ATHENE Whitepaper

Aktive Cyberabwehr[1]

10. Oktober 2022[2]

Prof. Dr. Haya Shulman
Fraunhofer-Institut für Sichere Informationstechnologie SIT,
Institut für Informatik, Goethe-Universität Frankfurt am Main *und*
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
haya.shulman@sit.fraunhofer.de

Prof. Dr. Michael Waidner
Fraunhofer-Institut für Sichere Informationstechnologie SIT,
Fachbereich Informatik, Technische Universität Darmstadt *und*
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE

michael.waidner@sit.fraunhofer.de

[1] Teile dieses Whitepaper sind erschienen als: Haya Shulman, Michael Waidner: Der Weg zur aktiven Cyberabwehr; Frankfurter Allgemeine Zeitung FAZ, 25.April 2022, Seite 18 (https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html).

[2] Für die jeweils aktuelle Version dieses Whitepapers siehe https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf

ATHENE
National Research Center for Applied Cybersecurity

Impressum

Kontaktadresse
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Herausgeber
Fraunhofer-Institut für Sichere Informationstechnologie SIT

Hinweise
Die in diesem Dokument enthaltenen Arbeitsergebnisse sind sorgfältig und unter Zugrundelegung des bekannten Standes der Wissenschaft erstellt worden, stellen jedoch Forschungsansätze dar. Eine Haftung oder Garantie dafür, dass die Arbeitsergebnisse bzw. Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird aus diesem Grund nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse bzw. Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Zusammenfassung

Unter aktiver Cyberabwehr verstehen wir eine Reihe von Technologien und Maßnahmen, die Strafverfolgungsbehörden dabei unterstützen können, Straftaten im Cyberraum zu verhindern, abzumindern oder zu verfolgen. Im Folgenden diskutieren wir vier Klassen solcher Maßnahmen: I) Manipulation des Internet-Verkehrs, II) Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerk-Ressourcen, III) Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer, IV) Eingriffe in für Angriffe genutzte Systeme. Für alle vier Klassen geben wir Beispiele für konkrete Maßnahmen.

Aktive Cyberabwehr wird in der Öffentlichkeit häufig mit Hackbacks gleichgesetzt. Unter einem Hackback versteht man allerdings einen digitalen Vergeltungsangriff gegen den Cyberangreifer, also eine Maßnahme, die auf Rache angelegt ist, nicht auf die Verfolgung und Vereitelung von Straftaten. Hackbacks werden deshalb von Politik und Wissenschaft nahezu einhellig abgelehnt. Bedauerlicherweise führt die fälschliche Gleichsetzung von aktiver Cyberabwehr und Hackbacks aber dazu, dass auch aktive Cyberabwehr oft pauschal abgelehnt wird.

Ein Ziel dieses Whitepapers ist deshalb, zur Versachlichung der Diskussion zur aktiven Cyberabwehr beizutragen. Man sollte Maßnahmen, die zu einer Verbesserung der Cybersicherheit führen können, nicht pauschal ablehnen, sondern sie verstehen und so gestalten, dass bei ihrem Einsatz die positiven Effekte die negativen bei weitem ausgleichen oder die negativen Effekte gänzlich vermieden werden.

1 Zum Stand der Cybersicherheit

Die eigene IT konsequent abzusichern, ist das wichtigste Instrument, um Cyberangriffe abzuwehren. Trotz aller Fortschritte in der Weiterentwicklung und der Verbesserung der IT-Sicherheit hat sich die Cybersicherheitslage bislang im Vergleich zu den Vorjahren allerdings nicht wesentlich verbessert. Laut Bitkom entstanden 2021 in der deutschen Wirtschaft Schäden von rund 203 Milliarden Euro durch Angriffe auf IT; 84% aller Unternehmen waren betroffen.[3] Die gegenwärtige geopolitische Situation gibt keine Hoffnung auf Besserung. Ganz im Gegenteil: Schlechte wirtschaftliche Aussichten begünstigen Cyberkriminalität. Der Krieg Russlands gegen die Ukraine, die Spannungen mit China, die Lage im Iran führen alle zu mehr Spionage und vermutlich auch zu mehr Sabotage.

Die Ziele der Angreifer sind vielfältig, es geht um Spionage, Erpressung, Raub von Kryptowährungen, Identitätsdiebstahl zum Kreditkartenbetrug, Desinformation zur Destabilisierung, Sabotage und die Zerstörung physischer Systeme. Häufig sollen Systeme auch „nur" lahmgelegt werden. Die Urheber von Cyberangriffen reichen von Einzeltätern über kriminelle Gruppen, die Angriffe als Dienstleistung anbieten, bis hin zu Gruppen, die im Auftrag von Staaten operieren und gezielt vorgehen.

