ukraine zusammen.

Seit 2014 greifen russische Hacker als Teil einer hybriden Kriegsführung die Ukraine verstärkt an. So kam es im Dezember 2015 im Westen des Landes zum weltweit ersten Stromausfall, der durch einen Hackerangriff verursacht wurde. Mit der militärischen Invasion in das gesamte Territorium der Ukraine im Februar 2022 intensivierte Russland seine Cyberangriffe – nach ukrainischen Angaben waren es allein im Jahr 2022 über 2000.

Die Fragen zur Cybersicherheit in Deutschland sind vielfältig: Welche Strategien führen zu mehr IT-Sicherheit? Welche Reformen sind notwendig, um die deutsche Cybersicherheitsarchitektur zu stärken? Wie soll auf den IT-Fachkräftemangel reagiert werden? Und welche Risiken und Chancen birgt Künstliche Intelligenz für die Cybersicherheit? Bei der Beantwortung dieser Fragen sind sich die Bundesregierung und Vertreterinnen und Vertreter aus Wissenschaft und Zivilgesellschaft nicht immer einig – Cybersicherheit ist nicht nur eine technische, sondern auch eine politische Herausforderung.

Lorenz Abu Ayyash

HASE UND IGEL IM DARKNET

Computerwürmer, kriminelle Banden und ihre Widersacher

Eva Wolfangel

Ein Besuch bei der Polizeidirektion Esslingen kann sich anfühlen wie eine Zeitenwende. Nicht wegen des altmodischen Backsteinbaus, nicht wegen des mittelalterliche Flairs der Altstadt des kleinen schwäbischen Städtchens, nicht wegen der aus Filmen bekannten Schleuse im Eingang eines Präsidiums, in dem Kleinkriminelle ausnüchtern ebenso wie Kommissare Spuren auswerten. Sondern wegen der neuartigen Herangehensweise an Cyberkriminalität. Die Zeitenwende verkörpern in diesem Fall Kriminalhauptkommissar Daniel Lorch und sein Team. Es steht eine Frage im Raum: Wie kann es sein, dass das FBI neuerdings auf die Hilfe der Esslinger Einheit schwört?

Lorch ist Leiter der Ermittlungsgruppe Dawnbreaker – eine internationale Kooperation, der im Februar 2023 ein Schlag gegen eine der gefährlichsten und am schnellsten wachsenden Ransomware-Gruppen gelungen war. Ransomware ist Schadsoftware, die Dateien verschlüsselt, um Lösegeld für deren Freischaltung zu verlangen. Die Gruppe Hive hatte zuvor tausende Unternehmen verschlüsselt und es insbesondere auf kritische Infrastrukturen abgesehen. Dabei seien auch Krankenhäuser in Brasilien getroffen worden, die lebenswichtige Operationen unterbrechen mussten und über Wochen nicht arbeiten konnten. Patienten seien gestorben, sagt Lorch im Gespräch mit der Autorin.

„Das muss aufhören!“, ruft der Kommissar bei solchen Gelegenheiten dann energisch, „wir müssen das Leiden stoppen!“ Mit dieser Energie verfolgt der Ermittler seine Arbeit – und vermutlich sind es diese Energie und der damit verbundene Aufwand, die zum Erfolg solcher Operationen beitragen. Den Behörden aus zahlreichen Ländern gelang schließlich der *take down* hunderter Websites im Darknet sowie die Beschlagnahmung eines Großteils der Infrastruktur der Ransomware-Gruppe, unter anderem 15 Server in den USA und den Niederlanden. Seither prangt das Logo des Polizeipräsidiums Reutlingen direkt unter dem des FBI und des Secret Service auf den beschlagnahmten Websites im Darknet.

Die Gruppe sei „sehr gefährlich“, habe das BKA den Esslinger Ermittler:innen gesagt, als es Anfang 2022 bat, die bundesweiten Ermittlungen zu bündeln. Das war Zufall: Das Team ermittelte damals im Falle des ersten baden-württembergischen Opfers und hatte offenbar einen exklusiven Zugang gefunden. Bis heute gibt es mehr als 70 deutsche Opfer, weltweit 1500, mehr als 100 Millionen Euro Lösegeld hat die Gruppe erpresst.

An Lorchs Wand hängt eine Grafik. Ein Blatt A3-Papier, und was darauf ist, sieht aus wie ein Spinnennetz, an das immer wieder angebaut wurde. Es hat viele mehr oder weniger zentrale Punkte, an denen sich die Linien kreuzen und hunderte kleiner Verästelungen an den Rändern, aus denen manchmal neue Zentren wachsen und manchmal lose Enden ragen. Es sind die Server und Knotenpunkte einer Ransomware-Gruppe, die Architektur einer wohl geplanten kriminellen Operation. Lorch zeigt auf einen Punkt. „Wenn du hier landest, weißt du erstmal gar nicht, wo du bist.“ Wenn Lorch und seine Kolleg:innen einen solchen Server gehackt haben, schauen sie sich dort möglichst unauffällig um und versuchen herauszubekommen, wie dieser mit anderen zusammenhängt. Das ist extrem aufwendig. Aber Lorch gibt nicht auf. Er löchert die Forensiker im Nachbarbüro: „Was macht das Ding? Mit wem baut es Verbindungen auf? Woher kommt es?“ – und gibt zu: „Unsere Forensiker kriegen dann immer erst mal die heilige Krise.“

Die gesamte Architektur des Netzwerkes herauszubekommen von Computern in Esslingen, Tampa oder Amsterdam aus, mit unzähligen kleinen Erfolgen auf zig Servern – das verlangt Geduld und Ausdauer. Immer wenn sie einen Schritt weiterkamen, nach und nach Zugriff auf die Kommunikation der weltweit agierenden Ransomware-Bande erlangten, die gesamte Buchhaltung der Gruppe oder die Pläne für künftige Angriffe mitlesen konnten, war der Feierabend zweit-

rangig. „Das verursacht so viel Leid", sagt Lorch. Unzählige Male ist er nachts oder am Wochenende zu betroffenen Unternehmen ausgerückt, in der Hoffnung, noch etwas retten zu können oder eine entscheidende Spur zu finden.

Das Entsetzen über Cyberangriffe ist nicht neu – das begleitet die Behörden seit dem ersten Computerwurm. Was die Zeitenwende auszeichnet, ist die Entschlossenheit und die Zuversicht, dass es möglich ist, die Kriminellen zu stoppen. Wer Lorch zuhört, hört einen „Wir können das schaffen!"-Tonfall in jedem zweiten Satz. Das ist selten – häufig hört man von Behörden eher die Klage, wie schwierig alles sei und dass die Kriminellen so gut organisiert seien, dass man ohnehin keine Chance habe.

PROFESSIONALISIERUNG UND SPEZIALISIERUNG

Im Bereich des Cybercrime stehen wir gerade vor einer Situation, in der wir mit zwei Arten von Angreifer:innen konfrontiert sind: Auf der einen Seite stehen top organisierte Gruppen, die mit maßgeschneiderten Angriffen und viel Ausdauer Unternehmen und Institutionen angreifen. Und auf der anderen Seite steht eine große Menge kleinkrimineller, häufig jugendlicher Hacker:innen, die meist automatisiert bekannte Sicherheitslücken ausnutzen – und auch mit diesen „Angriffen von der Stange" ist noch viel zu holen. Hier ist die schiere Zahl der Angriffe die Herausforderung, während es bei den organisierten Gruppen die Schwere ist.

Diese Dynamik ergibt sich aus der Geschichte der Computerwürmer: Denn auch wenn es erste Viren und Würmer schon in den 1980er Jahren gab, die sich damals über Disketten verbreiteten, waren dies meist harmlose, wenn auch nervige, Spielereien. Mit dem Aufkommen des World Wide Webs wurde die Möglichkeit, andere Computer in großem Stil zu infizieren und deren Nutzer:innen zu schaden, auch für Kriminelle interessant. Seither gibt es kriminelle Unternehmer:innen, die ein untrügliches Gespür für Sicherheitslücken haben und dafür, wie sie diese ausnutzen können und ihr Wissen zu Geld machen.

Die Geschichte dieser Professionalisierung ist verknüpft mit einem Namen: Jewgeni Bogatschew. Der russische Kriminelle hat nicht nur einen der ersten Computerviren entwickelt, er hat seine Schadsoftware ausgebaut zu einem massiven Botnetzwerk – und er hat das Geschäftsmodell der heutigen Ransomware-Banden begründet, in dem jeder Schritt professionalisiert wird, Schadsoftware lizenziert und Zugänge in Systeme verkauft werden. Und er wird seit mehr als zehn Jahren vom FBI gesucht – bisher erfolglos. Drei Millionen Dollar Kopfgeld hat die US-Behörde auf ihn ausgesetzt. Das ist die höchste Summe, die das FBI für Hinweise auf einen Internetkriminellen je ausgelobt hat. Auf dem Fahndungsplakat beschreibt ihn die Behörde als einen weißen Mann mit braunen Haaren, er wiege wohl etwa 80 Kilogramm und sei 1,75 Meter groß; als Geburtsdatum wird der 28. Oktober 1983 angegeben. „Er ist bekannt dafür, dass er gerne Boot fährt und mit seinem Boot zu Orten am Schwarzen Meer reist", schreibt das FBI.

Anhand der Geschichte von Jewgeni Bogatschew lässt sich die bisherige Dynamik zwischen Kriminellen und ihren Verfolger:innen beobachten: Meist waren die Kriminellen einen Schritt voraus – oder mehrere. Dabei gab es schon immer Typen wie Daniel Lorch, die fest daran glaubten, dass eine effektive Verfolgung möglich ist. Aber womöglich wurden sie in der Vergangenheit zu wenig gehört, zu wenig ernst genommen und zu wenig gefördert.

Einer der hartnäckigsten Verfolger von Jewgeni Bogatschew ist der deutsche Sicherheitsforscher Tillmann Werner. Vor Bogatschew habe es keine professionelle Cyberkriminalität gegeben, erklärt Werner. Und auch keine Computersicherheitsbranche wie heute.

Doch es gab Windows und darin etliche Sicherheitslücken, die von Kriminellen ausgenutzt wurden. Microsoft hatte noch keine Strategie, damit umzugehen, es gab keine automatischen Updates und auch kein Verfahren, wie mit Sicherheitslücken umzugehen ist. Es gab nicht nur keine Prämien für unabhängige Hacker:innen, die Schwachstellen ausfindig machten und diese dem Konzern meldeten – es gab nicht einmal einen Kontakt, an den diese sich wenden konnten. „Wenn eine Schwachstelle gefunden wurde, konnte die ganze Welt alle Computer über das Internet angreifen", erinnert sich Werner. Und das geschah, wenn auch zunächst etwas ziellos.

KRIMINELL MIT ERFOLGSGARANTIE

Kriminelle bezahlten schnell stattliche Summen für Sicherheitslücken – und schneller als die Be-

hörden sehen konnten, entwickelte sich eine organisierte kriminelle Szene, die Windows-Sicherheitslücken systematisch ausnutzte.

Eine der ersten sichtbaren Gruppen Anfang der 2000er Jahre war das sogenannte „Russian Business Network“, eine hochprofessionelle kriminelle Gruppe, die in großem Tempo neue Geschäftsmodelle erschloss. „Wir haben das am Anfang gar nicht verstanden, was da passiert“, erinnert sich Werner. Die Gruppe betrieb damals sogar eigene Internetdienstanbieter – ein schlauer Schachzug, schließlich sind das die Strukturen, die von Behörden als erstes angegangen werden, wenn es um kriminelle Aktivitäten im Internet geht.

Die Gruppe entwickelte auch eine eigene Sprache: Es gab bereits Begriffe für kriminelle Aktivitäten im Internet, von denen die Sicherheitsforschung noch nicht einmal wusste, dass sie existieren. Werner rätselte lange, was die Werbesprüche der Gruppe bedeuten sollten: „Wir konvertieren traffic“, boten sie anderen Kriminellen an. Was soll das sein? Was für ein Verkehr wird hier umgewandelt – und in was? Schließlich ging ihm ein Licht auf: „Die haben Internetverkehr umgewandelt in Zugriff auf Systeme.“ Es war ein früher Service dessen, was sich heute immer mehr verbreitet und professionalisiert: Angriffe auf Computersysteme als Service, den andere Kriminelle buchen können.

Vor allem ein Mann stach dabei hervor: Über Slavik, wie sich Jewgeni Bogatschew im Netz nannte, war lange nichts weiter zu finden als dieses Pseudonym und unendlich viele Spuren seines cleveren Geschäftssinns. Er schien überall gleichzeitig zu sein, seine Schadsoftware Zeus fand rasante Verbreitung. Er schrieb zu einer Zeit ausgefeilte Computerviren, zu der die meisten Menschen froh waren, dank des modernen Betriebssystems Windows XP ihren Computer endlich einigermaßen intuitiv bedienen zu können. Sie hatten keine Ahnung, dass sich hinter der bunten Oberfläche überhaupt Sicherheitslücken verbergen können.

Es sind die Anfänge der Spezialisierung, die wir heute in der Cybercrime-Szene sehen: Bogatschew war Experte für ausgefeilte Banking-Trojaner. Schon in den frühen 2000er Jahren erkannte er, dass es eine Nachfrage für Schadsoftware gibt. Das ist die Geburtsstunde des Trojaners Zeus. Er entwickelte sich zu einer der beliebtesten Waffen der Cyberkriminellen, mit dem diese Bank-Zugangsdaten klauten, sich in fremde Accounts hackten und Millionen erbeuteten.

Bogatschew professionalisierte sich von da an immer mehr – und entkam seinen Verfolger:innen stets. Und er sorgte dafür, dass seine Schadsoftware funktionierte, auch dann, wenn seine Gegner:innen technische Maßnahmen gegen sie entwickelt hatten. Kriminelle, die mit ihm kooperierten, hatten quasi eine „Erfolgsgarantie.“ Dafür waren sie bereit, entsprechende Summen zu bezahlen. Der Trojaner schien unendlich anpassungsfähig – ähnlich wie die Schadsoftware der Ransomware-Gruppe Hive, die sich vor dem Schlag der internationalen Behörden-Kooperation 2023 immer wieder neu erfunden hatte. Einmal, als das FBI Hive auf die Schliche gekommen war, übertrug die Gruppe ihren gesamten Angriffscode in eine andere Programmiersprache, um nicht mehr erkannt zu werden.

Auch Bogatschews Kundschaft wurde immer professioneller, weil sich der Hacker seinen Service immer mehr kosten ließ: Er verkaufte seine Schadsoftware in Form von Lizenzen, die an einzelne Personen gebunden sind, sie war gut gemacht und gegen Piraterie geschützt. Eine Kopie kostete nach Informationen des Magazins „Wired“ mehr als 10 000 US-Dollar.[01]

War ein Computer mit Zeus infiziert, konnte er zudem schon damals in ein Botnetz eingebunden werden, also in ein Netzwerk infizierter Computer, die von einem zentralen Server gesteuert werden. Die Kriminellen konnten sie von dort quasi fernsteuern. Beispielsweise wurde über diese dann weitere Schadsoftware verschickt in Form betrügerischer E-Mails. Oder es wurden sogenannte DDoS-Angriffe (Distributed Denial of Service) ausgeführt, bei denen unzählige Computer eines solchen Netzes eine bestimmte Website aufrufen – sodass diese für niemand anderen mehr zu erreichen ist.

STORM WORM

Tillmann Werner betrachtete diese Entwicklung mit Sorge. „Eines Tages wird so ein krasser Angriff passieren, dass wir froh sein werden, wenn wir uns frühzeitig mit Botnetzen beschäftigt haben“, warnte er die Sicherheitsszene. Doch die ersten Jahre ist er auf verlorenem Posten – die Gefahr von Botnetzen wurde unterschätzt.

01 Vgl. Garrett M. Graff, 21.3.2017, www.wired.com/2017/03/russian-hacker-spy-botnet.

Im Januar 2007 jedoch wurde vielen in der Branche klar, wie groß die Gefahr ist. Innerhalb kürzester Zeit breitete sich der Computerwurm Storm Worm weltweit aus, mit einem Schwerpunkt in Europa und den USA. Er hieß deshalb so, weil er sich unter anderem mittels E-Mails verbreitete, die angeblich Neuigkeiten über Todesopfer eines verheerenden Sturms in Europa beinhalteten.

Mit der Kontrolle über einige Millionen Computer gewann das Botnetz eine enorme Rechenleistung: Es übertraf die Leistung der damals größten Supercomputer, also der stärksten Computer der Welt. Diese werden meist von staatlichen Forschungseinrichtungen betrieben, ihre Infrastruktur füllt mehrere Stockwerke aus. Der australische Informatiker Peter Gutmann merkte alarmiert an: So werde zum ersten Mal einer der stärksten Supercomputer der Welt „nicht von einer Regierung oder einem Megakonzern kontrolliert, sondern von Kriminellen." Schon das machte die neue Qualität deutlich.

Aber es kommt noch etwas dazu, was die Sicherheitsforschung damals sehr viel mehr alarmierte als die schiere Größe des Botnetzes: Die besondere neuartige Art des Angriffs. „Storm Worm war das erste ernstzunehmende Peer-to-Peer-Botnetz", sagt Tillmann Werner. In diesem Fall werden die übernommenen Computer nicht von einem zentralen Server aus gesteuert, sondern sie geben ihre Informationen nach einem ausgeklügelten System von einem zum anderen weiter, unter Peers (also Gleichgestellten), von Angegriffenem zu Angegriffenem. Das funktioniert wie eine Telefonkette nach dem Schneeballprinzip: Wenn zehn Personen eine Information haben und die an jeweils zehn andere weitergeben, lässt sich diese Telefonkette nicht stoppen, wenn eine Person daran gehindert wird zu telefonieren. Von daher lässt sich ein solches Botnetz kaum einfangen.

Nächtelang brütete Werner mit einigen Kollegen über dem Code von Storm Worm: Maschinencode, für Menschen unverständlich. Der Binärcode ist alles, was Forschenden in die Hände fällt, wenn sie eine Schadsoftware einfangen. Sogenanntes Reverse Engineering versucht dann, diesen Binärcode wieder in für Menschen verständlichen Programmiercode zurückzuübersetzen. Da es aber keine eindeutige Rückübersetzung gibt, kann es immer nur eine Annäherung sein, eine mögliche Repräsentation. Werner beschreibt es so: Man müsse rekonstruieren, welche Logik hinter einem Programm stecke. „Der heilige Gral ist, die Motivation des Entwicklers nachzuvollziehen."

Doch dann geschah etwas, was in der Anfangszeit der Computerviren häufig passierte: Der Wurm wurde plötzlich nicht weiter betrieben – er schlief gewissermaßen ein. Bis heute ist unbekannt, wer dahintersteckte. Möglicherweise war es nur eine Spielerei, die aus dem Ruder lief: Denn die ersten Autor:innen von Computerviren und -würmern hatten nicht unbedingt immer böse Absichten. Es war vielmehr eine Spielwiese für junge, meist männliche, wohlhabende Entwickler, die austesten wollten, was möglich ist. Die Möglichkeiten, die Computer anderer fernzusteuern, auf ihnen Code auszuführen oder seltsame Nachrichten zu präsentieren, faszinierte sie.

Oder es gab gar mehr oder weniger legitime Gründe: Der erste Windows-Virus namens „Brain" war 1986 von den Brüdern Basit Farooq Alvi und Amjad Farooq Alvi entwickelt worden. Diese hatten eine medizinische Software entwickelt und per Diskette vertrieben – und wollten diese gegen Raubkopien schützen. Mit auf der Diskette war der Virus, der erst dann aktiv wurde, wenn jemand eine Raubkopie anlegte. Der Virus verlangsamte Computer und verbrauchte Speicherplatz, zudem konnten die Entwickler den Standort der Computer sehen. Die Brüder hatten in ihren Code sogar eine Nachricht aufgenommen, in der ihre Namen und Adresse standen sowie der Hinweis, wie man sie erreichen könne, damit sie bei der Reparatur infizierter Rechner helfen konnten. Doch dann verbreitete sich der Virus so stark – weil die Diskette so oft kopiert wurde –, dass sich die Brüder gar nicht retten konnten vor Hilfegesuchen betroffener Nutzer:innen.

Vielleicht war Storm Worm auch nur ein aus dem Ruder gelaufenes Experiment irgendeines Nerds. Allerdings ein ausgefeiltes. Es sollte ein Rätsel bleiben – eines, das die Gefahren klar machte.

CONFICKER

Doch es dauerte keine zwei Jahre, bis das nächste massive Botnetz Ende 2008 um die Welt zog: Diesmal waren bis zu 15 Millionen Rechner auf der ganzen Welt infiziert, und das Botnetz richtete erstmals reale Schäden an: Conficker – so wurde es getauft – legte unter anderem die Uniklinik Düsseldorf lahm. Noch nie hatte sich ein Botnetz in so rasendem Tempo und so erbarmungslos ausgebreitet.