Die Erfahrung der letzten Jahre zeigt: mit ausreichend Zeit, Geld und Aufwand gelangen organisierte Cyberkriminelle und staatlich unterstützte Cyberangreifer fast immer an ihr Ziel. Das ist nicht völlig überraschend, da es sehr viel einfacher ist, Cyberangriffe durchzuführen als diese zu verhindern. Eine Konsequenz ist der aktuelle Fokus der Branche auf Cyberresilienz, also die Frage: Wie kann sich eine Organisation so absichern und vorbereiten, dass der Schaden durch Cyberangriffe minimiert und möglichst schnell und ohne existenzielle Folgen behoben werden kann? Dahinter stecken Technologien wie Zero Trust Architekturen, die die Ausbreitungsmöglichkeiten von Angreifer stark begrenzen, und Methoden aus dem Business Continuity Management, ausgerichtet auf Cyberangriffe.

Die andere Konsequenz und unser Thema in diesem Whitepaper ist die Diskussion um aktive Cyberabwehr, also Methoden und Technologien, die Cyberangriffe blockieren und verhindern, indem sie in IT-Infrastrukturen außerhalb der Systeme der angegriffenen Opfer eingreifen.

2 Was ist aktive Cyberabwehr?

Für die meisten Cyberangriffe benötigen die Angreifer Netze, Server und mehr, also eine eigene IT-Infrastruktur. Die Verteilung von Schadsoftware erfolgt oft durch vom Angreifer aufgesetzte, gefälschte Webseiten. Um einmal installierte Schadsoftware zu kontrollieren, zu aktualisieren und gestohlene Daten abgreifen zu können, bauen die Angreifer eine sogenannte Command-and-Control (C2)-Infrastruktur im Internet auf: Ransomware erhält so das Kommando, Daten an die C2-Infrastruktur zu schicken und lokal zu verschlüsseln. Spionagesoftware wird so direkt gesteuert. Die Bots in einem Botnetz erhalten so beispielsweise das Kommando, einen DDoS-Angriff durchzuführen und

[3] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

das Opfer mit Nachrichten zu fluten. Auch um Nachrichten im Internet über Server der Angreifer umzuleiten oder das Opfer ganz vom Internet abzuhängen braucht es eine entsprechende Infrastruktur.

Wird ein Angriff entdeckt, so ist es in vielen Fällen möglich, diese IT-Infrastruktur der Angreifer im Internet zu lokalisieren, also festzustellen, welche Netze, Internet-Domänen, IP-Adressbereiche und Server für den Angriff genutzt werden. Mit etwas mehr Aufwand gelingt dies oft sogar dann, wenn die Angreifer Anonymisierungsdienste verwenden.[4,5] Lokalisierung bedeutet allerdings nicht, sofort zu wissen, welche Person, Gruppe oder welches Land hinter einem Angriff steckt. Diese sogenannte Attribution ist deutlich schwieriger als die Lokalisierung, da Angreifer im Allgemeinen ihre Identität und Herkunft bewusst verschleiern und oft sogar unter „Falscher Flagge" operieren, etwa indem sie Hinweise auf andere Hackergruppen und andere Länder streuen.[6,7] Gelingt die Lokalisierung, so gehen Strafverfolgungsbehörden, allen voran das FBI in den Vereinigten Staaten, vermehrt gegen solche Angriffsinfrastrukturen vor. Beispielsweise gab das amerikanische Justizministerium Anfang April bekannt, dass das dem russischen Geheimdienst GRU zugeschriebene Botnet „Cyclops Blink" ausgeschaltet wurde.[8] Hierdurch wurden laufende Angriffe gestoppt und künftige Angriffe verhindert.

Dieses Vorgehen ist ein typisches Beispiel für aktive Cyberabwehr. Im Gegensatz zu den USA ist die aktive Cyberabwehr in Deutschland umstritten. Die öffentliche Diskussion hierzulande ist oft geprägt von Missverständnissen, vorgefassten Meinungen und eingeschränkten Vorstellungen davon, wie aktive Cyberabwehr tatsächlich funktioniert. Oft wird deshalb das Konzept pauschal abgelehnt und nicht differenziert nach Ausprägungen, die einen hohen Mehrwert bei überschaubarem Risiko schaffen, und solchen, bei denen einem hohen Risiko kein entsprechend hoher Mehrwert gegenübersteht.

Wenn von aktiver Cyberabwehr die Rede ist, geht es nicht um „Hackbacks", also nicht um digitale Vergeltungsangriffe und nicht um die Cyberfähigkeiten der Bundeswehr, sondern darum, die Strafverfolgungsbehörden dabei zu unterstützen, Straftaten zu vereiteln und zu verfolgen.

Bundesinnenministerin Faeser spricht sich für aktive Cyberabwehr und gegen Hackbacks aus: *„Die Gefahr durch Cyberangriffe hat sich massiv erhöht. Und passive Sicherungsmaßnahmen allein reichen nicht immer aus, um diesen zu begegnen. Stattdessen brauchen wir auch gefahrenabwehrende Befugnisse, mit denen Cyberangriffe verhindert, beendet oder zumindest abgeschwächt werden. […]*

[4] Xinwen Fu, Zhen Ling: One Cell is Enough to Break Tor's Anonymity; Black Hat DC 2009 (https://www.blackhat.com/presentations/bh-dc-09/Fu/BlackHat-DC-09-Fu-Break-Tors-Anonymity.pdf).

[5] Joseph Cox: Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds; VICE, Feb. 2016 (https://www.vice.com/en/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds).

[6] Andy Greenberg: A Brief History of Russian Hackers' Evolving False Flags; Wired, Oct. 21, 2019 (https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/).

[7] Es gibt aber auch Beispiele erfolgreicher Attribution, z.B. https://interaktiv.br.de/elite-hacker-fsb/en/index.html.

[8] Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU); The United States Department of Justice, April 6, 2022 (https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation).

Ich betone: Das bedeutet nicht, dass wir auf „Vergeltungsschläge" abzielen, die gemeinhin als „Hackbacks" bezeichnet werden."[9] Auch im Koalitionsvertrag hat sich die Bundesregierung klar gegen Vergeltungsangriffe als Mittel der Cyberabwehr ausgesprochen.[10]

Es gibt viele Methoden der aktiven Cyberabwehr – über Schwachstellen in die Server von Angreifern einzubrechen, ist nur eine davon, und diese ist weder die wichtigste noch die effizienteste. Aktive Cyberabwehr umfasst allgemein technische Maßnahmen, die Angriffe stoppen oder proaktiv verhindern sollen, indem sie in die Infrastrukturen oder digitalen Ressourcen der Angreifer eingreifen. Dafür gibt es grundsätzlich vier Ansätze (siehe Abbildung 1).

I. Manipulation des Internet-Verkehrs → Abschnitt 2.1	**II. Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerk-Ressourcen** → Abschnitt 2.2
III. 2.3 Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer → Abschnitt 2.3	**IV. Eingriffe in für Angriffe genutzte Systeme** → Abschnitt 2.4

Abbildung 1. Möglichkeiten aktiver Cyberabwehr

2.1 Manipulation des Internetverkehrs

Dieser Ansatz zur aktiven Cyberabwehr besteht darin, den Internetverkehr von oder zum Angreifer zu manipulieren. Ist ein Netz identifiziert, von dem aus der Angreifer agiert, kann der Verteidiger gezielt die Nachrichten aus diesem blockieren und dadurch den Angriff stoppen. Wird erkannt, dass der Angreifer Nachrichten für ein bestimmtes Netz im Internet so umlenkt, dass sie über vom Angreifer kontrollierte Netze laufen, so kann der Verteidiger diese Verkehrsumlenkung ganz oder teilweise abwehren. Technisch gibt es eine Vielzahl an Möglichkeiten, den Angreiferverkehr zu manipulieren. Keine davon erfordert, in das Netz des Angreifers einzudringen. Stattdessen greift man in die Kontrollmechanismen des Internets ein. Im Kern geht es immer darum, Konfigurationsdaten zum Beispiel in Routern, Internet Exchange Points (IXPs) wie DE-CIX in Frankfurt, Internetdienstleister, Internet-Registries oder Internet-Registrars zu ändern. Wie genau man das tut, hängt auch davon ab, welche Methoden der Angreifer verwendet.

Zum Hintergrund: Das Internet besteht aus einer Reihe von Netzen, sogenannten Autonomen Systemen (AS), und jedes AS kontrolliert einen oder mehrere zusammenhängende Blöcke von IP-Adressen,

[9] Nancy Faeser: Der resiliente Staat: Die Folgen des Ukraine-Krieges für das digitale Deutschland; Manuskript zur Rede auf der re:publica 2022 (https://www.bmi.bund.de/SharedDocs/reden/DE/2022/faeser-20220609-republica.html).