Eines war schnell klar: Hinter diesem Netz standen Profis. Das Verschlüsselungsprotokoll, das der Wurm nutzte, war das allerbeste, was die Welt zu diesem Zeitpunkt zu bieten hatte – unter anderem war der Algorithmus MD6 implementiert, der erst wenige Wochen vor dem erstmaligen Auftauchen Confickers am Massachusetts Institute of Technology entwickelt worden und noch nicht öffentlich war.

Das Sicherheitsunternehmen Panda ging im Januar 2009 davon aus, dass rund sieben Prozent aller deutscher Windows-Computer mit Conficker infiziert seien – was hochgerechnet weltweit bedeuten würde, dass 50 Millionen Maschinen betroffen waren. Im Verlauf der Infektion kämpften unter anderem die Bundeswehr und die französische Luftwaffe mit dem Wurm. Im September 2010 entsorgte das Bildungsministerium von Mecklenburg-Vorpommern 170 teils nagelneue Computer, weil sie mit Conficker befallen waren. Im AKW Gundremmingen wurde sogar im April 2016 noch eine Infektion mit Conficker entdeckt – was offenbar zu keiner akuten Gefährdung führte, aber ein Hinweis auf fragwürdige IT-Sicherheit ist. Denn offenbar gab es dort nicht nur dermaßen alte Computer ohne Update, sondern auch Wege, wie die Schadsoftware dorthin fand – infiziert war ein Rechner ohne Verbindung zum Internet.

Im Frühjahr 2009, auf dem Höhepunkt der Angriffe, wartete die IT-Sicherheitsszene gebannt und ängstlich auf den nächsten Schritt des unbekannten Botmasters. Er hatte Millionen von Computern in der Hand. Sie kommunizierten regelmäßig mit einem unbekannten Mastermind und warteten auf Befehle. Millionen ferngesteuerter Computer.

Doch auch dieser Computerwurm verschwand so plötzlich, wie er gekommen war. Auch hier stellte der unbekannte Botmaster plötzlich die Arbeit ein. Genaugenommen ist der Wurm nie ganz verschwunden, weil ältere Windows-Versionen nach wie vor anfällig sind. Im Juni 2019 schätzte der Journalist und Autor Mark Bowden, dass nach wie vor 500 000 Computer weltweit mit Conficker infiziert seien.[02] Bis heute ist nicht wirklich klar, wer genau hinter Conficker stand und was der Plan war. Doch er hat der Welt gezeigt, wie gefährlich ein Botnetz sein kann.

GAMEOVER ZEUS

Jewgeni Bogatschew schaute den Entwicklungen nicht tatenlos zu – im Gegenteil: Er entwickelte sich weiter und baute seine eigene Schadsoftware ebenfalls zu einem ausgefeilten Botnetz aus: Gameover Zeus. Denn nachdem Bogatschew beobachtet hatte, wie immer mehr Kriminelle eigene Botnetze bauten und dabei Zeus benutzten, teilweise in Form von Raubkopien, wollte er mehr Kontrolle. Er beschloss, selbst ein Botnetz zu betreiben und es als Dienstleistung zu vermieten. „Gameover Zeus war leistungsfähiger und ausgeklügelter als alles, was bis dahin auf dem Markt war", sagt Werner. Ähnlich wie Storm Worm hatte Gameover Zeus eine dezentrale Befehlsstruktur: Die neue Zeus-Variante stützte sich also auch auf die Peer-to-Peer-Kommunikation zwischen den übernommenen Rechnern. Die infizierten Rechner führten dafür eine ständig aktualisierte Liste anderer infizierter Rechner und kommunizierten untereinander.

Der Botmaster konnte neue Befehle an jeder Stelle einstreuen, und diese wurden weitergegeben: Das Netzwerk hatte eine Architektur, die jeden Angriff von Behörden verhinderte. Es ließ sich nicht abschalten – jedenfalls nicht von einer einzelnen Stelle aus. „Es war perfekt abgesichert gegen uns", sagt Werner. Klassische Methoden der Abwehr funktionierten nicht mehr: Würden Behörden einen Server vom Netz nehmen, könnte Bogatschew einfach einen neuen Server starten und das Peer-to-Peer-Netzwerk auf diesen umleiten.

Der Schaden, den Bogatschew und seine kriminellen Mitstreiter:innen damit anrichteten, ging schnell in die Millionen. Sie fingen in großem Stil Kontodaten ab, überwiesen das Geld der Opfer auf ihre eigenen Konten – und gleichzeitig nutzten sie das Netz für DDoS-Attacken auf die entsprechenden Banken, um die Angestellten abzulenken und so Zeit zu gewinnen: Die Betroffenen sollten erst dann merken, dass ihnen Geld fehlte, wenn das Geld bereits über mehrere Ecken ins Ausland überwiesen war. Am 6. November 2012 beobachtete das FBI, wie das Game-Over-Netzwerk 6,9 Millionen Dollar in einer einzigen Transaktion stahl.[03]

In diesen Tagen im Winter 2012 tat Werner etwas ähnliches wie Daniel Lorch zehn Jahre später: Zusammen mit Kolleg:innen visualisierte er das Botnetz. Die Sicherheitsforscher erstellten Kar-

02 Vgl. Mark Bowden, The Enemy Within, Juni 2010, www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/308098.

03 Vgl. Graff (Anm. 1).

ten und zeichneten Netzwerke – teilweise ähnlich wie das, was an Lorchs Bürowand hängt. Dabei wurde klar, wie ausgefeilt die Architektur des Netzes ist. Es brauchte mehrere Anläufe, denn die Verfolger:innen übersahen, wie gut das Netz gegen die Übernahme ausgestattet war. Das Finale fand schließlich Ende Mai 2014 in einem FBI-Büro in Pittsburgh statt:[04] Werner war damals zusammen mit seinem Freund und Kollegen Brett Stone-Gross extra eingeflogen worden, denn inzwischen galt er als einer der wenigen erfahrenen Expert:innen, wenn es um Botnetze ging. Werner und Stone-Gross kämpften dort zwei Tage und Nächte lang gegen Bogatschew, der sich erbittert wehrte. Immer wieder flammte das Netzwerk an verschiedenen Ecken auf, immer wieder schaffte er es angesichts der ausgefeilten Architektur des Netzes, einen Teil der gekaperten Computer erneut zu übernehmen und das Netz wieder auszubauen. Doch irgendwann gab er auf.

ERSCHWERTE VERFOLGUNG

Seither ist es ruhig geworden um den berühmten russischen Internetkriminellen. Wo steckt Bogatschew und was macht er heute? Manche Sicherheitsforscher:innen vermuten, dass der kriminelle Hacker einen Deal mit dem russischen Staat hat, der ihn versteckt und im Gegenzug von seinen Fähigkeiten profitiert. Mindestens einmal wurde das Zeus-Botnetz offenbar für politische Spionage genutzt. Zwischen 2015 und 2017 sei im Zuge der russischen Angriffe auf die Ukraine außerdem eine neue, noch unbekannte Zeus-Variante aufgetaucht, sagt Werner.

Heute arbeitet Werner beim US-Unternehmen Crowdstrike, das sowohl kriminelle als auch staatliche Akteure im Cyberspace verfolgt und deren Angriffe analysiert. Er beobachtet, dass diese beiden Gruppen immer mehr verschwimmen, und sich nicht immer klar trennen lassen. Bogatschew sei einer der besten Leute. Wieso sollte der russische Staat auf die Kapazitäten eines der begabtesten Hacker des Landes verzichten? Dass der russische Geheimdienst das Können seiner Bürger:innen breit anzapft, zeigen nicht zuletzt die sogenannten Vulkan Files, die im April 2023 von einer Medienkooperation ausgewertet wurden und darauf hindeuten, wie ein privates Unternehmen Cyberangriffe für die russischen Geheimdienste entwickelt.

Bogatschews geistiges Schaffen wirkt weiter. Bis heute entdecken Sicherheitsforscher:innen immer wieder Spuren von überarbeiteten Zeus-Banking-Trojanern, die gewiefte Kriminelle in ausgefeilte Strategien einbauen, um in Bankkonten einzudringen. Noch schwerer wiegt freilich die Professionalisierung, die er in die Szene gebracht hat: Der gesamte Prozess eines Angriffs wird heute in viele Zwischenschritte aufgeteilt – und für jeden davon gibt es in der Branche Expert:innen, erklärt Daniel Lorch: „Es gibt Initial Access Brokers, also Täter, die allein für den ersten Zugang in ein Unternehmen zuständig sind, darunter wiederum Experten für Social Engineering“, – soziale Manipulation also, in deren Rahmen Opfer mit überzeugenden Phishing-E-Mails sowie gut gefälschten Websites hinters Licht geführt werden, um ihre Zugangsdaten zu verraten oder sich Schadsoftware herunterzuladen. Und auch für die folgenden Schritte gibt es Fachleute, beispielsweise für die Suche nach offenen Schwachstellen in den Netzen von Unternehmen, für das Verfassen des Angriffscodes, für das Ausspähen der Opfer und den Angriff selbst, für den Verkauf der erbeuteten Daten – und am Ende der Kette stehen Spezialist:innen für Geldwäsche.

Das erschwert die Verfolgung, denn jeder einzelne Schritt ist nahezu perfekt organisiert und gegen Behörden-Eingriffe abgesichert. Dennoch: Am Ende gewinnt, wer nicht aufgibt. Daniel Lorch und seinen Kolleg:innen ist es gelungen, in das innere Netzwerk der Ransomware-Bande Hive einzudringen. Ein halbes Jahr lang haben sie alles verfolgt, was dort diskutiert wurde. Wer so viel Kommunikation krimineller Hacker mitliest, kennt einzelne von ihnen schon sehr gut. Lorch kennt ihre Decknamen, ihre Rolle in der Gruppe und ihre Probleme. Einen Täter habe er beobachtet, wie er immer wieder an Sicherheitsmaßnahmen scheiterte. Er sah zu, wie er Zugriff auf einen kleinen Teil des Netzwerks bekam, nur um dann von einem Schutzsystem wieder abgemeldet zu werden. Jede einzelne Schutzmaßnahme habe sich gelohnt. „Der war irgendwann richtig genervt“, sagt Lorch lachend. Und dann habe er aufgegeben.

EVA WOLFANGEL
ist Wissenschaftsjournalistin. Zuletzt erschien von ihr das Buch „Ein falscher Klick. Hackern auf der Spur: Warum der Cyberkrieg uns alle betrifft“.
mail@ewo.name

04 Vgl. ebd.

INTERVIEW

„DIE GEFÄHRDUNGSLAGE IST SO HOCH WIE NIE ZUVOR“

Ein Gespräch über die aktuelle Cybersicherheitslage, den IT-Fachkräftemangel und die Frage, wie die Informationssicherheit in Deutschland verbessert werden kann

mit Gerhard Schabhüser

Wie schätzen Sie die aktuelle Cybersicherheitslage in der Bundesrepublik ein?
Gerhard Schabhüser – Die Gefährdungslage im Cyberraum ist so hoch wie nie zuvor. Wir hatten bereits im BSI-Lagebericht 2021 die Lage in Teilen mit „Alarmstufe Rot“ bewertet. Wenn ich jetzt sage, dass die aktuelle Gefährdungslage höher ist, müsste ich eigentlich von einer Krise sprechen. Und in der Tat sind wir zweimal an einer Krise vorbeigeschrammt – in beiden Fällen waren es Folgen des russischen Angriffskrieges gegen die Ukraine. Der erste Fall war der Hack des Viasat-Satellitennetzwerkes unmittelbar zu Beginn der Invasion. In der Folge waren alle Modems des Netzwerks gestört. In Deutschland führte der Hack dazu, dass die Fernwartung von Windparks nicht mehr möglich war. Wäre auch die Steuerung der Windparks über das Viasat-System erfolgt, wäre es möglicherweise zu einem Energieengpass gekommen. Der zweite Fall geht auf die Hackergruppe Anonymous zurück. Die Hacker haben im März 2022 die Rosneft Deutschland GmbH gehackt. Die Rosneft Deutschland ist eine Tochter des russischen Mineralölkonzerns Rosneft, aber auch Teil der kritischen Infrastruktur in Deutschland. Die Systeme von Rosneft Deutschland waren so gestört, dass wir dort in eine Engpasssituation gekommen wären, wenn die Systeme nicht innerhalb von 10 bis 20 Tagen mit Unterstützung des BSI in einen Notbetrieb gebracht worden wären. Dann hatten wir noch eine ganze Reihe DDoS-Angriffe von pro-russischen Hackergruppen im vergangenen Jahr und Anfang dieses Jahres. Aber diese Angriffe auf Websites waren relativ leicht abzuwehren.

Insgesamt ist Ransomware immer noch die größte Bedrohung für Wirtschaft und Gesellschaft. Diese Erpressungsversuche haben oft unmittelbare Auswirkungen auf Bürgerinnen und Bürger, insbesondere wenn die öffentliche Verwaltung angegriffen wird. Manchmal werden auch IT-Dienstleister angegriffen. Wenn solche Firmen lahmgelegt werden, sind sehr viele Kunden unmittelbar betroffen.

Bei den Angreifern dreht sich derzeit viel um Russland und russische Hackergruppen. Welche anderen Gruppen gibt es?
– Es gibt sehr viele Angreifergruppen. Im Crime-Bereich ist das sehr heterogen. Da kann man kaum einen Schwerpunkt ausmachen. Bei Spionage gibt es circa über 130 aktive Gruppen. Aber man sieht schon eine Häufung aus Russland, China, Nordkorea und Iran.

Wie stellt das BSI den Schutz vor all diesen Gruppen her?
– In den Netzen des Bundes sind wir befugt, Sicherheitsmaßnahmen zu treffen, die bis in das Fernmeldegeheimnis hineinreichen. Wir dürfen Schadsoftware-Erkennungssysteme an den Grenzen zu den Netzen des Bundes betreiben. Dort suchen wir in E-Mails automatisiert nach Schadsoftware. Wenn die Automatisierung eine Warnung anzeigt, dann dürfen wir auch „mit Menschen“ da reinschauen. Umgekehrt dürfen wir auch Schadsoftware-Prävention betreiben, wenn wir sehen, dass aus den Netzen des Bundes seltsame IP-Adressen angesteuert werden. Dann können wir diese Mails blockieren und schauen, ob vielleicht schon etwas im Netz verseucht ist. Ebenso operativ arbeiten wir bei der Fallbearbeitung. Etwa wenn es einen Cybervorfall in der Bundesverwaltung, einer kritischen Infrastruktur

oder bei Organisationen von besonderem öffentlichen Interesse gibt. Dann leisten wir mit unserem Mobile Incident Response Team Erste Hilfe und analysieren die Situation. Das können wir nicht für jeden machen, aber für diese Bereiche schon. Wir sind dann vor Ort, installieren forensische Sensoren und machen sogenanntes Reverse Engineering. Und natürlich beraten wir die Betroffenen, wie sie den Schaden begrenzen und/oder stoppen können.

An wen wende ich mich als mittelständisches Unternehmen, wenn ich Opfer eines Cyberangriffs werde?
– Gerne an das BSI, allein schon für das Lagebild ist das wichtig. Und wir können Betroffenen auch Materialien zur Verfügung stellen, eine Art Erste-Hilfe-Paket, wo unter anderem auch von uns qualifizierte Dienstleister aufgelistet sind.

Was bietet das BSI für Bürgerinnen und Bürger?
– Informationskampagnen mit Hilfetipps, die sich auch an Mitarbeitende in kleineren Unternehmen richten: Da geht es um das einfache Erklären von schwierigen IT-Sicherheitsproblemen, um konkrete Handlungsempfehlungen zu geben. Meine Einschätzung ist, dass die Sensibilität für das Thema schon vorhanden ist. Aber die Handlungsbereitschaft ist noch nicht so hoch, wie sie sein sollte. Jeder weiß, dass etwas getan werden muss, aber der Schritt vom Wissen zum Handeln wird noch nicht oft genug getan. Das hat viele Gründe. Ein Grund ist, dass Cyberprobleme oft erst sehr spät erkannt werden. Die Probleme sind nicht immer unmittelbar erlebbar. Ransomware ist natürlich sehr erlebbar und hat die Sensibilität drastisch nach oben getrieben. Zum Teil fehlt aber auch das Wissen darum, was zu tun ist, um aus den Problemen wieder herauszukommen. Da versuchen wir, mit zielgruppenspezifischen Kampagnen zu helfen. Und wir wollen den Verbraucherinnen und Verbrauchern mit unserem IT-Sicherheitskennzeichen ganz direkt Orientierung geben. Das ist ein freiwilliges Siegel, das ein Produkteanbieter beim BSI beantragen kann. Der Anbieter muss einige formale Voraussetzungen erfüllen. Dann darf er das Sicherheitskennzeichen auf seiner Produktverpackung anbringen – zusammen mit einem QR-Code, der zur Website des BSI führt, wo aktuelle Informationen zum Sicherheitsstatus des Produkts abgerufen werden können. Das Siegel soll Verbraucherinnen und Verbraucher in die Lage versetzen, das Thema Informationssicherheit bei ihrer Kaufentscheidung angemessen zu berücksichtigen.

Was müsste aus Ihrer Sicht passieren, damit das BSI für mehr Sicherheit sorgen kann?
– Die Angreifer entwickeln ihre Technik weiter. Wir müssen prüfen, ob unsere Befugnisse ausreichen, um Schützen zu können, zum Beispiel die Scanbefugnisse des BSI. Wir können durchaus in den Netzen des Bundes nach Schwachstellen scannen. Was wir brauchen, ist eine Scanbefugnis des BSI für die gesamte kritische Infrastruktur, um zu schauen, wo Schwachstellen und Einfallstore sind. Kürzlich wurden die sogenannten Vulkan Files veröffentlicht. Dort fand man ein groß skalierbares Scantool, mit dem die Angreifer sehen konnten, wo es Schwachstellen gibt. Jetzt scannen unsere Angreifer überall nach Verwundbarkeiten, um irgendwo reinzukommen. Die halten sich an kein Gesetz, an keine Regeln und bereiten Angriffe vor, und wir sitzen hier und könnten technisch nach solchen Verwundbarkeiten suchen, dürfen es aber nicht. Wir können daher Betroffene nicht warnen.

Dann sehe ich noch Handlungsbedarf bei der Cybersicherheitsarchitektur in Deutschland, was die Bund-Länder-Aufstellung angeht. Nach dem Grundgesetz gilt das Trennungsprinzip, das heißt jede staatliche Ebene hat ihre Aufgaben eigenverantwortlich und mit eigenen Ressourcen zu erfüllen. Eine Zusammenarbeit zwischen Bund und Ländern ist daher nur in explizit geregelten Fällen möglich. Deshalb ist die Bundesregierung dabei, das BSI zu einer Zentralstelle auszubauen. Einseitig kann das BSI die Länder im Moment nur im Rahmen der Amtshilfe unterstützten. Das müssen wir ändern.

Was verstehen Sie unter aktiver Cyberabwehr?
– Aktive Cyberabwehr muss man zunächst deutlich von sogenannten Hackbacks trennen. Es gibt zum Beispiel die Möglichkeit, den Angreifer von seinen Opfern fernzuhalten. Technisch realisiert man das, indem man Umleitungen im Internet einrichtet. Dann kommen die Datenabfragen der Angreifer gar nicht erst

beim Opfer an. Wir dürfen also die Netzbetreiber anweisen, IP-Adressen umzuleiten. Die Anordnungsbefugnis umfasst auch das Blockieren. Wenn wir zum Beispiel sehen, dass Einrichtungen aus einem Land massiv angreifen, dann können wir den IP-Verkehr blockieren. Das ist schon ein sehr starkes Mittel. Der letzte Schritt ist dann, in die Systeme des Angreifers selbst einzudringen und dort Schritte zur Abstellung des Angriffs einzuleiten. Beispielsweise Daten löschen oder Prozesse beenden. Ich denke, wenn man die Befugnisse des BSI in den genannten Bereichen noch etwas erweitert, kann man Cyberangriffe so weit abwehren, dass sie in Deutschland keine großen Auswirkungen haben.

Welche Herausforderungen und Chancen sieht das BSI im Bereich Künstliche Intelligenz und Cybersicherheit?