[10] Mehr Fortschritt wagen; Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP; Berlin, 2021, Seite 16 (https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800).

sogenannte IP-Präfixe. Die einzelnen IP-Adressen bezeichnen die Endpunkte der Kommunikation im Internet, d.h. von ihnen und an sie kann man Nachrichten schicken. Die Kommunikation von einem Sender in einem AS zu einem Empfänger in einem anderen AS erfolgt meist nicht direkt, sondern über eine Reihe von anderen Autonomen Systemen. Deren Auswahl und ihre Reihenfolge, die Route, wird durch einen Mechanismus bestimmt, auf den sich die Internet-Erfinder einst verständigt haben und der den Namen Border Gateway Protocol (BGP) trägt. Sogenannte BGP-Router verwenden Tabellen, die jeweils angeben, über welche Nachbar-Router welche IP-Präfixe zu erreichen sind. Jeder Router kann gegenüber seinen Nachbarn „Announcements" machen, für welche IP-Präfixe er eine gute Route anbieten kann – und diese „Announcements" sind nicht gesichert.

Es gibt nun verschiedene Möglichkeiten, Verkehr im Internet umzulenken. Sehr häufig realisieren Angreifer Verkehrsumleitungen durch eine Methode namens IP-Präfix-Hijacking: Ein Angreifer, der einen BGP-Router kontrolliert, kann einen IP-Präfix seines Opfers einfach dadurch übernehmen (hijacken), dass er ein falsches „Announcement" macht, in dem er behauptet, den IP-Präfix seines Opfers zu besitzen. Akzeptieren die BGP-Router dieses „Announcement", so werden sie alle Nachrichten für diesen IP-Block an den Angreifer schicken, anstatt an das Opfer. Als Gegenmaßnahme kann der Verteidiger wiederum selbst ein „Announcement" machen, nachdem er einen Teil dieses gehijackten IP-Präfixes besitzt. BGP gibt „Announcements" für kleinere IP-Präfixe eine höhere Priorität, nach und nach wird die Verkehrsumleitung für diesen Teil darum abgewehrt. Und das ist nur eine Methode, um eine Verkehrsumlenkung abzuwehren.

Auch um angreifende Netze zu blockieren, gibt es verschiedene Wege. Einer nutzt die sogenannte „Resource Public Key Infrastructure" (RPKI). RPKI setzt sich langsam im Internet durch und ist eigentlich dazu gedacht, unter anderem IP-Präfix-Hijacking zu verhindern mittels Zertifikaten darüber, wer welche IP-Präfixe besitzt. In Kooperation etwa mit einer der Organisationen, die für die Verwaltung von Internet-Ressourcen verantwortlich sind (z.B. RIPE NCC in Europa) kann der Verteidiger ein RPKI-Zertifikat erzeugen, das der Routing-Information für das angreifende Netz widerspricht. RPKI sorgt dann dafür, dass der Verkehr dieses Netzes nach und nach aus dem Internetverkehr herausgefiltert wird und sein Ziel nicht mehr erreicht.

Maßnahmen zur Manipulation des Internetverkehrs haben den Vorteil, dass sie – sobald die Entscheidung zum Einsatz gefallen ist – gut automatisiert werden können. Dies setzt allerdings eine entsprechend gut vorbereitete Zusammenarbeit zwischen den Beteiligten voraus, also Strafverfolgungsbehörden, ISPs, Internet Registries, Registraren.

2.2 Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerk-Ressourcen

Zur aktiven Cyberabwehr kann man auch die für einen Angriff genutzten Netzwerk-Ressourcen komplett übernehmen oder abschalten. Hierdurch kann man beispielsweise manche DDoS-Angriffe stoppen oder die Kommunikation zwischen einem Botnetz und seiner C2-Infrastruktur unterbinden und

das Botnetz damit effektiv unschädlich machen. Da C2-Infrastrukturen üblicherweise für sehr viele Angriffe verwendet werden, stoppt diese Maßnahme nicht nur laufende Angriffe, sondern verhindert auch künftige. Es gibt viele praktische Beispiele für diese Möglichkeit der aktiven Cyberabwehr. Beispielsweise gelang es im Jahr 2020 in den Vereinigten Staaten, die Server-Infrastruktur des Trickbot-Botnetzes zu lokalisieren.[11] Nach einem Gerichtsbeschluss wurden alle genutzten IP-Adressen deaktiviert, so dass die Angreifer den Zugriff auf ihre Infrastruktur verloren. Im Allgemeinen setzt ein solcher Vorgang die Kooperation einer Internet-Registry, z.B. in Europa RIPE NCC, voraus.