– Für uns hat das Thema drei Dimensionen: IT-Sicherheit für KI, IT-Sicherheit durch KI und Angriffe durch KI. Bei der Sicherheit für KI stellen sich zunächst die üblichen Fragen: Wie ist die Software geschrieben? Ist der Zugriff vernünftig organisiert und so weiter. Das ist nicht die große Herausforderung. Interessant wird es erst bei der Frage, wie KI zu Entscheidungen kommt. Das sehen wir durchaus als Sicherheitsaspekt. Und zum anderen: Wie wird KI trainiert, beziehungsweise wie lernt KI? Ist die KI robust gegen vergiftete Lernmengen? Wenn ich zum Beispiel unausgewogene Trainingsmengen nutze, dann kann es sein, dass die KI „schiefe" Ergebnisse produziert. Schaffe ich es zum Beispiel, die KI bei der Erkennung von Verkehrsschildern so zu trainieren, dass Aufkleber auf den Schildern nicht zu Fehlinterpretationen führen? Dass also ein Aufkleber auf einem Stoppschild nicht dazu führt, dass die KI das Stoppschild für ein Tempo-80-Schild hält? Das hätte natürlich unmittelbare Auswirkungen auf die Sicherheit. Mit so einem kleinen Aufkleber kann man tatsächlich das ganze Bild verbiegen. Das ist auch ein Bereich, mit dem wir uns beschäftigen, und das ist eine Herausforderung. Das Ziel sind automatische Prüfkriterien für den Hersteller oder den unabhängigen Prüfer einer solchen Anwendung. Dann bietet KI natürlich ein enormes Potenzial, große Datenmengen strukturiert zu analysieren, Anomalien zu erkennen und mit neuronalen Netzen Aussagen zu treffen, die für unsere Entscheidungsfindung sehr wichtig sein können. Angriffe durch KI wären genau das Gegenteil: Schwachstellen suchen, um sie auszunutzen. Also die dunkle Seite der Künstlichen Intelligenz. Was wir heute auch schon sehen, sind Deepfakes. Heute kann man Fakes oft noch mit bloßem Auge erkennen. Aber die Angreifer werden immer besser darin. Wir simulieren solche Dinge. Kürzlich besuchte eine Bundestagsabgeordnete das BSI, der wir das vorgeführt haben. Einer unserer Kollegen hat eine einminütige Rede aufgenommen. Und dann hat er eine zehnsekündige Sprachsequenz seines Chefs in das Tool geladen, und es klang so, als hätte sein Chef die Rede gehalten. Das war erstaunlich gut. Solche Tools erhöhen das Risiko für Desinformationskampagnen. Unsere Aufgabe ist es, Detektionsmechanismen zu finden.

Wie begegnet das BSI dem Fachkräftemangel?

– Personalgewinnung ist für uns kein Problem. Wir sind bei einer Besetzungsquote von 90 Prozent. Und das, obwohl wir uns in den drei Jahren zuvor verdoppelt haben. Wir begrüßen zwischen 100 und 200 neue Mitarbeitende im Jahr. Eigentlich heißt das, dass es für uns das Fachkräftemangel-Problem nicht gibt. Wir denken, dass der öffentliche Dienst durch Corona und die Unwägbarkeiten des Arbeitsmarktes insgesamt an Attraktivität gewonnen hat. Außerdem scheint es so zu sein, dass gerade Berufseinsteiger bei der Berufswahl nicht nur das Thema Geld im Kopf haben, sondern auch die Frage: Tue ich etwas Gutes für die Welt? Bei den MINT-Studiengängen sind wir bei den Absolventinnen und Absolventen die beliebteste Bundesbehörde. Auch in die Personalbindung investieren wir viel. Wenn trotzdem jemand geht, reißt das erst einmal eine Lücke. Aber gesamtgesellschaftlich gesehen finde ich das gar nicht schlecht, weil dann hat der Einzelne hier ein Mindset bekommen und Methoden gelernt, die dann in andere Bereiche der Gesellschaft überschwappen. Das ist dann gut für ganz Deutschland. Wenn wir Personal verlieren, dann fast immer, wenn ein Angebot aus der Forschung und Lehre kommt. Für den Professorentitel verlässt man gerne mal das BSI. Aber auch das finde ich nicht schlecht, weil gerade in der Lehre und Forschung

diese wichtigen Themen weiterverbreitet werden müssen.

Wie erreichen wir als Gesellschaft Informationssicherheit?

– Auf der Nutzerseite würde ich mir wünschen, dass das Thema Informations- und Cybersicherheit ein integraler Bestandteil des Risikomanagements wird. Dann wäre das Thema auch immer für den Vorstand oder Aufsichtsrat relevant und würde sich als Chefinnen- und Chefsache etablieren. Auf der Herstellerseite wünsche ich mir, dass das Thema IT-Sicherheit integraler Bestandteil des Qualitätsmanagements wird. Auch hier haben wir eine regelmäßige Auditierung des Qualitätsmanagements, auch automatisch mit Vorstandsrelevanz. Und mit Blick auf die breite Öffentlichkeit halte ich zwei Dinge für wichtig: Leicht verständliche Botschaften und konkrete Hilfestellungen müssen für alle zugänglich sein. Das ist der eine Teil – der andere Teil ist etwas schwieriger umzusetzen. Eigentlich sollten die Bürgerinnen und Bürger gar nicht so viel selbst machen müssen. Wir brauchen Security by Design and Default – also Sicherheitsmechanismen, die von vornherein in die Anwendung eingebaut sind. Und darüber hinaus hätten wir einen Großteil der Probleme schon gelöst, wenn wir von Passwörtern wegkommen würden und immer eine einfach zu bedienende Zwei-Faktor-Authentifizierung integriert hätten. Dafür haben wir eigentlich schon die Plattformen. Wir haben in Deutschland über 60 Millionen elektronische Ausweise wie Personalausweise und so weiter. Wenn wir das flächendeckend in die Anwendungen reinbekommen, fällt ein Großteil der Probleme einfach weg. Neben Awareness- und Kompetenzmaßnahmen müssen wir die Probleme technisch lösen. Beim Autofahren werden uns ja auch viele Dinge abgenommen – und diesen Weg müssen wir auch bei der IT-Sicherheit einschlagen.

Das Interview führte Lorenz Abu Ayyash am 27. April 2023 in Bonn.

GERHARD SCHABHÜSER
ist Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

INTERVIEW

„WIR BRAUCHEN EINEN NOTFALLPLAN“

Ein Gespräch über die deutsche Cybersicherheitsarchitektur, Cyberoperationen und Grundgesetzänderungen

mit Sven Herpig

Wie stellt sich die aktuelle Cybersicherheitslage in Deutschland dar? Wie gefährdet ist Deutschland?
Sven Herpig – Laut der Innenministerin Nancy Faeser, die die auswertenden Behörden unter sich hat, haben wir im Cyberbereich die höchste Bedrohungslage, die wir je hatten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird in den Lageberichten der vergangenen Jahre nicht müde zu betonen, dass die Gefährdungslage auf einem sehr hohen Niveau stagniert. Dazu ist zweierlei zu sagen: Erstens sind Aussagen zur Gefährdungslage immer auch politische Aussagen. In den vergangenen Jahren wurden viele Ressourcen in das Thema gesteckt, um Deutschland sicherer zu machen. Es sieht natürlich schlecht aus, wenn es trotzdem jedes Jahr schlimmer wird – also stagniert es jedes Jahr auf hohem Niveau. Zweitens: Um ein umfassendes Bild zu bekommen, müssten wir alle Lagebilder wie ein Puzzle zusammensetzen. Es gibt das Lagebild des BSI, das des Bundeskriminalamtes und das des Bundesamtes für Verfassungsschutz. Beim Verfassungsschutz fließen die Informationen des Bundesnachrichtendienstes ein und bei der Bundeswehr, die Teile ihrer Erkenntnisse mit dem BSI teilt, die Informationen des Militärischen Abschirmdienstes. Dabei ist noch nicht berücksichtigt, dass nur Unternehmen der kritischen Infrastruktur meldepflichtig sind. Das heißt, alle anderen Unternehmen, und das sind die meisten, müssen Vorfälle nicht unbedingt melden. Dadurch haben wir eine sehr unvollständige Datenlage.

Sie verweisen auf die komplexe Sicherheitsarchitektur der deutschen Cybersicherheitspolitik. Was muss getan werden, um Deutschland besser zu schützen?
– Zur Komplexität sind zwei Dinge zu sagen: Zum einen sind wir ein föderaler Staat, und damit ist auch die Cybersicherheitspolitik föderal organisiert. In den vergangenen Jahren haben sich immer mehr Bundesländer eigene IT-Sicherheitsgesetze gegeben und eigene Akteure in ihrem Bundesland aufgebaut, die sich mit Cybersicherheit beschäftigen. Zweitens ist die Cybersicherheitspolitik für Deutschland ein relativ neues Feld. Das BSI wurde zwar schon 1991 gegründet, aber als Politikfeld ist das Thema in Deutschland erst in den 2010er Jahren richtig angekommen. Das hing auch mit der Stuxnet-Operation im Iran zusammen – das hat hohe Wellen geschlagen, als man gesehen hat, dass Nuklear-Anreicherungsanlagen mit Schadsoftware manipuliert werden können. Und dann hat man in Deutschland das gemacht, was man bei neuen Themenfeldern immer macht: Man schafft Akteure wie das Nationale Cyber-Abwehrzentrum, den Nationalen Cyber-Sicherheitsrat und so weiter. Und das ist auch gut so. Aber irgendwann muss man innehalten und die Architektur anschauen, evaluieren und im Zweifel reformieren. Und das ist bis heute nicht geschehen. Wir müssen eine Kommission einsetzen, die evaluiert, ob unsere Cybersicherheitsarchitektur noch den heutigen Anforderungen entspricht, und wenn sie das nicht tut, müssen wir auch entsprechende Reformschritte einleiten.

Welche Konflikte sehen Sie in der aktuellen Situation?
– Neben der internen Abstimmung innerhalb der Bundesregierung in bestimmten Politikbereichen gibt es ein Spannungsfeld zwischen der Regierung auf der einen Seite und der Zivilgesellschaft, der Wissenschaft und der Industrie auf der anderen Seite, insbesondere bei Themen wie intrusive Cyberoperationen, also das Einbrechen in IT-Systeme. Solche Operationen verhel-

fen zwar Nachrichtendiensten und Polizeien dazu, ihren gesetzlichen Auftrag zu erfüllen, schaffen aber selten ein Mehr an Cybersicherheit. Es gibt zum Teil starke Diskrepanzen zwischen dem, was das Innenministerium aus Gründen der öffentlichen Sicherheit umsetzen möchte, und dem, was die restlichen Akteure sagen, was für die IT-Sicherheit und damit auch für Deutschlands Wirtschaft und Gesellschaft sinnvoll wäre.

Können Sie Beispiele nennen?
– Bleiben wir bei den intrusiven Cyberoperationen, die zwei kontroverse Punkte beinhalten. Um intrusive Cyberoperationen durchführen zu können, müssen gefundene Schwachstellen zurückgehalten werden, damit Sicherheitsbehörden sie für einen bestimmten Zeitraum ausnutzen können. Wenn Schwachstellen zurückgehalten werden, bleiben jedoch alle IT-Systeme, in denen sie existieren, verwundbar gegenüber Kriminellen und Nachrichtendiensten. Für den staatlichen Umgang mit diesen Schwachstellen haben wir uns immer noch nicht auf einen Prozess geeinigt. So macht jede Behörde, was sie will – ohne das große Ganze im Blick zu haben. Der zweite Punkt ist, dass wir für diese Operationen Steuergelder ausgeben und dafür Überwachungswerkzeuge von Firmen einkaufen. Diese entwickeln die Werkzeuge weiter – mit deutschen Steuergeldern – und verkaufen sie auch an andere Länder wie zum Beispiel Saudi-Arabien, wo solche Technologien eingesetzt werden, um Menschenrechtsaktivistinnen oder Journalisten zu überwachen – oder Schlimmeres: Der Mord an dem Journalisten Jamal Khashoggi ist der bekannteste Fall, bei dem solche Überwachungssoftware eingesetzt wurde.

Wie funktioniert die Zusammenarbeit von staatlichen und nicht-staatlichen Akteuren?
– Zum einen gibt es die Zusammenarbeit, um Deutschland sicherer zu machen. Dazu gehört zum Beispiel die Zusammenarbeit zwischen Behörden und IT-Sicherheitsunternehmen, oder auch der Bereich, in dem wir als Stiftung tätig sind, nämlich darüber nachzudenken, was gute Policies sind, um Deutschland sicherer zu machen – aus einer gesellschaftlichen Perspektive und eben nicht aus einer Behördenperspektive. Dazu kommt der Bereich Forschungsförderung, unter anderem für sichere Hard- und Software. Und dann gibt es global gesehen noch eine weitere Art der Zusammenarbeit, die aber problematisch ist. Nämlich dann, wenn Staaten an Daten kommen wollen – zum Beispiel für intrusive Cyberoperationen. Dann arbeiten sie mit Unternehmen zusammen, die Überwachungswerkzeuge herstellen und verkaufen. Diese Firmen bewegen sich in einem Graubereich, oft einem sehr dunkelgrauen. Weiterhin gibt es sowohl die organisierte Kriminalität als auch Söldner, die im Cyberraum aktiv sind. Das sind nicht-staatliche Akteure, die zum Beispiel wie in Russland auch mal in Absprache mit den Sicherheitsbehörden agieren. Bei den Söldnern wiederum handelt es sich um Firmen, die für Staaten arbeiten, die selbst keine offensiven oder intrusiven Fähigkeiten aufbauen können oder wollen. So können mittlerweile sehr viele Staaten Geld in die Hand nehmen und Firmen damit beauftragen, iPhones von Menschenrechtsaktivisten zu kompromittieren. Staaten müssen diese Fähigkeiten gar nicht mehr entwickeln, sodass die Einstiegsschwelle für destabilisierende Aktivitäten im Cyberraum immer niedriger wird. Und so fließt viel Geld in dieses Ökosystem, sowohl über die organisierte Kriminalität als auch über die Staaten selbst. Und dieses Geld wird wiederum dafür genutzt, bessere Werkzeuge zu programmieren oder Schwachstellen zu finden. Das untergräbt weltweit die Sicherheit unserer IT-Infrastrukturen.

Woher nehmen Sie Ihr Wissen, wenn Sie keinen Zugang zu Geheimdienstinformationen haben?
– Natürlich sprechen wir wie viele andere auch mit Praktikern und Forscherinnen aus verschiedenen Bereichen. Aber grundsätzlich muss man eines verstehen: Der IT-Sicherheitsbereich ist ein sehr großer Markt. Es gibt viele IT-Sicherheitsfirmen, die Geld verdienen und Geld verdienen wollen. Die stehen natürlich in Konkurrenz zueinander und wollen deshalb gute PR-Arbeit machen. Das tun sie unter anderem dadurch, dass sie viele Cyberoperationen aufklären und Berichte darüber verfassen. Und diese stellen sie kostenlos zur Verfügung, weil sie das Ökosystem sicherer machen wollen, aber natürlich auch, weil es gute PR ist. Unternehmen wissen, dass Wettbewer-

ber sie für falsche Informationen kritisieren würden. Das ist einer der Gründe, warum es in diesem Bereich – vielleicht auch im Vergleich zu anderen Sicherheitsbereichen – eine gute öffentliche Informationsbasis gibt. Woher erhalten die Unternehmen ihre Informationen? Zum einen werden sie bei Vorfällen angerufen und müssen diese aufklären. Zum anderen läuft ihre Software auf vielen Systemen. Das heißt, sie sehen, was auf diesen Systemen passiert und können entsprechende Berichte schreiben.

Welche Auswirkungen hat der russische Angriffskrieg auf die Debatten im Bereich Cybersicherheit?
– Mit Blick auf die Debatten um intrusive Cyberoperationen, aktive Cyberabwehr im Ausland oder das Ausnutzen von Schwachstellen ist es tatsächlich so, dass Politikerinnen und Politiker, die schon vor dem Krieg eine Ausweitung der Befugnisse für Sicherheitsbehörden gefordert haben, nun auch von einer Zeitenwende im Cyberraum sprechen. Sie benutzen den Angriffskrieg, um zu rechtfertigen, dass bestimmte Fähigkeiten und Befugnisse nötig sind, um sich zu verteidigen. Das ist politisch verständlich. Ich glaube, wenn ich politisch verantwortlich wäre und diese Befugnisse wollte, dann würde ich das auch tun. Aber es ist auch ein bisschen unehrlich, weil der Angriffskrieg für den Cyberraum bisher zu keinen bahnbrechenden neuen Erkenntnissen geführt hat. Was Russland eingesetzt hat, war schon vorher bekannt. Wie die Russen es einsetzen und wie sie es mit ihren Land-, Luft- und Seekampagnen kombinieren, ist interessant, hat aber nichts damit zu tun, ob wir jetzt unsere intrusiven Fähigkeiten und Befugnisse erweitern sollten oder nicht.

Wie sehr ist Deutschland im Fokus von Angreifern? Ist Deutschland im internationalen Vergleich besonders gefährdet?
– Das kann man schon sagen. Gerade die deutschen Unternehmen stehen im Visier von nachrichtendienstlicher Spionage, zum Beispiel aus China, aber auch von organisierten Kriminellen im Cyberraum, die mit wenig Aufwand viel Geld machen wollen. Und wenn ich mir den gesamten Bereich der KMU, also der kleinen und mittleren Unternehmen, anschaue, dann ist es natürlich logisch, dass diese oft Ziel von Cyberkriminellen sind. KMUs haben oft ausreichend Geld, um für Kriminelle attraktiv zu sein, und sie setzen selten die IT-Sicherheitsmaßnahmen um, die sie umsetzen müssten. Daher ist die Gefährdungslage in Deutschland schon sehr hoch. Ich denke auch im Vergleich zu einigen anderen Ländern.

Und wie kann man diese Unternehmen besser schützen?
– Zwei Punkte sind hier sehr wichtig. Das eine ist die Frage der Fachkräfte. Ich kann natürlich den KMUs viele Informationen und Werkzeuge zur Verfügung stellen, aber wenn es dort niemanden gibt, der IT-Sicherheit macht, oder nur zwei Stunden in der Woche, dann nützt das nichts. Das heißt, wir müssen gerade die Aus-, Um- und Weiterbildung im Bereich der IT-Sicherheit fördern, wir müssen schauen, ob wir neue Curricula brauchen, ob wir neue Ausbildungsberufe brauchen und wie wir schnell Leute in den IT-Bereich bekommen. Und ich rede nicht davon, dass wir neue Masterstudiengänge für Cybersicherheit schaffen. Wir brauchen hier keine studierten Kryptologen oder was auch immer. Wir brauchen hier Leute, die wissen, wie man Firewalls konfiguriert, wie man Systeme härtet, wie man Backups richtig macht und so weiter. Dafür braucht man keinen Bachelor oder Master. Und wir müssen hier weit über Bedarf ausbilden. Es ist ein recht attraktiver Beruf, der meist gut bezahlt wird, und es gibt eine internationale Nachfrage. Ich glaube, das ist ein Weg. Der andere Punkt ist, sich zu überlegen, welche skalierenden Dienstleistungen Landesbehörden oder Landesbehörden in Verbindung mit Bundesbehörden für KMUs anbieten können.

Was heißt das?
– Ich habe eine Behörde, ich habe viele Kommunen und zehntausende von KMUs im Bundesland. Wie schaffe ich es, dass alle von der IT-Sicherheit der Behörde profitieren? Dabei fallen mir vor allem zentrale Dienstleistungen ein, die mit wenig Aufwand von KMUs und Kommunen in Anspruch genommen werden können. Deren IT-Sicherheit würde sich signifikant erhöhen, verglichen damit, wenn sie selbst für die Sicherheit sorgen müssten. Das kann der Betrieb von einzelnen Anwendungen, Websites und Sicherheitsmaßnahmen, aber auch von ganzen IT-Infrastrukturen sein.

Und diese Dienstleister müssen nicht staatlich sein?
– Nein, der Staat muss nur die Rahmenbedingungen schaffen, damit diese Dienstleister gut funktionieren, und ihnen im Zweifelsfall auf die Finger schauen. Natürlich können und sollen die Behörden dort, wo sie können, unterstützen, zum Beispiel mit Warnungen und technischem Wissen.

Bei der Stiftung Neue Verantwortung sind Sie Leiter für Cybersicherheitspolitik und Resilienz. Was versteht man unter Cyberresilienz?
– Im Bereich der IT-Sicherheit verstehen wir darunter ein erweitertes Notfallmanagement. Früher hieß es, man müsse seine Systeme und Netzwerke sicher machen, und dann sei es gut, heute lautet das Paradigma „Assume Breach“: Wir müssen davon ausgehen, dass unsere IT-Netzwerke irgendwann kompromittiert werden – dafür brauchen wir einen Notfallplan. Resilienz ist das, was nach einer Kompromittierung seine Schutzwirkung entfaltet. Wie gehe ich mit einem solchen Vorfall um? Zusammengefasst gibt es hier vier Komponenten: erstens antizipieren, was bei mir passieren kann. Das Zweite ist das, was man Mitigation nennt. Das heißt, ich muss lernen, den Schaden, den ich im Falle einer Kompromittierung meines Netzes habe, so gering wie möglich zu halten. Der dritte Schritt ist, den operativen Betrieb wiederherzustellen. Der letzte Schritt besteht darin, zu überlegen, wie man gestärkt aus dem Vorfall hervorgehen kann und wie Schwachstellen behoben werden können.

Im Kampf gegen Hacker wirbt die Bundesregierung für Grundgesetzänderungen und die Bündelung der Zuständigkeiten auf Bundesebene. Ist das notwendig?
– Wir diskutieren seit einigen Jahren über die Ausweitung der Befugnisse von Sicherheitsbehörden, um Cyberoperationen – auch im Ausland – abzuwehren. Das Innenministerium hat aber bis heute weder vorgelegt, was genau für Befugnisse vergeben werden sollen, noch welche Kontroll- und Schutzmaßnahmen damit einhergehen sollen. Im Koalitionsvertrag der Ampelkoalition wird eine Überwachungsgesamtrechnung angestrebt. Das bedeutet, dass sich die Bundesregierung dazu verpflichtet, eine Übersicht über alle Überwachungsbefugnisse anzufertigen, bevor sie weitere Überwachungsbefugnisse schafft. Im Koalitionsvertrag steht außerdem, dass die Bundesregierung keine Hackbacks – je nach Auslegung eine besonders intrusive Form von Abwehrbefugnissen – vornehmen will. Auf eine Anfrage des Bundestags an die aktuelle Bundesregierung, was unter dem Begriff „Hackback“ zu verstehen ist, wurde geantwortet, dass der Begriff konzeptionell grundsätzlich nicht verwendet wird. Dass eine Bundesregierung den Begriff „Hackback“ nicht verwendet, weil er aus der aktivistischen Szene kommt, ist verständlich. Aber spätestens wenn ich einen Koalitionsvertrag unterschreibe, in dem dieses Wort vorkommt, sollte ich auch eine Definition dafür haben. Und diese Definition ist die amtierende Regierung bis heute schuldig geblieben. Außerdem hat das Innenministerium leider bis heute nicht erläutert, welche Cyberoperationen gegen die deutsche Gesellschaft, Industrie und Behörden nicht mit den bereits bestehenden Befugnissen abwehrbar sind. Das muss aber vorher geklärt werden, bevor wir Grundgesetzänderungen vornehmen. Ich würde die Änderungen auch gar nicht pauschal ablehnen. Aber solange noch so viele Dinge offen sind, halte ich es aus meinem Demokratieverständnis her für problematisch, das Grundgesetz anzufassen.

Das Interview führte Lorenz Abu Ayyash am 5. Mai 2023 in Bonn.

SVEN HERPIG
ist Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung (SNV).
sherpig@stiftung-nv.de

WUNDERWAFFEN UND WIRKLICHKEIT

Russlands Cyberkrieg gegen die Ukraine

Lennart Maschmeyer

Zeitgleich mit dem Aufmarsch russischer Truppen an der Grenze zur Ukraine ab Ende 2021 mehrten sich die Warnungen vor einem Cyberkrieg. Das „Handelsblatt" meldete Anfang Februar 2022, dass Russland sich „auch auf Cyberattacken gegen die Ukraine vorbereitet – als Teil einer hybriden Kriegsführung".[01] Der „Tagesspiegel" titelte am 25. Februar 2022, einen Tag nach Beginn des Angriffskrieges, die Bundesregierung sehe „Alarmstufe Rot" und befürchte einen „Cyberkrieg zwischen Russland und dem Westen".[02] Diese Warnungen spiegeln die tiefe Angst vor dem Schreckgespenst des „hybriden Krieges": eine vermeintlich neue Form der Kriegsführung, die Mittel wie verdeckte Operationen, Desinformationskampagnen und Cyberoperationen mit bisher nicht gekannter Effektivität kombiniert.[03] Durch den Einsatz dieser neuen Mittel, so die Annahme, können Staaten strategische Ziele erreichen, die bisher der konventionellen Kriegsführung vorbehalten waren.[04] Insbesondere das seit nunmehr zwei Jahrzehnten vor allem in Medienberichten heraufbeschworene Szenario eines Cyberkrieges – großflächige Cyberangriffe auf kritische Infrastrukturen und Finanzsysteme – weckt Ängste vor einer diffusen, aber existenziellen Bedrohung.[05]

Die Ukraine ist seit 2014 Hauptschauplatz dieser hybriden Kriegsführung und gilt weithin als „Testlabor für Russlands Cyberwaffen".[06] Die Cyberoperationen boten Russland aber kaum messbaren strategischen Nutzen.[07] Russland ist es in acht Jahren hybrider Kriegsführung nicht gelungen, sein Kernziel zu erreichen: die Ukraine von ihrer westlich orientierten Außenpolitik abzubringen und die Unterstützung der ukrainischen Bevölkerung für diese Politik zu untergraben. Daher folgte im Februar 2022 die Invasion. Mit Russlands Eskalation der Mittel ging auch eine Eskalation der Ziele einher, nämlich die Unterwerfung der Ukraine – oder, mit den Worten Wladimir Putins: „Entnazifizierung" und „Entmilitarisierung".[08] Dies schließt auch einen Regimewechsel ein, wie Russlands Außenminister Sergei Lawrow im April 2022 klarstellte.[09] Darüber hinaus verfolgt Russland eine territoriale Expansion und hat bereits Provinzen annektiert, die es – in einigen Fällen nur teilweise – besetzt hatte. Um dieses Ziel zu erreichen, sind Russlands Streitkräfte das wichtigste Instrument, aber auch Cyberoperationen sollen eine entscheidende Rolle spielen.

CYBEROPERATIONEN ALS MITTEL DER SUBVERSION

Viele Forschungsberichte deuten darauf hin, dass Cyberoperationen eher ineffektive Mittel der Gewaltanwendung sind.[10] Deshalb hat es bisher auch keinen Cyberkrieg gegeben, und das wird höchstwahrscheinlich auch so bleiben.[11] Cyberoperationen sind in erster Linie Instrumente des Konflikts niedriger Intensität und am ehesten als Mittel der Subversion zu verstehen.[12] Subversion ist ein verdecktes und indirektes Machtinstrument, das Schwächen in einer bestehenden Ordnung ausnutzt, um dem politischen Gegner zu schaden. Es ist zum Beispiel ein Mittel in Geheimdienstoperationen, findet also im Schatten der offiziellen Machtpolitik statt.[13] Bei der traditionellen Subversion werden Spione gegen soziale Systeme eingesetzt, also gegen Organisationen, Institutionen und Gesellschaften. Cyberoperationen haben es hingegen auf gegnerische Computersysteme abgesehen. Die Systeme, gegen die sich die Subversionen richten, unterscheiden sich, doch die Mechanismen der Ausnutzung und Manipulation folgen derselben Logik.[14]

In der Theorie ist Subversion die perfekte Waffe. Sie ist ein billiges, einfaches und wirksames Mittel zur Einmischung in die Angelegenheiten des Gegners und kann bei geringeren Kosten und Risiken kriegsähnliche Ergebnisse erzielen. Subversion kann sowohl als eigenständiges Instrument als auch zur Unterstützung anderer Machtinstrumente, etwa Gewalt, eingesetzt werden. In der Praxis ist sie jedoch selten erfolgreich, weil eine Reihe von

operationellen Herausforderungen die Geschwindigkeit, Intensität und Kontrolle stark einschränkt. Es ist äußerst schwierig, unentdeckt in gegnerische Systeme einzudringen und diese dann so zu manipulieren, dass sie Effekte erzeugen, die von ihren Entwicklern und Nutzern nicht beabsichtigt waren, die aber dennoch den eigenen Erwartungen entsprechen – ohne dass der politische Gegner dies bemerkt.

Diese Herausforderungen führen zu einem Trilemma: Je mehr man versucht, eine der drei Variablen – Geschwindigkeit, Intensität und Kontrolle – zu verbessern, desto mehr verschlechtern sich die anderen. Geschwindigkeit steht für die Zeit, die von der Planung der Operation bis zum Eintreten ihrer Wirkung vergeht. Intensität steht für den Umfang als auch das Ausmaß der Effekte. Und Kontrolle steht für die Fähigkeit, die durch die Operation erzeugten Effekte zu steuern und beherrschen. Wird zum Beispiel nur wenig Zeit in die Operation investiert, werden ihre Effekte weniger intensiv und weniger kontrollierbar. Aufgrund dieser Einschränkungen ist Subversion in der Praxis oft zu langsam, zu schwach oder zu unberechenbar, um strategische Ziele zu erreichen oder einen größeren Beitrag zu deren Erreichung zu leisten. Das Gleiche gilt für Cyberoperationen – und diese Einschränkungen sind in der Ukraine deutlich erkennbar.

WIPER UND DDOS

Russlands Cyberoffensive 2022 begann mit einer Drohung. Am 14. Januar wurden Besucherinnen und Besucher von rund 70 Websites ukrainischer Regierungsbehörden mit einer beunruhigenden Nachricht konfrontiert: „Alle Informationen über Sie sind öffentlich gemacht worden, haben Sie Angst und erwarten Sie das Schlimmste."[15] Medienberichten zufolge handelte es sich um einen massiven Cyberangriff.[16] Wie das ukrainische Computernotfallteam jedoch klarstellte, waren weder staatliche noch persönliche Daten betroffen – die Hacker hatten nur Zugriff auf die Content-Management-Systeme der Websites erlangt.[17] Angriffe dieser Art werden als *website defacements* (Website Entstellungen) bezeichnet. Spätere Untersuchungen brachten diese Operation mit einer belarussischen Hackergruppe in Verbindung.[18]

01 Teresa Stiens et al., Militäreinsatz und Cyberattacken: Experten warnen vor Doppelschlag Russlands, 7.2.2022, www.handelsblatt.com/28045348.html.

02 Frank Jansen/Jens Ohlig, Bundesregierung sieht „Alarmstufe Rot". Cyberkrieg zwischen Russland und dem Westen droht, 25.2.2022, www.tagesspiegel.de/politik/cyberkrieg-zwischen-russland-und-dem-westen-droht-4311196.html.

03 Vgl. Frank G. Hoffman, Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict, in: Strategic Forum 240/2009, https://apps.dtic.mil/dtic/tr/fulltext/u2/a496471.pdf.

04 Vgl. Christopher S. Chivvis, Hybrid War: Russian Contemporary Political Warfare, in: Bulletin of the Atomic Scientists 5/2017, S. 316–321.

05 Siehe etwa Jason Ryan, CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor, 11.2.2011, https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905; John Arquilla, Cyberwar is Already Upon Us, 27.2.2012, https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us; Benjamin Mueller, Why We Need a Cyberwar Treaty, 2.6.2014, www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty.

06 Andy Greenberg, How an Entire Nation Became Russia's Test Lab for Cyberwar, 20.6.2017, www.wired.com/story/russian-hackers-attack-ukraine; Oliver Fitton, Cyber Operations and Gray Zones: Challenges for NATO, in: Connections 2/2016, S. 109–119.

07 Vgl. Lennart Maschmeyer, The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations, in: International Security 2/2021, S. 51–90.

08 Zit. nach Andrew Osborn/Polina Nikolskaya, Russia's Putin Authorises „Special Military Operation" Against Ukraine, 24.2.2022, www.reuters.com/world/europe/russias-putin-authorises-military-operations-donbass-domestic-media-2022-02-24.

09 Vgl. Susie Blann, Russia Says It Wants to End Ukraine's „Unacceptable Regime", 25.7.2022, https://apnews.com/article/russia-ukraine-zelenskyy-kyiv-black-sea-arab-league-b5c583e8d057897cfdef6b407e113339.

10 Vgl. Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, in: Security Studies 3/2013, S. 365–404; Erica D. Borghard/Shawn W. Lonergan, Cyber Operations as Imperfect Tools of Escalation, in: Strategic Studies Quarterly 3/2019, S. 122–145.

11 Vgl. Thomas Rid, Cyber War Will Not Take Place, Oxford 2013.

12 Vgl. Maschmeyer (Anm. 7); ders., A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict, in: Journal of Strategic Studies 2022, https://doi.org/10.1080/01402390.2022.2104253.

13 Vgl. Paul W. Blackstock, The Strategy of Subversion. Manipulating the Politics of Other Nations, Chicago 1964.

14 Vgl. Lennart Maschmeyer, Subversion, Cyber Operations, and Reverse Structural Power in World Politics, in: European Journal of International Relations 1/2023, S. 79–103.

15 Zit. nach Kim Zetter, What We Know and Don't Know about the Cyberattacks Against Ukraine – (Updated), 17.1.2022, https://zetter.substack.com/p/what-we-know-and-dont-know-about.

16 Vgl. Luke Harding, Ukraine Hit by „Massive" Cyber-Attack on Government Websites, 14.1.2022, www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

17 Vgl. Computer Emergency Response Team of Ukraine, Fragment einer Cyberangriffsforschung 14.01.2022 [aus dem Ukrainischen], 26.1.2022, https://cert.gov.ua/article/18101.

18 Vgl. Pavel Polityuk, Ukraine Suspects Group Linked to Belarus Intelligence over Cyberattack, 16.1.2022, www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15.

Forensische Daten deuten auf eine eher kurze Vorbereitungszeit von nur wenigen Wochen hin.[19] Diese Operation verlief also relativ schnell, geriet nicht außer Kontrolle, erzielte aber auch so schwache Effekte, dass sie strategisch irrelevant blieb. Betroffene Websites wurden bald wiederhergestellt, und öffentliche Panik brach auch nicht aus.

Es folgte eine Welle sogenannter Wiper – das sind Viren, die alle Daten auf infizierten Systemen löschen. Operation WhisperGate machte Mitte Januar 2022 den Anfang. Ihr Ziel waren mehrere ukrainische Ministerien, die bereits von den *website defacements* betroffen waren. Der Mechanismus der Datenzerstörung funktionierte ähnlich wie bei der Operation NotPetya von 2017. Während jedoch Letztere große Teile der ukrainischen Wirtschaft lahmlegte, waren bei WhisperGate nur eine Handvoll Regierungssysteme betroffen.[20] Gleichzeitig gibt es keine Berichte oder Hinweise auf eine Störung der ukrainischen Regierung. Vermutlich hatten die Angegriffenen ein effektives Gegenmittel: Backups. Das geringe Ausmaß von WhisperGate im Vergleich zu NotPetya ist das Resultat des manuellen Ausbreitungsmechanismus. NotPetya verbreitete sich automatisch und weltweit. Bei WhisperGate mussten die Hacker hingegen jedes System einzeln infiltrieren.[21] Das erhöhte zwar die Kontrollmöglichkeit, verringerte aber das Ausmaß der Effekte auf die Ukraine. Forensische Daten deuten auf bis zu neun Monate Vorbereitungszeit hin,[22] drei Monate länger als für die Entwicklung von NotPetya.[23] Kurzum, diese Operation war relativ schnell geplant, gut kontrollierbar, aber von so geringer Intensität, dass sie strategisch irrelevant blieb.

Einen Monat später folgte die nächste Operation, ein sogenannter DDoS-Angriff (Distributed Denial of Service). Bei dieser Technik werden Systeme durch eine Vielzahl von Anfragen überlastet und so für die Nutzer unerreichbar gemacht. Hinter dem Angriff steckte der russische Militärgeheimdienst GRU.[24] Am 15. Februar 2022 wurden die Server mehrerer Ministerien und Banken mit dieser Technik für Stunden überlastet. Auch Geldautomaten waren davon betroffen.[25] Es entstand zwar ein wirtschaftlicher Schaden, Panik in der Bevölkerung blieb jedoch aus. Medienberichten zufolge beliefen sich die Kosten auf mehrere Millionen US-Dollar. Die betroffenen Unternehmen und ihre Kunden blieben entspannt, der Service wurde rasch wiederhergestellt.[26] Strategisch blieb auch dieser Einsatz ohne Bedeutung.

Die Invasion selbst begann am 24. Februar 2022 und wurde von mehreren Cyberoperationen begleitet. Zunächst erfolgte erneut ein DDoS-Angriff, und zwar mit derselben Technik gegen dieselben Ziele wie neun Tage zuvor.[27] Es gibt keine Berichte über nennenswerte Auswirkungen. Die Ukrainerinnen und Ukrainer hatten offensichtlich aus früheren Cyberoperationen gelernt und konnten entsprechend schnell Gegenmaßnahmen einleiten, die den Schaden auf ein Minimum reduzierten.[28]

Gleichzeitig wurde ein neuer Wiper mit dem Namen HermeticWiper aktiv, der laut der Cybersecurity-Firma ESET einige hundert Systeme der ukrainischen Regierung lahmlegte.[29] Wie sein Vorgänger WhisperGate löschte auch HermeticWiper Daten unwiederbringlich, hatte aber

19 Vgl. Microsoft, Destructive Malware Targeting Ukrainian Organizations, 15.1.2022, www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations.

20 Vgl. Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, 22.8.2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world. Siehe hierzu auch den Beitrag von Eva Wolfangel in dieser Ausgabe (*Anm. d. Red.*).

21 Vgl. Secureworks, WhisperGate: Not NotPetya, 21.1.2022, www.secureworks.com/blog/whispergate-not-notpetya.

22 Vgl. Cisco Talos, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, 21.1.2022, https://blog.talosintelligence.com/ukraine-campaign-delivers-defacement.

23 Vgl. Maschmeyer (Anm. 7), S. 71.

24 Vgl. Adrienne Watson, Tweet vom 18.2.2022, https://twitter.com/NSC_Spox/status/1494796573959725057.

25 Vgl. Katerina Kuznetsova, „PrivatBank" und „Oschadbank" nehmen nach der zweiten großen Cyberattacke ihren Betrieb wieder vollständig auf [aus dem Ukrainischen], 16.2.2022, https://tsn.ua/ukrayina/privatbank-ta-oschadbank-povnistyu-vidnovili-robotu-pislya-drugoyi-potuzhnoyi-kiberataki-1979029.html.

26 Vgl. ukrainische Nachrichtenportale: Dana Gordiichuk, Cyberattacke für Millionen von Dollar: Russland könnte hinter dem Angriff stecken, 16.2.2022, www.epravda.com.ua/news/2022/02/16/682428; Kateryna Kuznetsova, Der mächtigste Cyberangriff in der Geschichte der Ukraine: das Ziel der Hacker, wer wird verdächtigt und was sind die Folgen für den Staat, 17.2.2022, https://tsn.ua/ukrayina/naypotuzhnisha-kiberataka-za-vsyu-istoriyu-ukrayini-cil-hakeriv-kogo-pidozryuyut-i-yaki-naslidki-dlya-derzhavi-1979239.html.

27 Vgl. Lauren Feiner, Cyberattack Hits Ukrainian Banks and Government Websites, 23.2.2022, www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html.

28 Vgl. Oksana Orsach, Kabinetts-Webseiten lassen sich nicht öffnen – Finanzministerium meldet massiven DDoS-Angriff [aus dem Russischen], 23.2.2022, https://nikcenter.org/newsItem/65950.

29 Vgl. ESET Research, Tweet vom 23.2.2022, https://twitter.com/ESETresearch/status/1496581903205511181.

ebenfalls keine messbaren Auswirkungen auf das Funktionieren der ukrainischen Regierung und ihre Fähigkeit, sich gegen die russischen Invasoren zu wehren.[30] Allerdings wurden mehr Systeme als beim Vorgänger infiziert, da HermeticWiper darauf programmiert war, sich in lokalen Netzwerken automatisch zu verbreiten.[31] Dementsprechend brauchte die Operation mit nur zwei Monaten eine deutlich kürzere Vorbereitungszeit.[32] Trotz dieser effizienteren Vorgehensweise blieb ein strategisch relevanter Effekt aus.

Ähnliches gilt für IsaacWiper und CaddyWiper, die in den darauffolgenden Wochen erschienen und ebenfalls keinen messbaren strategischen Nutzen brachten. IsaacWiper hatte etwa die gleiche Reichweite wie HermeticWiper, während CaddyWiper nur einige Dutzend Systeme betraf.[33] Für keine der beiden Operationen gibt es Hinweise auf spürbare Auswirkungen auf die ukrainische Regierung, das öffentliche Leben oder die ukrainische Wirtschaft. Gleiches gilt für die Schadsoftware RansomBoggs und Prestige, die erstmals im Herbst 2022 in Erscheinung traten.[34]

VIASAT UND UKRTELECOM

Die genannten Operationen spielten alle eine strategische Rolle, die nicht unmittelbar mit den Kriegshandlungen verknüpft waren. Der russische Hack gegen das Satellitennetzwerk KA-SAT des Anbieters Viasat war hingegen ein Versuch, den russischen Streitkräften Vorteile auf dem Schlachtfeld zu verschaffen. Der KA-SAT-Dienst wird von tausenden Kunden in Europa genutzt, darunter auch vom ukrainischen Militär. Pünktlich zum Beginn der Invasion, am frühen Morgen des 24. Februars, brach dieser Service zusammen.[35] Victor Zhora vom Staatlichen Dienst für Sonderkommunikation und Informationsschutz in der Ukraine (SSSCIP) sprach zunächst von einem „riesigen Kommunikationsverlust" für die Armee.[36] Später machte er jedoch deutlich, dass der Satellitenhack kaum Auswirkungen auf das militärische Geschehen gehabt hätte, weil der Armee alternative Kommunikationskanäle zur Verfügung gestanden hätten.[37] Zwar lässt sich dies nicht unabhängig überprüfen, es deckt sich aber mit dem Kriegsverlauf. Die materiell weit unterlegene ukrainische Armee hielt dem russischen Angriff deutlich besser stand, als von den meisten Militärexperten vorhergesagt.[38] Mit einem großflächigen Kommunikationszusammenbruch wäre dies kaum möglich gewesen.

Diese Operation hatte gleichwohl wesentlich intensivere Effekte als die bisher diskutierten, nämlich Schäden an physischen Geräten. Sie erforderte daher erwartungsgemäß eine längere Vorbereitungszeit, wahrscheinlich mindestens ein Jahr,[39] und gleichzeitig ein höheres Risiko des Kontrollverlustes. Dennoch scheint die Operation die gewünschte Wirkung auf das Ziel selbst verfehlt und erhebliche Kollateralschäden verursacht zu haben. Betroffen waren nicht nur KA-SAT-Nutzer in der Ukraine, sondern in ganz Europa. Zu diesen gehörte etwa auch der deutsche Hersteller von Windenergieanlagen Enercon, der den Kontakt zu tausenden Windrädern verlor. Die durch den Hack beschädigten Satellitenmodems mussten teuer ersetzt werden.[40] Dieses Er-

30 Vgl. J.A. Guerrero-Saade, Tweet vom 23.2.2022, https://twitter.com/juanandres_gs/status/1496607141888724997.

31 Vgl. ESET Research, IsaacWiper and HermeticWizard: New Wiper and Worm Targeting Ukraine, 4.3.2022, www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine.

32 Vgl. dass., Tweet vom 23.2.2022, https://twitter.com/ESETresearch/status/1496581904916754435.

33 Vgl. dass., Tweet vom 14.3.2022, https://twitter.com/ESETresearch/status/1503436423818534915.

34 Vgl. Natalia Zarudnia, Russische Ransomware RansomBoggs zielt auf mehrere ukrainische Organisationen [aus dem Ukrainischen], 30.11.2022, https://cybercalm.org/novyny/rosijska-programa-vymagach-ransomboggs-natsilylasya-na-kilka-ukrayinskyh-organizatsij; Microsoft Threat Intelligence, New „Prestige" Ransomware Impacts Organizations in Ukraine and Poland, 14.10.2022, www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland.

35 Vgl. NetBlocks, Tweet vom 28.2.2022, https://twitter.com/netblocks/status/1498365220107997191.

36 Zit. nach Raphael Satter, Satellite Outage Caused „Huge Loss in Communications" at War's Outset – Ukrainian Official, 15.3.2022, www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15.

37 Vgl. Kim Zetter, Viasat Hack „Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says, 26.9.2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.

38 Vgl. BBC, Ukraine Tensions: US Sources Say Russia 70% Ready to Invade, 6.2.2022, www.bbc.com/news/world-europe-60276342.

39 Vgl. Yaroslav Kucher, Wie wir die Verbindung halten konnten, Cyberangriffe auf die Ukraine, Militärsatelliten blockiert [aus dem Ukrainischen], 18.6.2022, www.youtube.com/watch?v=-K9OyhGWDRI.

40 Reuters, Satellite Outage Knocks out Thousands of Enercon's Wind Turbines, 28.2.2022, www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28.

gebnis unterstreicht die Unberechenbarkeit von Cyberoperationen, vor allem wenn sie das Ausmaß von Effekten maximieren. Nach derzeitigem Kenntnisstand hat die Operation keinen strategischen Vorteil für Russland gebracht, dafür aber Kollateralschäden für Dritte.

Eine andere, vermutlich von Russland gesponserte, Cyberoperation hatte jedoch einen klaren strategischen Nutzen: Am 28. März 2022 waren die meisten User des ukrainischen nationalen Anbieters Ukrtelecom 15 Stunden lang vom Internet abgeschnitten.[41] Dieser Ausfall hatte nicht nur erhebliche wirtschaftliche Schäden zur Folge, sondern wirkte sich auch massiv auf den Alltag der Ukrainerinnen und Ukrainer aus. Es existieren keine genauen Angaben, doch allein der wirtschaftliche Schaden dürfte im zweistelligen Millionenbereich (US-Dollar) liegen. Die Operation gelang mit nur einem Monat Vorbereitungszeit. Hatten die Hacker also einen genialen Ausweg aus dem Trilemma gefunden? Keineswegs: Wie eine spätere Untersuchung des SSSCIP feststellte, nutzten die Hacker eine Schwachstelle aus, die erst durch die Invasion entstanden war: Die Infrastruktur von Ukrtelecom befand sich in den von Russland eroberten Gebieten. Die Hacker, beziehungsweise russische Sicherheitskräfte, hatten so direkten Zugang auf das interne Netzwerk und setzten einen Ukrtelecom-Mitarbeiter so unter Druck, dass er die entsprechenden Zugangsdaten preisgab.[42]

SCHLUSS

Mit Ausnahme des Viasat-Hacks spielten die Cyberoperationen gegen die Ukraine in erster Linie eine von der Invasion unabhängige strategische Rolle. Die meisten Cyberoperationen basierten auf relativ schnellen und einfach anzuwendenden Techniken. Die Hacker maximierten die Geschwindigkeit und versuchten, die Auswirkungen zu kontrollieren. Dies ging zulasten der Intensität. Dementsprechend richteten die Operationen – zumindest nach bisherigen Erkenntnissen – kaum Schäden an oder trugen zur Erreichung der Kriegsziele bei.[43] Die einzigen bisher messbaren Schäden sind (begrenzte) wirtschaftliche Verluste und vorübergehende Beeinträchtigungen für Internetnutzerinnen und -nutzer. Die Unterbrechung des Satellitennetzwerkes KA-SAT stellt eine Ausnahme dar und könnte der russischen Armee taktische Vorteile verschafft haben. Der Kriegsverlauf stellt dies jedoch infrage.

Gerade wenn es um die Zerstörung kritischer Infrastruktur geht, sind klassische Gewaltmittel – Artillerie, Bomben und Marschflugkörper – noch immer effektiver. Aber es sind nicht nur diese brachialen Mittel, die Cyberoperationen in den Schatten stellen, sondern auch traditionelle subversive Operationen. Das ist wichtig, denn in der medialen Berichterstattung stehen die Gefahren des Cyberkrieges auch für Deutschland nach wie vor im Mittelpunkt. Natürlich ist Cyberabwehr wichtig und notwendig, und Deutschland hat hier Nachholbedarf, aber die Erfahrungen aus der Ukraine zeigen, dass die Gefahr für die nationale Sicherheit relativ gering ist. Ganz anders sieht es bei der klassischen Subversion wie Sabotageakten aus. In den vergangenen Monaten haben sich die Hinweise verdichtet, dass Deutschland seit Jahren Ziel koordinierter Kampagnen ist, die Schlüsselpositionen in Ministerien, Politik und sogar Nachrichtendiensten infiltriert und manipuliert haben und mit hoher Wahrscheinlichkeit zu politischen Ergebnissen im Interesse Russlands beigetragen haben, wie etwa dem Bau der Pipeline Nord Stream 2.[44] Der großflächige Ausfall der Deutschen Bahn durch einfache Sabotage im Oktober 2022 hat unterdessen gezeigt, welche fatalen Auswirkungen solche traditionellen Mittel haben können – auch wenn hier offenbar kein staatlicher Akteur beteiligt war.

LENNART MASCHMEYER
ist wissenschaftlicher Mitarbeiter am Center for Security Studies (CSS) der ETH Zürich.
lennart.maschmeyer@sipo.gess.ethz.ch

41 Vgl. Melanie Mingas, Ukrtelecom Restores 85 % of Services after „Powerful Cyberattack", 29.3.2022, www.capacitymedia.com/article/29wch971qqy0z3dyifx8g/ukrtelecom-restores-85-of-services-after-powerful-cyberattack.

42 Vgl. State Service of Special Communications and Information Protection of Ukraine, Cyberattack Against Ukrtelecom on March 28: The Details, 6.4.2022, https://cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali.

43 Dies kann sich selbstverständlich noch ändern, wenn mehr Daten zur Verfügung stehen. Zur Zeit sind nur drei der Operationen – die DDoS-Attacken, CaddyWiper und Viasat – relativ sicher Russland zugeschrieben worden.

44 Vgl. Holger Stark, Russischer Spion: Hintermann in der BND-Spionageaffäre festgenommen, 26.1.2023, www.zeit.de/politik/2023-01/russischer-spion-bnd-mittaeter-carsten-l; Maik Baumgärtner et al., Hacker, Spione, Killer: Wie die Agenten von Wladimir Putin Deutschland unterwandern, in: Der Spiegel 35/2022.

SICHERHEITSLOGIK DER CYBERDOMÄNE

Matthias Schulze

Sicherheitspolitik ist nie statisch, da sich Bedrohungen, Akteure, Technologien, aber auch die Parameter der Umwelt stets verändern. Nationale Sicherheitsstrategien müssen für eine größtmögliche Übereinstimmung zwischen staatlichem Handeln und den Bedingungen der Umwelt sorgen. Eine Nichtübereinstimmung kann fatale Folgen haben. Beispiele für veränderte Sicherheitsparameter sind die Erfindung des Maschinengewehrs und des Stacheldrahts im 19. Jahrhundert. Bevor diese Technologien erfunden wurden, herrschte in vielen Streitkräften ein impliziter „Kult der Offensive", eine Strategie, die auf Initiative und Angriffe setzte. Noch in den Napoleonischen Kriegen zu Beginn des 19. Jahrhunderts galt, dass Schlachten durch koordinierte Manöver angreifender Soldatenmassen, auch unter Einsatz der Kavallerie, zu gewinnen seien.[01] Irgendwann kollidierte diese Annahme mit der veränderten technologischen Realität, dass ein Anstürmen auf Artillerie- und Maschinengewehrbefestigungen zu katastrophalen Verlusten führt. Die Parameter der strategischen Umwelt hatten sich durch Technologien von der Offensive zugunsten der Defensive verändert.[02]

Die Erfindung von Nuklearwaffen und Interkontinentalraketen veränderte die strategische Umwelt erneut. Gegen diese Waffen gab und gibt es keine sinnvollen Verteidigungsmöglichkeiten. Die Defensive war auf einmal wieder im Nachteil, und die Offensive, in Form von Erstschlägen, hatte zumindest theoretische Vorteile. Die Sicherheitsstrategie der Abschreckung durch die Androhung von Vergeltung (*deterrence by punishment*) kompensierte diese Lücke, indem sie eine Pattsituation des Gleichgewichts des Schreckens entstehen ließ, welche die Offensivvorteile neutralisierte.

Für die Cybertheoretiker Michael P. Fischerkeller, Emily O. Goldman und Richard J. Harknett stellen das Internet und der globale Cyber- und Informationsraum eine völlig neue strategische Umwelt zwischenstaatlicher Machtausübung dar, in der die alten Paradigmen der konventionellen und nuklearen Domäne nicht mehr gelten.[03] Die Charakteristika des Cyberspace erfordern ein neues strategisches Denken.

CYBERKONFLIKTE

Auseinandersetzungen im Cyberspace haben nur wenig mit den Merkmalen klassischer Kriege zu tun. Das Gros der Aktivität von Cyberoperationen lässt sich dem Bereich Cyberkriminalität zuordnen. Hierbei ist das Ziel nicht, einen Gegner militärisch niederzuringen, sondern Geld zu verdienen, etwa durch Erpressung mit Ransomware oder Phishing von Zugangsdaten. Eine Subkategorie von Cyberkriminalität ist Hacktivismus, der sich insbesondere im Kontext des russischen Angriffskrieges gegen die Ukraine zeigt: Aktivisten nutzen temporär störende DDoS-Angriffe (Distributed Denial of Service), um Dienste und Webserver zum Beispiel für das Onlinebanking zeitlich begrenzt lahmzulegen. Die Effekte sind meist reversibel und somit relativ geringfügig.[04] Auch Staaten nutzen die Strategien der Cyberkriminalität. Nordkorea ist bekannt dafür, im staatlichen Auftrag alles zu hacken, womit sich im Internet Geld verdienen lässt, um den Staatshaushalt zur Finanzierung des eigenen Nuklearprogramms aufzubessern.[05]

Daneben ist Cyberspionage mit politischen oder wirtschaftlichen Zielen eines der häufigsten Phänomene im Cyberspace. Durch den systematischen Diebstahl geistigen Eigentums mittels Cyberkampagnen, also mehrere aufeinander aufbauende Cyberoperationen etwa gegen zentrale Unternehmen eines Wirtschaftszweiges, können Staaten ihre Machtressourcen vergrößern. Chinesische Akteure betreiben sehr intensiv Cyberspionage in Sektoren, in denen China bis 2025 weltweit führend oder von westlichen Technologien unabhängig sein will, darunter Künstliche Intelligenz, autonomes Fahren, Luftfahrt, Fotovoltaik, Halbleitertechnologie und vieles mehr. Exemplarisch sind Spionageoperationen gegen Unternehmen wie Solarworld, deren Solarpanel-Techno-

logie gestohlen und kurz darauf in chinesischen Produkten auftauchte. Dies drängte Solarworld aufgrund günstigerer Preise aus dem Markt.[06] China ist heute Weltmarktführer in der Produktion von Solarpanels und kann dies als Machtmittel gegenüber dem Westen einsetzen.[07] Hier zeigt sich wie durch Cyberoperationen strategische Gewinne erzielt und Machtbalancen verschoben werden können.

In den vergangenen Jahren zeigte sich zudem, dass der Cyber- und Informationsraum eine geeignete Domäne für Subversionskampagnen ist, die darauf abzielen, das politische System in anderen Ländern zu beeinflussen. Diese Strategie, die Teil der hybriden Kriegsführung ist, wird etwa von Russland eingesetzt. Ein Beispiel dafür ist die Beeinflussung der US-Wahlen 2016 durch eine „Hack and Leak"-Operation, bei der interne E-Mails der US-Demokraten veröffentlicht wurden, um diesen zu schaden.[08] Insbesondere autoritäre Staaten machen sich Tools zur Manipulation von Internetinhalten zur Konsolidierung ihrer Macht zunutze.[09]

Statistisch gesehen sind Cyberkriminalität, Hacktivismus, politische und wirtschaftliche Spionage sowie Informationsoperationen die häufigsten Anwendungsfelder von Cyberoperationen.[10] Militärische Cyberoperationen, die etwa darauf abzielen, Zielgeräte zu hacken und zu zerstören, kommen zwar vor, sind aber selten. Prominent zu nennen sind die Operationen Stuxnet, Industroyer und Industroyer2 sowie der Viasat-Hack im Kontext der russischen Invasion 2022.[11] Hierbei wurden tatsächlich physische Effekte hervorgerufen und Computer-Hardware beziehungsweise im Falle Stuxnets und Industroyer auch industrielle Steuerungsanlagen sabotiert und beschädigt.[12] Dennoch ist der empirische Befund relativ deutlich: Die große Mehrzahl aller Cyberoperationen entspricht nicht der Logik militärischer Gewalt- und Zwangsausübung und ist deshalb völkerrechtlich nicht als Einsatz von Waffengewalt zu klassifizieren.[13] Aufgrund dieses Befundes sieht die Cyberkonfliktforschung die Domäne weniger als eine der militärischen Gewaltaustragung, auch wenn Cyberoperationen in Kombination mit konventioneller Waffengewalt etwa in Kriegen eingesetzt werden (können). Die Metapher des Cyberkrieges ist insofern irreführend, als sie Parameter der strategischen Umwelt des Cyberspace fehlerhaft charakterisiert.

CHARAKTERISTIKA DER CYBERDOMÄNE

Für die Cybertheoretiker Fischerkeller, Goldman und Harknett ist die strategische Umwelt des Cyberspace wie folgt gekennzeichnet: die Summe aller durch Netzwerke verbundenen Hard- und Software, die von Menschen gemacht und daher veränderbar sind.[14] Das heißt, die Akteure können und müssen die Bedingungen ihrer Sicherheit

01 Vgl. Stephen Van Evera, The Cult of the Offensive and the Origins of the First World War, in: International Security 1/1984, S. 58–107.

02 Vgl. Charles L. Glaser/Chaim Kaufmann, What is the Offense-Defense Balance and Can We Measure It?, in: International Security 4/1998, S. 44–66.

03 Vgl. Michael P. Fischerkeller/Emily O. Goldman/Richard J. Harknett, Cyber Persistence Theory. Redefining National Security in Cyberspace, Oxford 2022.

04 Vgl. Matthias Schulze, Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022, 2.5.2022, www.laender-analysen.de/ukraine-analysen/267/cyber-vorfaelle-im-krieg.

05 Vgl. ders., Cyberspace. Asymmetrische Kriegführung und digitale Raubzüge, in: Hanns Günther Hilpert/Oliver Meier (Hrsg.), Facetten des Nordkorea-Konflikts. Akteure, Problemlagen und Europas Interessen, Stiftung Wissenschaft und Politik (SWP), SWP-Studie 18/2018, S. 75–79.

06 Vgl. Diane Cardwell, Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying, 1.9.2014, www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html.

07 Vgl. Konrad Fischer, Stoppt die Abhängigkeit von China den Solarboom?, 10.8.2022, www.wiwo.de/technologie/umwelt/tracking-der-energiewende-21-stoppt-die-abhaengigkeit-von-china-den-solarboom/28575394.html.

08 Vgl. David E. Sanger, The Perfect Weapon, New York 2018.

09 Vgl. Paula Köhler/Daniel Voelsen, Content Moderation in autoritären Staaten, SWP, SWP-Aktuell 39/2022.

10 Vgl. European Repository on Cyber Incidents, Cyber Incident Dashboard. Incidents Originating in All Countries Against Global (States) Between 1.1.2000 and 28.3.2023, https://eurepoc.eu/de/dashboard.

11 Vgl. Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, in: Security Studies 3/2013, S. 365–404; Kai Biermann/Eva Wolfangel, Angriff im Rücken der ukrainischen Armee, 23.2.2023, www.zeit.de/digital/internet/2023-02/ukraine-krieg-cyberwar-hacker-viasat; Anton Cherepanov/Robert Lipovsky, Industroyer. Biggest Threat to Industrial Control Systems Since Stuxnet, 12.6.2017, www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet.

12 Vgl. Andrew C. Foltz, Stuxnet, Schmitt Analysis, and the Cyber „Use-of-Force" Debate, in: Joint Force Quarterly 67/2012, S. 40–48.

13 Vgl. European Repository on Cyber Incidents (Anm. 10).

14 Vgl. Fischerkeller/Goldman/Harknett (Anm. 3).

weitgehend selbst gestalten, indem sie ihre Hard- und Software modifizieren. Dazu gehören die Installation von Schutztechnologien für Netzwerke, die Schließung von Sicherheitslücken oder die Etablierung neuer organisatorischer Policies wie User-Rechtemanagement und Backupstrategien.

Die zentrale Dynamik von Konflikten im Cyberspace ist die Ausnutzung (*exploitation*) von Sicherheitslücken und der Versuch, diese zu schließen beziehungsweise zu verkleinern: Die Angreifer versuchen unbefugt in Systeme einzudringen und deren Vertraulichkeit, Integrität oder Verfügbarkeit zu beeinträchtigen. Die Netzwerkverteidiger versuchen hingegen, dies durch Modifikation des Terrains, also der eigenen Netzwerk- und Softwareinfrastruktur, zu vereiteln. Aufgrund dieser Dynamik ist der Cyberspace auf der Makroebene resilient – es ist schwierig, das gesamte Internet auf einmal abzuschalten – und gleichzeitig auf der Mikroebene verwundbar, da jedes einzelne System mit genügend Aufwand gehackt werden kann und nie hundertprozentig sicher ist.

Die Eintrittsbarrieren für Cyberoperationen sind niedrig: Anders als in der nuklearen Domäne können auch nicht-staatliche Akteure mit geringerem Aufwand zur Bedrohung werden und Staaten herausfordern, und das von überall auf der Welt.[15] Die grenzüberschreitende Natur führt dazu, dass der Kontakt zwischen Antagonisten, etwa staatlichen Rivalen oder Bedrohungsakteuren, permanent stattfindet und nicht etwa nur episodisch, wie im Falle von konventionellen Kriegen.

Die sogenannte Cyber-Persistenz-Theorie geht davon aus, dass die Kombination von Vernetzung und konstantem Kontakt mit dem Gegner sowie die Strukturmerkmale – wie Makro-Resilienz und Mikro-Verwundbarkeit – die Grundlage für eine bestimmte Handlungslogik bilden: Staaten und nicht-staatliche Akteure versuchen ständig, die Initiative zu ergreifen, um nicht ins Hintertreffen zu geraten – das sprichwörtliche Katz- und Maus- Spiel zwischen immer neuen Angriffstechniken und Abwehrtechnologien. So erklären sich die Autoren die Zunahme von Cyberaktivitäten am unteren bis mittleren Ende des Konfliktspektrums, also Cyberkriminalität, Subversion und Spionage.[16] Gleichzeitig erklärt sich damit auch das weitgehende Ausbleiben zerstörerischer, militärischer Cyberangriffe: Eine kumulative Strategie vieler kleiner, niedrigschwelliger Cyberoperationen ist langfristig gewinnbringender als große Cyberoperationen mit destruktiven Effekten, die nur einmal wirken.[17]

Als eine der ersten umfassenden Theorien zur Erklärung von Cyberkonflikten hat die Cyber-Persistenz-Theorie natürlich auch einige Schwachpunkte. Sie fokussiert stark auf strukturelle Merkmale und staatliches Handeln, ähnlich wie der Realismus als Theorie in den internationalen Beziehungen, an dem sie sich orientiert. Die Motive und Interessen nicht-staatlicher Akteure bleiben weitgehend unterbelichtet. Sie ist stark von rationalistischen Annahmen wie Kosten und Nutzen geprägt. Andere Faktoren, die das Verhalten von Akteuren erklären, wie Ideen, Normen und Rechte, bleiben unterbelichtet.

GEFAHRENABWEHR

Die Cyber-Persistenz-Theorie ist auch für Deutschlands nationale Sicherheitsstrategie interessant. Die erste Lehre ist: Sicherheit im Cyberspace lässt sich nur global herstellen – der Fokus auf eine rein nationale (Cyber-)Sicherheitsstrategie greift also zu kurz. Alle Beteiligten im global vernetzten Raum müssen die Bedingungen ihrer Sicherheit verbessern, damit es für jeden sicherer wird. Die Dynamik gleicht dem Problem des Klimawandels: Alle müssen ihre schädlichen Emissionen, in Form von digitalen Verwundbarkeiten und Schwachstellen, reduzieren, damit die Umwelt für alle sicherer wird.

Problematisch ist auch die unkritische Übertragung von Sicherheitskonzepten aus der nuklearen oder konventionellen Domäne auf den Cyberspace. Dazu gehört die Vorstellung, Cyberoperationen primär als Mittel militärischer Gewalt zu verstehen, mit dem der eigene politische Wille einem Gegner aufgezwungen werden kann. Das ist nach dem preußischen Generalma-

15 Vgl. Zscaler, Of Exploits and Experts: The Professionalization of Cybercrime Of Exploits and Experts, 1. 12. 2022, www.darkreading.com/zscaler/of-exploits-and-experts-the-professionalization-of-cybercrime.

16 Immer mehr Staaten nutzen Cyberoperationen zur Erlangung eigener Vorteile, etwa in Form von Überwachung fremder Regierungsnetzwerke. Siehe hierzu Cyber Arms Watch, Uncovering the Stated & Perceived Offensive Cyber Capabilities of States, The Hague Centre for Strategic Studies, Mai 2022.

17 Vgl. Daniel Moore, Offensive Cyber Operations, London 2022.

jor und Militärtheoretiker Carl von Clausewitz das primäre Ziel des (konventionellen) Krieges: den gegnerischen Willen mit Waffengewalt und Zwang zu brechen.[18] Das gesamte völkerrechtliche Instrumentarium und auch das Grundgesetz basieren auf der Annahme, militärische Gewalt begrenzen zu wollen. Deswegen gibt es eine klare, rechtliche Trennung zwischen Krieg und Frieden, ziviler Gefahrenabwehr und militärischer Landes- und Bündnisverteidigung. Dazu gehört auch das Konzept der Aufteilung der Welt in voneinander abgegrenzte Staatsterritorien, über die die Staaten souverän verfügen und äußere Einmischung verhindern wollen.[19] All diese (juristischen) Konzepte, die aus der Westfälischen Ordnung seit 1648 entspringen, sind in einem globalen Cyber- und Informationsraum nur wenig hilfreich.[20]

Die globale Natur des Cyberspace bedeutet, dass eine reine Perimeterlogik, also der Schutz durch Abschottung und Barrieren wie der Grenzschutz im konventionellen Bereich, unzureichend ist. Gleichzeitig liegt in der Interkonnektivität das größte Wertschöpfungspotenzial des Internets, weshalb Abschottung keine sinnvolle Strategie ist. Cyberoperationen können von überall auf der Welt gestartet werden, auch vom eigenen Land aus. Sie können eine nationale Perimeterverteidigung umgehen, etwa durch VPN-Tunnel. Ein Grenzschutzparadigma reicht daher nicht aus. Sicherheit muss überall im Innern der Gesellschaft stattfinden.

Zudem ist die Dichotomie zwischen Krieg und Frieden wenig hilfreich, da Cyberoperationen weder Krieg noch Frieden sind. Der Politikwissenschaftler Lucas Kello prägte hierfür den Begriff „Unfrieden".[21] Westliche Demokratien, die sich an das Völkerrecht gebunden fühlen, können daher nicht angemessen auf Cyberoperationen reagieren, da Ausnahmen vom Gewaltverbot wie das Recht auf Selbstverteidigung bei den meisten Cyberoperationen nicht greifen. Militärische Cybergegenschläge sind nur zulässig, wenn der initiale Angriff in Umfang und Wirkung einem bewaffneten Angriff gleichkommt.[22] Dies gilt auch für Cyberoperationen der Bundeswehr zur Landes- oder Bündnisverteidigung, die erst in einem Szenario des Verteidigungsfalls gestartet werden könnten – dies wäre beim Großteil der angesprochenen Bedrohungen – Spionage, Cyberkriminalität und Subversion – nicht der Fall.[23]

Zudem zeigt sich, dass die Reaktion mit nicht-militärischen Mitteln, etwa in Form von Wirtschaftssanktionen, Einreisebeschränkungen und Kontensperrungen, kaum dazu führen, dass russische, chinesische oder nordkoreanische Angreifer von ihren Operationen ablassen.[24] Ähnliches gilt für westliche Bemühungen, unverbindliche Normen für staatliches Verhalten im Cyberspace zu etablieren, etwa eine normative Ächtung von Angriffen auf kritische Infrastrukturen.[25] Diese haben in den vergangenen Jahren trotz bestehender Normen eher zu- als abgenommen. Laut Goldman, Harknett und Fischerkeller ist das auch kein Wunder: Die mit Cyberoperationen angestrebten strategischen Gewinne sind weitaus höher als der wirtschaftliche Schaden, der durch kleinere Sanktionen oder moralische Ächtung entsteht – zumal Nordkorea bereits so hoch sanktioniert ist, wie kaum ein anderes Land. Für den Politikwissenschaftler Tobias Liebetrau erzeugt dieser Umstand der ineffektiven Reaktionswerkzeuge eine strategische Lücke für westliche Staaten. Im gegenwärtigen völkerrechtlichen Rahmen sind Cybersanktionen das schärfste Schwert, das man ziehen kann, ohne in eine Kriegssituation eskalieren zu wollen. Dennoch zeigt sich, dass sie kaum wirken. Die nächsthöhere Reaktionsstufe wäre die Ausrufung des Verteidigungsfalles analog zu Artikel 5 der NATO, der auch militärische Gegenreaktionen – einschließlich Cyberoperationen

18 Vgl. Douglas A. Ollivant, On Will and War, 17.6.2019, https://warontherocks.com/2019/06/on-will-and-war.

19 Vgl. Lucas Kello, Cyber Legalism, in: Journal of Cybersecurity 1/2021, S. 1–15.

20 James A. Caporaso, Changes in the Westphalian Order, in: International Studies Review 2/2000, S. 1–28.

21 Vgl. Kello (Anm. 19).

22 Vgl. Michael N. Schmitt, The Use of Force, in: ders. (Hrsg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge 2017, S. 328–356.

23 Vgl. Matthias Schulze, German Military Cyber Operations Are in a Legal Gray Zone, 8.4.2020, www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.

24 Vgl. Sameer Patil, Assessing the Efficacy of the West's Autonomous Cyber-Sanctions Regime and its Relevance for India, Observer Research Foundation, Occasional Papers 364/2022.

25 Vgl. Michael Mazarr et al., Competition and Restraint in Cyberspace. The Role of International Norms in Promoting U.S. Cybersecurity, RAND Corporation, Santa Monica 2022.

durch die NATO – ermöglichen würde.[26] Cyberoperationen unterhalb der rechtlich notwendigen Gewaltschwelle erlauben die Ausrufung des Verteidigungsfalles jedoch nicht. Zudem hätte die Ausrufung auch konventionelles Eskalationspotenzial, weshalb die meisten Staaten davor zurückschrecken dürften.[27] Insofern gibt es derzeit kaum wirksame Strategien, das Kosten-Nutzen-Kalkül von Angreifern zu beeinflussen.

TRUGSCHLÜSSE

Die hohe operative Geschwindigkeit und der ständige Kontakt mit Gegnern erfordern permanente Investitionen in die IT-Sicherheit sowie proaktives Handeln und Antizipieren der nächsten Schritte der Angreifer. Laut dem Oberbefehlshaber des United States Cyber Command (USCYBERCOM), Paul Nakasone, sind rein reaktive Strategien zum Scheitern verurteilt.[28] Eine einzelne Reaktion auf lediglich besonders schwerwiegende Cybervorfälle, analog zur militärischen Gewaltanwendung, reicht in einem Kontext kumulativer, niedrigschwelliger Cyberkampagnen nicht aus. Deshalb greift auch die Idee zu kurz, einzelne, besonders schwerwiegende Cyberangriffe durch Hackbacks zu stoppen, also durch das Ausschalten gegnerischer Angriffsinfrastruktur mithilfe eigener Cyberoperationen.[29] Es gibt nur wenige plausible Szenarien, bei denen so etwas taktisch sinnvoll wäre. Selbst wenn die Operation gelingen sollte, stellt sich die Frage, wie nachhaltig das Deaktivieren gegnerischer Angriffsinfrastruktur ist. Angriffsinfrastruktur ist aufgrund der geringen Einstiegskosten günstig, und resiliente Angreifer können diese bei Verlust schnell auswechseln. Mittlerweile existiert ein komplexes Untergrundökosystem für Cyberkriminelle, in dem alle Bestandteile für Cyberoperationen günstig und anonym erworben werden können.[30] Die Vorzüge von Hackbacks sind also extrem kurzlebig und rein taktischer Natur, nicht aber strategisch nachhaltig. Für Goldman, Harknett und Fischerkeller ist auch dies aus Sicht der Angreifer nicht verwunderlich: Die Einstiegskosten sind gering, verwundbare Systeme vielfältig verfügbar, und permanentes Agieren und Ergreifen der Initiative führen zu Gewinnen.

Ein zweiter Trugschluss ist die Übertragung des Abschreckungsparadigmas auf den Bereich „Cyber". Die Idee der Abschreckung durch Androhung von Vergeltung stammt aus der nuklearen Domäne, wo diese Androhung glaubhaft mit katastrophalen Folgen verbunden ist. In der Cyberdomäne ist diese Glaubwürdigkeit sehr schwer zu erreichen, da Cyberoperationen auf Geheimhaltung angewiesen sind, um erfolgreich zu sein.[31] Statt einiger Atommächte gibt es Dutzende von Staaten mit Cyberfähigkeiten und eine unüberschaubare Zahl nicht-staatlicher Akteure, deren Identität oft unklar ist. Da Abschreckung auf die Entscheidungsfindung eines Akteurs und seine Interessen zugeschnitten sein muss, um wirksam zu sein, ist unklar, wie dies in der multipolaren Welt des Cyberspace erreicht werden kann. Oft weiß man gar nicht, wer der Angreifer ist, den man abschrecken will.[32] Neben diesen praktischen Schwierigkeiten gibt es strategische Probleme: Es ist unwahrscheinlich, dass mit Androhung einer Cyberoperation das strategische Verhalten von Gegnern manipuliert werden kann. Goldman, Hartnett und Fischerkeller argumentieren, dass die Chance auf eine Belohnung und nicht die Angst vor Vergeltung der Hauptanreiz für Staaten ist, sich an Cyberoperationen zu beteiligen. Das bedeutet, dass sie dieses Verhalten nicht aufgeben werden, solange Gewinnanreize existieren.

Deshalb ist für USCYBERCOM die Strategie eine andere: Es geht nicht um das Deaktivieren gegnerischer Angriffsinfrastruktur mittels eigener, disruptiver Cyberoperationen, sondern darum, vom Angreifer zu lernen. Die Idee ist, Angreifer in ihrer eigenen Angriffsinfrastruktur

26 Vgl. Matthias Schulze, Can Russia and the West Avoid a Major Cyber Escalation?, 15.4.2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-russia-and-west-avoid-major-cyber.

27 Vgl. ders./Josephine Kerscher/Paul Bochtler, Cyber Escalation. The Conflict Dyad USA/Iran as a Test Case, SWP, Working Paper 1/2020.

28 Vgl. Paul M. Nakasone, A Cyber Force for Persistent Operations, in: Joint Force Quarterly 92/2019, S. 10–14.

29 Vgl. Thomas Reinhold/Matthias Schulze, Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von „hack backs", SWP, Arbeitspapier 1/2017.

30 Vgl. Matthias Schulze, Ransomware. Technische, nationale und multilaterale Gegenmaßnahmen, SWP-Aktuell 56/2021.

31 Vgl. ders., Überschätzte Cyber-Abschreckung, SWP-Aktuell 39/2019.

32 Vgl. Thomas Rid/Ben Buchanan, Attributing Cyber Attacks, in: Journal of Strategic Studies 1–2/2015, S. 4–37.

oder beim *threat hunting* in Opfernetzwerken zu beobachten und die dort gesammelten Informationen über ihr Verhalten und ihre Pläne für die Verteidigung zu nutzen. Dieses Wissen wird gesammelt, um eigene Verteidigungssysteme proaktiv darauf einzustellen.

CYBERRESILIENZ

In der IT-Sicherheit fand in den vergangenen Jahren ein Paradigmenwechsel statt, der der Strukturbeschreibung der Cyber-Persistenz-Theorie Rechnung trägt. Statt wie in der konventionellen Domäne geht es nicht mehr nur darum, Angreifer durch erfolgreiche Verteidigung am Betreten des eigenen Territoriums zu hindern. Moderne Strategien sind von der folgenden Annahme gekennzeichnet: Gehe davon aus, dass deine Verteidigung bereits versagt hat und ein Angreifer bereits in deinem Netzwerk aktiv ist.[33] Es reicht also nicht, wie in der konventionellen Domäne, sich allein auf Verteidigung zu konzentrieren. Das Ziel muss Cyberresilienz sein. Resilienz beschreibt die schnelle Wiederanlauffähigkeit nach einem erfolgreichen Cybervorfall.[34] Sie greift also dann, wenn die Verteidigung bereits versagt hat und wirkt ergänzend zu dieser.

Resilienzstrategien sind nicht neu: Viele Maßnahmen des analogen Katastrophenschutzes im Kalten Krieg, etwa das Anlegen strategischer Vorräte oder das Zurückhalten analoger Kommunikationssysteme für den Fall eines Stromausfalls, basieren auf dem Resilienzgedanken. Aus dem Paradigma ergeben sich unter anderem vier Trends: *Erstens* müssen die Verteidiger Ressourcen, Strukturen und Prozesse definieren, um erfolgreiche Cyberangriffe auf ihre Infrastruktur zu bewältigen. Das heißt, sie müssen Pläne für die Wiederherstellung der Infrastruktur erstellen und sogenanntes Incident Response üben. Es geht also darum, den Worst Case zu planen, um im Ernstfall vorbereitet zu sein. Dies ist ein kontinuierlicher Prozess, der immer wieder überdacht und erweitert werden muss, um sich an neue Angriffsmethoden anzupassen. Für Betreiber kritischer Infrastrukturen ist dies in Deutschland bereits verpflichtend, eine Ausweitung auf weitere Sektoren wäre sinnvoll.

Zweitens gibt es seit einigen Jahren den technischen Trend der Zero-Trust-Architektur. Zero Trust geht davon aus, dass es aufgrund der Mischung von Cloud- und Vor-Ort-Infrastruktur keine klassischen Netzwerkgrenzen mehr gibt und somit keinem Element in der eigenen Infrastruktur vollständig vertraut werden kann. Nutzerinnen und Nutzer müssen sich also permanent authentifizieren, und Geräte müssen permanent hinsichtlich ihres Verhaltens und ihrer Privilegien geprüft werden. Im November 2022 verkündete das US-Verteidigungsministerium eine Zero-Trust-Strategie[35], die eine Umstellung aller internen Systeme auf diese Architektur vorsieht. Für sensible Regierungsnetzwerke ist dieser Ansatz sinnvoll, wenngleich ein komplexes Unterfangen.

Drittens müssen die Verteidiger ständig die Bedingungen ihrer eigenen Sicherheit gestalten, indem sie die Parameter ihres eigenen Terrains verändern und updaten. Ziel muss es sein, Angreifern die erfolgreiche Ausnutzung von Schwachstellen zu verwehren. Dazu gehören das schnelle Einspielen von Sicherheitsupdates für Soft- und Hardware sowie die Etablierung von Prozessen zur Erkennung und Behebung von Sicherheitslücken. Da viele Sicherheitslücken außerhalb der Kontrolle von Endkunden liegen, etwa bei Netzwerkdienstleistern, gilt hier für die Hersteller von Software, dass diese sogenannte Coordinated Vulnerability Disclosure Policies etablieren sollten.[36] Dies ist ein Prozess, bei dem Schwachstellenforscher legal Sicherheitslücken an die Hersteller melden können, und diese sich dazu verpflichten, die Lücken zu schließen und gegebenenfalls Belohnungen auszuzahlen, sogenannte Bug Bounties. Dadurch können schwerwiegende, unbekannte Sicherheitslücken schneller gefunden und geschlossen werden, bevor sie von Angreifern ausgenutzt werden können. Staaten wie die Niederlande, Belgien, Litauen und Frankreich haben solche Policies bereits etabliert.

33 Digital Academy, Assume-Breach-Paradigma, www.digitalacademy.de/glossar/cybersecurity/assume-breach-paradigma.

34 Vgl. Sven Herpig, Mehr Resilienz für Deutschlands IT-Systeme, 23.1.2023, https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme.

35 Vgl. Department of Defense Office of Republication and Security Review, DoD Zero Trust Strategy, Washington D.C. 2022.

36 Vgl. Agentur der Europäischen Union für Cybersicherheit, Coordinated Vulnerability Disclosure Policies in the EU, 13.4.2022, www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

Viertens ist es wichtig, die nächsten Schritte der Angreifer zu antizipieren, um Abwehrstrategien schnell anpassen zu können. Spätestens seit dem Krieg in der Ukraine zeigt sich der Mehrwert von Threat Intelligence, also Informationen über das Verhalten von Angreifern, ihre Motive, Tools, Techniken und Vorgehensweisen.[37] Dieses Wissen ermöglicht es den Verteidigern, voneinander zu lernen. Da komplexe, fortgeschrittene Angreifer in der Regel mehrere Ziele gleichzeitig attackieren und eben auf kumulative Operationen setzen, helfen die Informationen allen potenziellen Opfern dieser Kampagne. Diese müssen aber rasch von einem Unternehmen zu allen anderen vergleichbaren Organisationen gelangen, die vielleicht ebenfalls von der gleichen Kampagne betroffen sind. Idealerweise geschieht dies in Echtzeit, etwa durch automatisierte Bedrohungsfeeds, die direkt live in die Verteidigungssysteme eingebettet sind. Eine erweiterte Form dieses Threat Intelligence Sharing ist das sogenannte Threat Hunting: Im Kontext des Ukrainekrieges entsandten die Europäische Union und USCYBERCOM Netzwerkverteidiger in die Ukraine, um in Netzwerken potenzieller Opfer gezielt nach der Präsenz von Bedrohungsakteuren zu suchen und die daraus generierten Informationen mit anderen Stellen zu teilen.[38] Threat Hunting soll die Vorteile von Angreifern reduzieren. Allerdings ist es eine rein taktische Maßnahme und wird nicht dazu führen, dass Angreifer ihre Motivationen ändern. Aber es macht Cyberoperationen schwieriger, erhöht somit die Friktion und führt bisweilen zur Minderung der Gewinne. Damit all dies hierzulande wirken kann, braucht es aber den Abbau von Barrieren und Informationssilos sowie die Reduktion des Behörden- und Zuständigkeitswirrwars des deutschen Föderalismus in der Cybersicherheit. Lange behördliche Genehmigungsketten und der schleppende Austausch über die sinnbildlichen Faxgeräte der deutschen Verwaltung sind zu langsam. Im weiteren Sinne gilt das natürlich auch für die EU: Eine nationalstaatliche Logik reicht nicht aus, im Idealfall gibt es ein EU-weites Threat Intelligence Sharing in Echtzeit.

Fünftens wird für all diese Elemente Personal benötigt. Gegenwärtig herrscht in Deutschland jedoch ein IT-Fachkräftemangel.[39] Dies gilt insbesondere für die öffentliche Verwaltung. Knappes Angebot führt zu steigenden Preisen und Löhnen für qualifiziertes Personal und in der Summe dazu, dass IT-Sicherheit immer noch recht teuer ist. Gleichzeitig wird es aufgrund der geringen Einstiegskosten und das arbeitsteilige Untergrundökosystem immer billiger für Angreifer, komplexe Angriffe zu starten. Solange die Defensive teuer und Offensive billig ist, wird sich das Katz- und Maus-Spiel nicht zugunsten der Defensive verändern. Die Maßnahmen, die getroffen werden können, sind seit Jahren bekannt und werden von anderen Ländern wie Israel oder Estland vorgelebt.[40] Dazu gehören verpflichtende Programmierkenntnisse und Informatikunterricht an Schulen, einschließlich der Vermittlung von digitaler Medienkompetenz und IT-Sicherheitshygiene. Und letztlich müssen die Hürden für die Anwerbung ausländischer Fachkräfte gesenkt werden, und es muss ein Paradigmenwechsel in der Rekrutierung stattfinden: weg von der deutschen Fixierung auf Hochschulabschlüsse und Zertifikate, hin zu einer breiteren Anerkennung alternativer Karrierewege – schließlich sind viele gute Hackerinnen und Hacker Studienabbrecherinnen und Autodidakten.[41]

37 Vgl. Brad Smith, Defending Ukraine: Early Lessons from the Cyber War, 22.6.2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war.

38 Vgl. U.S. Cyber Command Public Affairs, CYBER 101: Hunt Forward Operations, 15.11.2022, www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations.

39 Vgl. Bitkom, Trotz Krieg und Krisen: In Deutschland fehlen 137 000 IT-Fachkräfte, 16.11.2022, www.bitkom.org/Presse/Presseinformation/Deutschland-fehlen-137000-IT-Fachkraefte.

40 Vgl. Parmy Olson, Why Estonia Has Started Teaching Its First-Graders To Code, 6.9.2012, www.forbes.com/sites/parmyolson/2012/09/06/why-estonia-has-started-teaching-its-first-graders-to-code/?sh=3e664f461aa3.

41 Vgl. Satavisa Pati, Self-Taught Ethical Hackers Are Preferred by Big Tech Comps! Why?, 12.7.2022, www.analyticsinsight.net/self-taught-ethical-hackers-are-preferred-by-big-tech-comps-why.

MATTHIAS SCHULZE
ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik (SWP) sowie Principal Investigator im European Repository of Cyber Incidents Projekt (EuRepoC). Er betreibt zudem den Podcast „percepticon.de" zum Thema Cyberkonflikte.
matthias.schulze@swp-berlin.org

KLEINE GESCHICHTE DER HACKERKULTUR

Von der Modelleisenbahn zur Ideologie radikaler Transparenz

Christian Stöcker

Der US-amerikanische Journalist Steven Levy führt den Ursprung des Begriffs „Hacker" auf einen besonderen Ort Ende der 1950er Jahre zurück: den Modelleisenbahnclub der Eliteuniversität Massachusetts Institute of Technology (MIT) in Boston. In seinem Buch „Hackers" beschreibt er 1984 das zentrale Merkmal dieses Orts:[01] „Sie füllte den Raum fast vollständig aus, und wenn man in dem kleinen Kontrollbereich stand, der ‚Die Mulde' genannt wurde, sah man eine kleine Stadt, ein kleines Industriegebiet, eine winzige funktionierende Straßenbahn, einen Berg aus Pappmaché und natürlich jede Menge Züge und Gleise." Für diese Schauseite der Modelleisenbahn des Tech Model Railroad Club (TMRC) waren junge Männer zuständig – es scheinen tatsächlich ausschließlich Männer gewesen zu sein –, die sich für Züge und Loks interessierten und die eine möglichst hübsche, realistische Miniaturlandschaft erschaffen wollten.

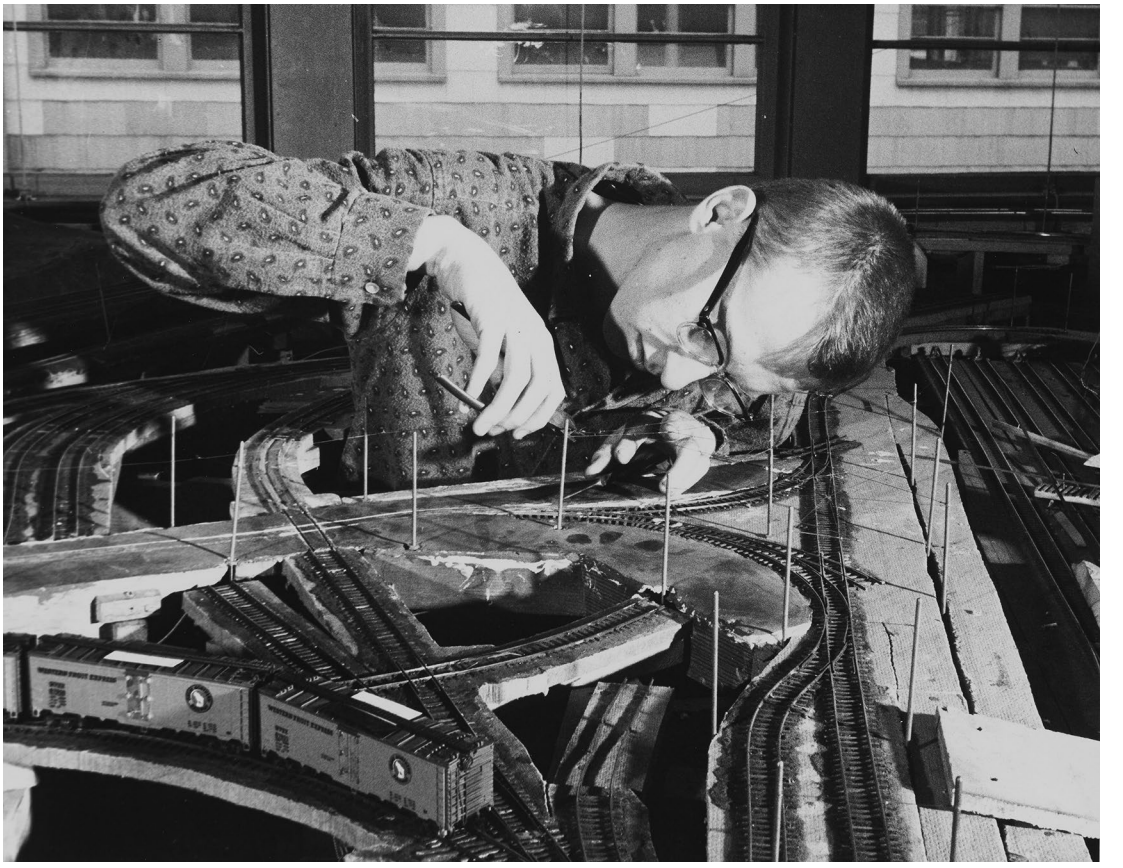
Diejenigen, die sich selbst später „Hacker" nennen sollten, gehörten zum sogenannten Signals and Power Subcommittee. Sie fanden die Unterseite der Plattform viel interessanter: „Unterhalb befand sich ein ungleich größeres Netzwerk von Drähten, Relais und Kreuzschienenschaltern", mit einem „verzweigten Gewirr aus roten, blauen und gelben Drähten, verzwirbelt und verdreht wie eine regenbogenfarbige Explosion von Einsteins Haar".

Viele der elektronischen Bauteile, die dafür sorgten, dass die Züge sich von oben steuern ließen, waren Geschenke der lokalen Telefongesellschaft. Die Mitglieder des Subcommittee interessierten sich vor allem dafür, wie dieses bemerkenswert komplexe Netz aus Kabeln, Schaltern und Relais funktionierte, wie es sich verfeinern und verbessern ließ. „Sie waren lebenslange Jünger des Imperativs der Praxis", wie Levy es formuliert.

HACKEN UND PROGRAMMIEREN

Der Begriff „Hack" war Teil einer Kunstsprache, die sich die Bastler zugelegt hatten. Ein Hack war, so Levy, „ein Projekt oder ein Produkt, das nicht nur um eines konstruktiven Ziels willen in Angriff genommen wurde, sondern aufgrund einer wilden Lust am Machen". Ein echter Hack musste „von Innovation, Stil und technischem Können durchdrungen sein". Elaborierte Streiche, die zum Campusleben des MIT dazu gehörten, seien zwar schon vorher „Hack" genannt worden, „aber wenn die Leute vom TMRC das Wort benutzen, schwang dabei echter Respekt mit". Bald nannten sich die aktivsten Bastler an der Unterseite der Modelleisenbahn selbst „Hacker". Einer von ihnen schrieb darüber sogar ein Gedicht, eine Ode an die „schmutzigen, haarigen, wuchernden Hacks der Jugend". Der Autor dieses Gedichts heißt Peter Samson, und er ging als einer der ersten in die Geschichte ein, die den Begriff „Hacker" Ende der 1950er Jahre mit einer damals neuen Technologie verknüpften: digitalen Computern.

Am MIT gab es zu dieser Zeit einen raumgroßen, frühen IBM-Computer mit der Typbezeichnung 704. Ein Gerät, das von ausgewähltem Personal mit Lochkarten gefüttert wurde. Steven Levy nennt die Männer, denen es gestattet war, das Gerät anzufassen, „Priesterkaste". Die röhrenbasierten Großrechner dieser Zeit wurden für Rüstungs- oder Forschungsprojekte eingesetzt. Rechenzeit war teuer und kostbar. Es war ein unerhörter Gedanke, Computer anders als für die vorgesehenen Zwecke einzusetzen.



Tech Model Railroad Club am Massachusetts Institute of Technology
© MIT Museum

Ab 1959 unterrichtete ein Mann, dessen Name heute in Büchern über die Geschichte des Computers verlässlich auftaucht, das Programmieren. John McCarthy war Mathematiker und gehörte zu einer Gruppe, die in den 1950er Jahren mit Algol (kurz für *algorithmic language*) eine der ersten Programmiersprachen entwickelt hatte.[02] McCarthy vertrat die damals ungewöhnliche Position, dass Computer mehr als reine Werkzeuge sein könnten, ja, dass etwas wie eine Computerwissenschaft möglich und nötig sein könnte. Die akademischen Disziplinen wie *computer science* oder Informatik existierten damals noch nicht.

01 Hier und im Folgenden Steven Levy, Hackers. Heroes of the Computer Revolution, New York 1984. Bei allen folgenden Zitaten aus englischsprachiger Literatur handelt es sich um eigene Übersetzungen.

02 Vgl. Thomas Haigh/Paul E. Ceruzzi, A New History of Modern Computing, Cambridge, MA 2021.

ERSTER SCHACHCOMPUTER

In McCarthy fanden die frühen Hacker am MIT einen Mentor. Er war, wie sein Kollege Marvin Minsky, der Meinung, dass es eines Tages „künstliche Intelligenz" geben werde, eine damals geradezu lächerliche Position. McCarthy nutzte den IBM 704 des MIT unter anderem, um ein Programm zu schreiben, das Schach spielen sollte. Peter Samson, Alan Kotok und andere Mitglieder des TMRC übernahmen die Arbeit an dem Mammutprojekt, als McCarthy mehr und mehr seiner Zeit der Entwicklung der Programmiersprache Lisp widmete. Das verschaffte den Männern, die sich selbst Hacker nannten, zumindest mittelbaren Zugang zum IBM 704 und seinem Nachfolger, dem Modell 7090.

Die Situation änderte sich, als ein Militärlabor dem MIT einen Rechner namens TX-0 stiftete. Für die Hacker des TMRC war dies der Moment, auf den sie gewartet hatten: Endlich gab es einen

Computer am Institut, den sie selbst bedienen durften. Die 24 Stunden, die der Rechner jeden Tag lief, wurden stundenweise unter den Interessenten aufgeteilt. Die Hacker verbrachten deshalb oft die Nächte dort, angetrieben von sehr viel Coca-Cola, und manchmal nur in der Hoffnung, dass jemand, der eine Stunde Rechenzeit von drei bis vier Uhr morgens gebucht hatte, nicht auftauchen würde. „Die Atmosphäre war 1959 locker genug, auch die Streuner aufzunehmen", so Levy, „wissenschaftsverrückte Leute, deren Neugier wie Hunger brannte".

Die TMRC-Hacker nahmen sogar einen Schuljungen namens Peter Deutsch in ihre Reihen auf, den zwölfjährigen Sohn eines MIT-Physikprofessors. Der Junge war mathematisch begabt, neugierig, besserwisserisch und sehr talentiert im Umgang mit Computern, also war sein Alter den Hackern im Bachelor-Studium egal. Die promovierten Wissenschaftler, die sonst dort arbeiteten, fanden ihn nur lästig. Später entwickelte Deutsch eigene Programmiersprachen und Betriebssysteme, arbeitete für Xerox PARC und Sun Microsystems und gründete ein Softwareunternehmen.

Die ersten Hacker nahmen sich Projekte vor, die sich durch ihre Kühnheit und technische Eleganz auszeichneten, nicht unbedingt durch ihre Nützlichkeit. Peter Samson brachte der Maschine bei, in monoton fiependen Sinustönen Bach-Melodien zu spielen. Er kann damit auch als einer der Erfinder der digitalen Musik gelten. Später entwickelte er einen der ersten Synthesizer. Ein größeres Publikum konnte man mit einem Sinustöne pfeifenden Drei-Millionen-Dollar-Computer nicht beeindrucken, aber das spielte keine Rolle. Samson hatte der Maschine etwas Neues beigebracht und damit bewiesen, dass ein Computer mit nichts als Nullen und Einsen praktisch alles ver- und bearbeiten konnte, „ob eine Bach-Fuge oder ein Flugabwehrsystem", so Levy. Das heutige Verständnis des Begriffs Digitalisierung war geboren.

Damals entstand auch das Konzept des Personal Computer: „Als Produkt gab es den Personal Computer erst in den 1970er Jahren. Anders betrachtet aber ist das, was einen Computer ‚persönlich' macht, sein Verhältnis zu denen, die ihn nutzen. Ein Personal Computer steht Einzelpersonen zur Verfügung, um deren persönliche Bedürfnisse zu befriedigen."[03]

03 Ebd.

KI-Pionier John McCarthy spielt Schach mit einem IBM 7090-Computer.

© picture alliance/AP

HACKERETHIK UND DAS ERSTE VIDEOSPIEL

Steven Levy leitete aus seinen vielen Gesprächen mit Leuten wie Samson, Kotok und ihren Nachfolgern sechs Leitprinzipien ab, die er 1984 als „Hackerethik" zusammenfasste. Sie spiegeln die Erfahrungen der ersten Hacker mit Hochschulbürokratie und akademischer Arroganz, aber auch ihren Schöpfergeist. Die Regeln lauten:

1. Zugriff auf Computer und alles, was einen etwas über die Welt lehren kann, soll unlimitiert und total sein. Der Imperativ der Praxis gilt immer.
2. Alle Information sollte frei zugänglich sein.
3. Misstraue Autorität, setze Dich für Dezentralisierung ein.
4. Hacker sollten nur nach ihrer Fähigkeit im Hacken beurteilt werden, nicht nach Scheinkriterien wie Abschlüssen, Alter, Rasse oder Position.
5. Du kannst mit Computern Kunst und Schönheit schaffen.
6. Computer können dein Leben zum Besseren verändern.

1961 kam ein neuerer Rechner hinzu, ein kleineres, deutlich günstigeres Gerät namens PDP-1, hergestellt von der Digital Equipment Corporation. Auf diesem Computer entwickelte ein weiterer MIT-Hacker namens Steve „Slug" Russell das erste Computerspiel der Geschichte: „Spacewar!". Darin beschießen sich zwei Raumschiffe auf einer für ganz andere Zwecke gebauten Anzeige mit Torpedos.

Dan Edwards und Peter Samson spielen „Spacewar!" auf einem PDP-1-Computer.

Russell hatte die Idee und entwarf den ersten Prototypen, dann verfeinerten die anderen Hacker das Spiel immer weiter. Der eine programmierte einen beweglichen Sternenhimmel, der reale Sternbilder zeigte, der andere eine zentrale Sonne mit Gravitationsfeld, die dem Spiel eine ganz neue taktische Dimension verlieh. Ein Dritter ergänzte „Wurmlöcher", mit deren Hilfe man sein Schiff dreimal pro Runde an einen zufälligen Ort bewegen konnte, um einer drohenden Kollision zu entgehen.

„Spacewar!" vereinte erstmals viele Elemente dessen, was man heute Hackerkultur nennt: Begeisterung für Science-Fiction – Russell und seine Freunde liebten beispielsweise die Space-Opera-Romane des heute fast vergessenen Autors E.E. Smith; Begeisterung für Computerspiele, Koffein und Nachtaktivität – die Hacker veranstalteten nächtelange „Spacewar!"-Turniere; der Geist der kreativen Kollaboration, und natürlich die Begeisterung für die elegante Zweckentfremdung von Computern – zwei aus der Gruppe bauten mit Teilen aus dem Fundus des Modelleisenbahnclubs die ersten Joysticks der Geschichte.

Am MIT entstand in diesen Tagen auch das Konzept des Computers als „generative Plattform", das der auf die digitale Welt spezialisierte Jurist Jonathan Zittrain in Harvard Jahrzehnte später formulierte:[04] „Generative Plattformen regen Beiträge von allen an, die gerne beitragen möchten. Diese Beiträge kommen zunächst von Amateuren, die sich eher aus Lust und Laune beteiligen und nicht, um davon zu profitieren." Die größte generative Plattform der Geschichte ist das Internet.

Wenig später tauchte der Geist des Modelleisenbahnclubs auch an der Westküste der USA auf. John McCarthy eröffnete ein „AI Lab" an der Universität Stanford, Hacker wie Steve Russell folgten ihm. Auch am MIT ging die Entwicklung weiter, neue Hacker stießen zu der alten Gruppe dazu, neue Rechner wurden angeschafft, neue Spielwiesen entdeckt. Eine davon war das internationale Telefonnetz, das die Hacker mithilfe des PDP-1 im *blue box mode* erkundeten: Man konnte die Maschine mit dem Netz verbinden und es so manipulieren, dass sie kostenlose Ferngespräche ermöglichte.

Das *blue boxing* war ab Ende der 1960er Jahre nicht nur in Boston ein beliebter Zeitvertreib unter Hackern und sogenannten Phone Phreaks. Man brauchte dazu auch keine Hochleistungscomputer: MIT-Studierende verkauften Ende der 1960er Jahre bereits kleine Blue Boxes, die Töne erzeugen konnten, mit denen man im US-Telefonnetz eine Fernleitung bekam. Anschließend konnte man mit Tonfolgen der Frequenz 2600 Hertz eine beliebige Nummer „wählen". Für die Telefongesellschaften sahen die so erschlichenen Verbindungen aus wie kostenlose Ortsgespräche.

Erfunden – oder besser: gefunden – wurde diese Technik von Josef Carl Engressia alias Joybubbles, und zwar schon in den 1950er Jahren. Durch Zufall entdeckte der damals siebenjährige Engressia, dass er sich eine freie Leitung verschaffen konnte, indem er einen Ton in einer bestimmten Tonhöhe – eben 2600 Hertz – in den Hörer pfiff. Ein bekanntes Hacker-Magazin heißt bis heute „2600". Noch berühmter als Engressia wurde John T. Draper, der sich selbst Captain Crunch nannte. Er kam auf den Namen, nachdem er herausgefunden hatte, dass eine kleine Plastikpfeife, die den gleichnamigen Frühstücksflocken beilag, diesen Ton von 2600 Hertz erzeugen konnte. Zunächst pfiff Draper damit Leitungen frei, später entwickelte er die erste „Blue Box".

HIPPIES UND HACKER

Zu denen, die an der US-Westküste solche illegalen Blue Boxes bauten und verkauften, gehörten Anfang der 1970er Jahre auch die späteren Gründer von Apple, Steve Jobs und Steve Wozniak. Sie hatten Draper an einem Ort kennengelernt, der

04 Jonathan Zittrain, The Future of the Internet and How to Stop It, New Haven 2008.

für die Geschichte der Hackerkultur eine ebenso große Bedeutung hat wie der Tech Model Railway Club in Boston: Der Homebrew Computer Club, gegründet 1975 in Menlo Park, wo heute die Apple-Zentrale liegt.

Dort trafen sich Elektronikbastler – es waren einmal mehr nur Männer – und Leute, die sich für die ersten Computer interessierten, die zu diesem Zeitpunkt auch für Privatleute erschwinglich waren. Zunächst war das vor allem der Altair 8800, ein Computer, der ab 1974 als Bausatz für sensationelle 397 Dollar verkauft wurde – der Name ist der eines Planeten aus „Star Trek". Apple-Mitgründer Wozniak schrieb später: „Ohne Computer-Clubs gäbe es vermutlich keine Apple-Computer. Unser Club im Silicon Valley, der Homebrew Computer Club, war einer der ersten seiner Art."[05] Mit einem anderen berühmten Programmierer gerieten die Homebrew-Clubmitglieder in Streit: Der junge Bill Gates hatte in Harvard eine Programmiersprache namens Basic geschrieben, die auf dem Altair 8800 lief. Die Hobbyisten kopierten den Code einfach, ohne zu bezahlen. Gates schrieb ihnen einen wütenden, berühmt gewordenen Brief: „Was Ihr tut, ist Diebstahl."[06] Es ist der erste Konflikt zwischen dem Hacker-Ideal der freien Software und dem Konzept proprietären Codes. Später ging aus der Hackerkultur die „Free and Open Source Software"-Bewegung (FOSS) hervor, deren Erzeugnisse bis heute unter anderem wesentliche Teile der Internetinfrastruktur antreiben.

In Kalifornien traf zu dieser Zeit der Geist der Hippie-Ära auf die kalifornische Variante der Hackerkultur. Der in Stanford lehrende Literatur- und Kommunikationswissenschaftler Fred Turner hat diese Entwicklung in „From Counterculture to Cyberculture" detailreich nachgezeichnet.[07] Die Einflüsse, die im kalifornischen Underground damals zusammenflossen, reichten von den kybernetischen Arbeiten von Mathematikern und Informationstheoretikern wie Norbert Wiener über systemtheoretische Ansätze von Buckminster Fuller und Marshal McLuhan bis hin zu Zen-Buddhismus und Mystizismus.

Akteure wie Steward Brand, der Gründer des „Whole Earth Catalog" und der Zeitschrift „Co-Evolution Quarterly" (CQ), betrachteten Computer und Technik generell als logische Erweiterungen ihres Möglichkeitsraums, ganz im Sinne der Hackerethik. „Wie der Whole Earth Catalog diente CQ als Forum für die Diskussion und Integration von Wissenschaft, Technologie, Mystizismus und der richtigen Lebensweise", schrieb Turner. Technik wurde begriffen als Werkzeug der Selbstermächtigung, der Befreiung. Auf einer beispielhaften Doppelseite des „Whole Earth Catalog" findet man eine Rezension des Fachmagazins „Electronics", ein Angebot für das „Radio Amateur's Handbook" für Hobbyfunker und eine Besprechung eines Oszilloskops zum Ladenpreis von 735 Dollar („teuer, aber seinen Preis auf jeden Fall wert"). Ein paar Seiten weiter dann Kuppelzelte, Schaufeln und Saatgut für Landkommunarden.

VORLÄUFER DES INTERNETS

In dieser Atmosphäre arbeiteten Jobs und Wozniak zunächst für Atari, eine der ersten Videospielfirmen. Wozniak entwarf unter anderem die Hardware für das Spiel „Breakout", bei dem mit einem Schläger und einem Ball am oberen Bildrand angeordnete Ziegel nach und nach zerschlagen werden müssen. Der Spielhallenautomat war ein sensationeller Erfolg. Auf der Produktionsstraße von Atari, so ist in Steven L. Kents „Ultimate History of Video Games" zu lesen, habe es oft nach Marihuana gerochen.[08]

Stewart Brand, der auch als Fotograf, Journalist und Event-Organisator tätig war, war überzeugt, dass Computer und digitale Technik nicht Militär und Konzernen vorbehalten sein sollten. Später gründete er eines der ersten Online-Foren, das „Whole Earth 'Lectronic Link", kurz The WELL. Es basierte auf einer Art Vorform des Internets, die aus den Aktivitäten der Hacker und Phone Phreaks entstanden war: elektronische *bulletin boards*, benannt nach den Korkpinnwänden, die in US-amerikanischen Colleges aushingen.

05 Steve Wozniak, Homebrew And How The Apple Came To Be, www.atariarchives.org/deli/homebrew_and_how_the_apple.php.

06 Vgl. Christian Stöcker, Nerd Attack! Eine Geschichte der digitalen Welt vom C64 bis zu Twitter und Facebook, München 2011.

07 Fred Turner, From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism, Chicago 2008.

08 Steven L. Kent, The Ultimate History of Video Games: from Pong to Pokémon and Beyond: The Story Behind the Craze that Touched our Lives and Changed the World, Roseville 2001.

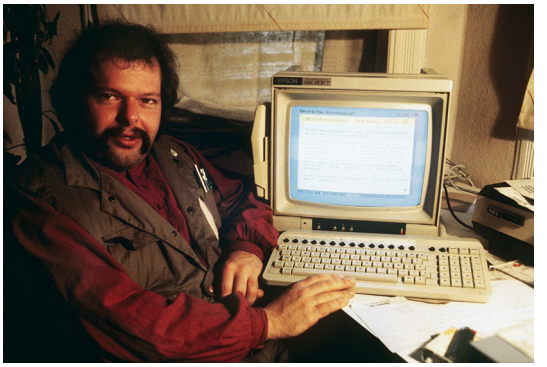
In ein *bulletin board system*, kurz BBS, konnte man sich mit einem Computer mithilfe eines Telefons und eines Modems oder Akustikkopplers einwählen. Das erste ging 1978 in Chicago ans Telefonnetz.[09] Diese frühen Server erlaubten in der Regel nur eine Verbindung zur gleichen Zeit. Sie enthielten sehr unterschiedliche Inhalte: „Ein Einkaufszentrum hatte vielleicht eine Liste von Läden, Telefonnummern und Kino-Spielpläne. Ein Geschäft Informationen über angebotene Dienstleistungen, Öffnungszeiten, Adresse und so weiter. Angebote für Erwachsene und der Austausch von Pornografie waren ebenfalls gängig."[10]

Die Verbindung zwischen Computern und Telefonen brachte schließlich den heutigen Hacker-Archetypen hervor. Im Film „War Games" von 1983 spielte Matthew Broderick einen Jugendlichen, der eigentlich Zugang zum BBS eines Computerspielherstellers sucht. Versehentlich wählt er sich in den Zentralcomputer der US-Luftabwehr ein und löst fast den dritten Weltkrieg aus. „War Games" hatte weitreichende Folgen: „Der Film half dabei, das Stereotyp des Hackers als junger Mann zu etablieren, ausgestattet mit beinahe mystischen Fähigkeiten, Computer-Sicherheitssysteme zu umgehen, und dem pathologischen Bedürfnis, an Information auf fremden Computersystemen herumzumachen oder sie zu stehlen. Die neue Hacker-Rolle hatte ihre Wurzeln in der ursprünglichen, am MIT entstandenen Wortbedeutung, doch sie war weit bedrohlicher."[11]

„War Games" inspirierte viele junge Leute, ein weiteres Mal überwiegend Männer, sich selbst am Hacken zu versuchen. Und zwar nicht nur in den USA. Die „weit bedrohlichere" Bedeutung des Wortes Hacker blieb bis heute bestehen: Auch Cyberkriminelle, Spione und Erpresser, die die Festplatten ihrer Opfer verschlüsseln, werden heute meist Hacker genannt – obwohl ihre Aktivitäten mit der ursprünglichen Bedeutung des Wortes wenig bis nichts zu tun haben.

DEUTSCHE HACKERKULTUR

Anfang der 1980er Jahre waren Heimcomputer wie der ZX Spectrum und der Commodore 64 (C64) erstmals massentauglich. Einmal mehr spielten Computerspiele eine zentrale Rolle. Meist Jugendliche „Cracker" machten es sich zur Aufgabe, Spiele vom Kopierschutz zu befreien und kostenlos in Umlauf zu bringen.[12] Manche stellten dazu sogar transatlantische Telefonverbindungen zu dortigen BBS her. So profitierten auch deutsche Nutzerinnen und Nutzer des C64, einer der meistverkauften Heimcomputer der Geschichte, von der ersten illegalen digitalen Tauschbörse der Geschichte, gewissermaßen ein Vorläufer von Napster – und ein typisches Produkt der Hackerethik, wenn auch weitgehend ohne ideologischen Überbau.



Wau Holland vom Chaos Computer Club in Hamburg an seinem Computer, 1984

Quelle: picture-alliance/dpa | Werner Baum

Auch die kalifornische Hackerkultur im engeren Sinn fand hierzulande schnell Freunde. Der bis heute bekannteste war Herwart „Wau" Holland-Moritz, einer der Gründer des Chaos Computer Clubs (CCC), der anfangs eine Art deutsche Variante der kalifornischen Clubs sein sollte.[13] Holland, der aus der Berliner Spontiszene stammte, las „Co-Evolution Quarterly" und glaubte wie Steward Brand an die befreiende Macht des Rechners – ganz anders als weite Teile der deutschen Linken, die Rechner damals primär als Werkzeuge der technokratischen Unterdrückung betrachteten, Stichwort Rasterfahndung.[14] Die grüne Bundestagsfraktion sperrte sich noch in der zweiten Hälfte der 1980er Jahre gegen vernetzte Computer, entgegen der expliziten Empfehlung des CCC.

09 Vgl. Ward Christensen/Randy Suess, Hobbyist Computerized Bulletin Board, in: Byte Magazine 3/1978, S. 150–158.
10 Haigh/Ceruzzi (Anm. 2).
11 Ebd.
12 Vgl. Stöcker (Anm. 6).
13 Vgl. ebd.
14 Vgl. Daniel Kulla, Der Phrasenprüfer: Szenen aus dem Leben von Wau Holland, Mitbegründer des Chaos-Computer-Clubs, Löhrbach 2003.

Holland, der gerne Weizenbier trank, Marihuana rauchte und dann lange Monologe über Politik und Technologie hielt, schrieb einmal: „Die sozialen Bewegungen, die sich vernetzen, rütteln am System." Im Zeitalter von Hashtag-Bewegungen wie #MeToo oder #FridaysForFuture wirkt das durchaus prophetisch. Schon vor dem Siegeszug dieser Bewegungen brachte die Hackerethik auf radikale Transparenz ausgerichtete Phänomene hervor – WikiLeaks etwa, gegründet von dem australischen Hacker und selbsternannten Cypherpunk Julian Assange, oder die dezentrale, schwer fassbare Netzbewegung Anonymous.[15]

Der CCC der frühen 1980er Jahre machte in Deutschland zuerst mit dem sogenannten BTX-Hack von sich reden. Irgendwie kamen die deutschen Hacker an ein Passwort, mit dessen Hilfe und einer eigenen Seite im BTX-Angebot der Deutschen Bundespost sie mehr als 100 000 D-Mark auf das Konto des Clubs transferierten. Das Geld gaben sie anschließend zurück: Es sei ihnen nur um eine Demonstration der Unsicherheit des BTX-Systems gegangen. BTX verstieß aus Hollands Sicht klar gegen die Hackerethik: Es gab Terminals für Anbieter und andere für Anwender, die nur „Tasten für ja, nein und kaufen" aufwiesen, wie ein frühes CCC-Mitglied später spottete. BTX war ein geschlossenes, zentralistisches System, keine generative Plattform im Sinne Jonathan Zittrains. Die zentralistische und bürokratische Bundespost, die nicht nur BTX betrieb, sondern sich auch noch anmaßte, den Betrieb nicht zugelassener Modems strafrechtlich verfolgen zu lassen, war ein Lieblingsfeind des frühen CCC. Sie wurde „der Gilb" genannt.

Im Dunstkreis des CCC geschahen damals aber auch Dinge, die den anfangs guten Ruf der Hacker in Deutschland zerstörten. 1987 erwischte der US-amerikanische Astrophysiker Clifford Stoll am Lawrence Berkeley National Laboratory in Kalifornien deutsche Hacker dabei, wie sie in dortige Rechnersysteme eindrangen.[16] Plötzlich interessierten sich US-Geheimdienste und das Bundeskriminalamt für deutsche Hacker. Schließlich stellte sich heraus, dass eine Vierergruppe aus Hannover nicht nur in US-Rechner eingedrungen war, sondern auch teils so erbeutete, teils im Laden eingekaufte Software und Daten an den KGB verkauft hatte. Die bescheidene Summe von gut 100 000 D-Mark, die sie so erlösten, investierten sie in Kokain und neue Rechner.

Einer von ihnen, der an einer Psychose leidende Vollwaise und Verschwörungstheoretiker Karl Koch, sagte später unter großem Druck gegen seine Kumpanen aus und nahm sich im Mai 1989 das Leben. Der Prozess gegen die „KGB-Hacker" erregte großes öffentliches Interesse und beschädigte das Image des CCC und des Begriffs „Hacker" in Deutschland nachhaltig.

Wau Holland machte sich lange Vorwürfe, weil er die Entwicklung in Hannover nicht hatte verhindern können. Und das, obwohl er den sechs Regeln von Steven Levy zwei weitere hinzugefügt hatte, die solche Ereignisse hätten verhindern sollen und die das Regelwerk bis heute relevant halten – alle acht sind die Leitsätze des CCC:

7. Mülle nicht in den Daten anderer Leute.
8. Öffentliche Daten nützen, private Daten schützen.[17]

Im Laufe der 1990er Jahre besserte sich der Ruf des Hackerclubs nach und nach wieder. Eines seiner ersten Mitglieder, der Informatiker und langjährige Club-Sprecher Andy Müller-Maguhn, wurde im Jahr 2000 sogar zu einem der ehrenamtlichen Direktoren der Internet-Adressverwaltungsorganisation ICANN gewählt. Heute ist der CCC eine Organisation, die weltweit für ihren jährlichen Kongress bekannt ist, an dem mittlerweile auch sehr viele Hackerinnen teilnehmen. Gleichzeitig ist er die wichtigste digitale Bürgerrechtsorganisation des Landes. Vertreterinnen und Vertreter des Clubs sagten zum Beispiel im Zusammenhang mit der anlasslosen Vorratsdatenspeicherung von Telefon- und Internetverbindungsdaten vor dem Bundesverfassungsgericht in Karlsruhe als Sachverständige aus. Hackerinnen wie Constanze Kurz und Lilith Wittmann sind wichtige Stimmen im Diskurs über Privatsphäre, Datenschutz und Cybersicherheit. Der CCC ist damit auch so etwas wie ein grobes Äquiva-

15 Vgl. Marcel Rosenbach, Staatsfeind WikiLeaks: Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert, München 2011; Ole Reißmann/Christian Stöcker/Konrad Lischka, We are Anonymous: die Maske des Protests – Wer sie sind, was sie antreibt, was sie wollen, München 2012.

16 Vgl. Clifford Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New York 1989.

17 Chaos Computer Club, Hackerethik, www.ccc.de/hackerethik.

lent zur Electronic Frontier Foundation (EFF), der wichtigsten digitalen Bürgerrechtsorganisation der USA.

DIGITALE BÜRGERRECHTE

Die EFF war Anfang der 1990er Jahre als Reaktion auf die Strafverfolgung von Hackern gegründet worden. Der Science-Fiction-Autor Bruce Sterling widmete dieser Zeit ein Buch mit dem Titel „The Hacker Crackdown".[18] Damals fanden in den USA zum Teil bizarre Razzien statt, um vermeintlich kriminellen Hackern – es waren wieder nur Männer – auf die Spur zu kommen. Unter anderem durchsuchte der Secret Service der USA am 1. März 1990 die Büros des Spieleherstellers Steve Jackson Games in Austin, Texas.[19] Beschlagnahmt wurden unter anderem Anleitungshefte für ein Rollenspiel namens „Cyberpunk", das in einer Science-Fiction-Welt spielt, angelehnt an Romane wie die von William Gibson, Autor von „Neuromancer" (1984), und Bruce Sterling selbst. Die Agenten hielten die Spielanleitungen offenbar für die Handbücher echter Cyberkrimineller.

Die ganze Episode liest sich wie ein Witz von Hackern für Hacker, hat sich aber tatsächlich so zugetragen. In einem anderen Verfahren, in dem es um die illegale Veröffentlichung von für Außenstehende im Grunde wertloser Firmware der Firma Apple ging, tauchte ein extrem unbedarfter FBI-Agent bei einem Nutzer von The WELL namens John Perry Barlow zu Hause auf. Dies veranlasste Barlow, zusammen mit einem Multimillionär die EFF zu gründen, die zunächst als eine Art Verteidigungsfonds für Hacker gedacht war. Der 2018 verstorbene Barlow war eine schillernde Figur: Er arbeitete einerseits als Rinderfarmer und Journalist, andererseits schrieb er Texte für die Band The Grateful Dead, und über die Jahre konsumierte er jede Menge Psychedelika und verbrachte viel Zeit bei The WELL. Zwischenzeitlich kandidierte er für die Republikaner für den Senat. Der zweite EFF-Gründer war der erfolgreiche und sehr wohlhabende Softwareunternehmer Mitch Kapor. Steve Wozniak und John Gilmore von Sun Microsystems steuerten weitere Startfinanzierung bei. Die EFF half tatsächlich Hackern und dem Beifang des „Hacker Crackdown" vor Gericht – Steve Jackson Games etwa bekam am Ende 50 000 Dollar Entschädigung.

Barlow ist auch der Autor der bis heute berühmten „Unabhängigkeitserklärung des Cyberspace" von 1996, mit der er gewissermaßen die antiautoritäre Hackerethik ins Zeitalter des Internets zu hieven versuchte: „Regierungen der industrialisierten Welt, ihr müden Giganten aus Fleisch und Stahl, ich komme aus dem Cyberspace, der neuen Heimat des Geistes. Im Namen der Zukunft bitte ich euch, die ihr aus der Vergangenheit stammt, uns in Frieden zu lassen. Ihr seid unter uns nicht willkommen. Wo wir uns versammeln, habt ihr keine Macht."[20]

Die EFF hat als zivilgesellschaftliche Lobbyorganisation nachweislich dazu beigetragen, dass das Internet bis heute kein rein kommerzieller Raum ist, wie er damals einigen Internetdienstanbietern vorschwebte, sondern eine offene Plattform – eine generative Plattform, wie Jonathan Zittrain schreibt, ganz im Sinne der Hackerethik.

18 Bruce Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, New York 1992.
19 Vgl. Electronic Frontier Foundation, Steve Jackson Games v. Secret Service Case Archive, 2011, www.eff.org/de/cases/steve-jackson-games-v-secret-service-case-archive.
20 John Perry Barlow, A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation, 2016, www.eff.org/cyberspace-independence.

CHRISTIAN STÖCKER
ist Professor für Digitale Kommunikation an der Hochschule für Angewandte Wissenschaften Hamburg (HAW).

AUS POLITIK UND ZEITGESCHICHTE

New Work

CALL FOR PAPERS

Spätestens seit der Corona-Pandemie sind wir gezwungen, Arbeit neu zu denken. Viele nutzen mittlerweile die Optionen des Homeoffice und des flexiblen Arbeitens, Gleitzeitmodelle hatten starre Arbeitszeiten schon vorher abgelöst. Oft werden diese Entwicklungen als „New Work“ bezeichnet, ein Konzept, das bereits seit den 1970er Jahren diskutiert wird und mit dem Anspruch an eine „Arbeit, die man wirklich, wirklich will“ (Frithjof Bergmann) verbunden ist. Welche Auswirkungen hat die Restrukturierung von Arbeit auf die Work-Life-Balance oder auf zentrale gesellschaftliche Fragen wie Angestelltenrechte, den Gender-Pay-Gap, die Vereinbarkeit von Beruf und Familie oder auch ökologische Nachhaltigkeit? Wie bewerten jüngere Generationen den Sinn von Arbeit? Welche Vor- und Nachteile sind von der „schönen neuen Arbeitswelt“ zu erwarten? Während die Auswirkungen von „New Work“ weit über die individuelle Arbeit hinausgehen, entwickeln sich durch die fortschreitende Digitalisierung neue Branchen und Arbeitsformen, etwa die Plattformarbeit. Mit ihnen wird die Diskrepanz zwischen unterschiedlichen Arbeitsmodellen immer größer, denn sogenannte systemrelevante Branchen wie Pflege oder Landwirtschaft profitieren von solchen Neuerungen kaum.

Für die Ausgabe 46/2023 suchen wir Beiträge, die sich aus unterschiedlichen fachwissenschaftlichen Perspektiven mit dem Thema „New Work“ beschäftigen. Exposés mit einem Umfang von höchstens 4000 Zeichen (1–2 Seiten) können bis zum 12. Juni 2023 per E-Mail an apuz@bpb.de eingereicht werden. Aus den Exposés sollen die zugrunde liegenden Leitfragen und die Struktur des Beitrags klar hervorgehen. Bitte fügen Sie auch einen Kurzlebenslauf bei.

Vor der Auswahl der Autorinnen und Autoren durch die APuZ-Redaktion werden alle eingereichten Exposés anonymisiert. Bewertungskriterien sind Originalität, politische Relevanz und Wissenschaftlichkeit. Die Autorinnen und Autoren haben anschließend bis zum 25. September 2023 Zeit, ihre Beiträge im Umfang von etwa 27 000 Zeichen inkl. Leerzeichen und Fußnoten zu schreiben. Diese werden in der Print- wie auch in der Online-Ausgabe der APuZ veröffentlicht.

„Aus Politik und Zeitgeschichte“ – die Beilage zur Wochenzeitung „Das Parlament“ – wird von der Bundeszentrale für politische Bildung herausgegeben. Sie veröffentlicht wissenschaftlich fundierte, allgemein verständliche Beiträge zu zeitgeschichtlichen und sozialwissenschaftlichen Themen sowie zu aktuellen politischen Fragen. Die Zeitschrift ist ein Forum kontroverser Diskussion, führt in komplexe Wissensgebiete ein und bietet eine ausgewogene Mischung aus grundsätzlichen und aktuellen Analysen. Sie fungiert als Scharnier zwischen Wissenschaft, politischer Bildung und breiter Öffentlichkeit.

Wir freuen uns auf Ihre Zuschriften!

Bundeszentrale für politische Bildung
Redaktion „Aus Politik und Zeitgeschichte“
Adenauerallee 86
53113 Bonn

apuz@bpb.de
www.bpb.de/apuz
twitter.com/apuz_bpb

Herausgegeben von der
Bundeszentrale für politische Bildung
Adenauerallee 86, 53113 Bonn

Redaktionsschluss dieser Ausgabe: 19. Mai 2023

ISSN 0479-611 X

bpb:

APuZ

Nächste Ausgabe
25/2023, 19. Juni 2023

ÖFFENTLICH-RECHTLICHER RUNDFUNK

bpb:

APuZ

AUS POLITIK UND ZEITGESCHICHTE

www.bpb.de/apuz