Sehr häufig werden Internet-Domänen, die von Angreifern zum Beispiel für eine C2-Infrastruktur verwendet werden, übernommen und etwa auf Systeme von Strafverfolgungsbehörden umgelenkt. Dieser Vorgang setzt wiederum die Zusammenarbeit mit der Organisation voraus, welche die jeweilige übergeordnete Domäne verwaltet. Beispielsweise wurden Anfang 2022 in den Vereinigten Staaten 65 Domänen abgeschaltet, die für die C2-Infrastruktur des Zloader-Botnets verwendet wurden.[12]

2.3 Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer

Cyberangriffe betreffen oft gleichzeitig eine große Anzahl von Opfern, insbesondere Angriffe mit Schadsoftware, die darauf abzielen, viele Bots in ein Botnetz einzugliedern. Manche Botnetze bestehen aus Hunderttausenden korrumpierten Geräten. Diese Botnetze werden oft wiederum für Angriffe gegen eine möglichst große Zahl von Opfern verwendet.

Die Schadsoftware in jedem Bot einzeln zu beseitigen, würde zu großen Aufwand verursachen. Statt dessen wehrt man solche Angriffe ab, indem bei möglichst allen Opfern zentral gesteuert die vom Angreifer installierte Schadsoftware gelöscht und die zur Installation genutzten Schwachstellen geschlossen werden. Auch hierfür stehen mehrere Möglichkeiten zur Verfügung.

Gelingt es, die C2-Server eines Botnetzes zu übernehmen, so kann man diese C2-Server oft auch dazu verwenden, die Bots abzuschalten. Auf diese Weise wurde 2021 das Emotet-Botnetz abgeschaltet, unter maßgeblicher Mitarbeit des Bundeskriminalamtes und der Generalstaatsanwaltschaft Frankfurt am Main.[13]

[11] Tom Burt: New action to combat ransomware ahead of U.S. elections; Microsoft, October 12, 2020 (https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/).

[12] Amy Hogan-Burney: Notorious cybercrime gang's botnet disrupted; Microsoft, April 13, 2022 (https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/).

[13] Infrastruktur der Emotet-Schadsoftware zerschlagen; Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main -ZIT- und des Bundeskriminalamtes vom 27. Januar 2021 (https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html).

Eine weitere Möglichkeit wurde im April 2021 in den USA verwendet, um eine von vermutlich chinesischen Hackern, der Gruppe „Hafnium", in Microsoft Exchange Servern eingebaute Hintertüre zu beseitigen: das FBI verwendete diese Hintertüre selbst, um die Server anzuweisen, sie zu schließen.[14]

Kooperieren die Hersteller der von einem Cyberangriff betroffen Systeme, so kann man deren Mechanismus zur Behebung von Schwachstellen (Patch-Funktion) zur Beseitigung der Schadsoftware verwenden. Technisch betrachtet ist die Kooperation der Opfer hierfür nicht notwendig. Auf diese Weise wurde im April 2022 das eingangs erwähnte Cyclops-Blink Botnetz abgeschaltet.[8] Für dessen C2-Infrastruktur wurden Tausende Netzwerkgeräte verwendet. In Kooperation mit den Herstellern dieser Netzwerkgeräte konnte die gesamte C2-Infrastruktur beseitigt werden, wodurch die Hackergruppe Sandworm die Kontrolle über ihr Botnetz verlor.

2.4 Eingriffe in für Angriffe genutzte Systeme

Der vierte Ansatz zur aktiven Cyberabwehr besteht darin, in von einem Angreifer genutzte Ressourcen – Endgeräte, Server, virtuelle Maschinen – einzugreifen. Kooperiert der Hersteller des Angreifersystems, so kann dieser beispielsweise schon während der Produktion oder später über die Patch-Funktion eine Hintertür in das Angreifersystem einbauen. Ein Beispiel für diesen Ansatz wurde im Jahr 2021 bekannt, allerdings nicht zur Cyberabwehr, sondern zur Abwehr von Drogenkriminalität: In der Operation „Trojan Shield" wurde über eine Tarnfirma ein scheinbar sicheres Krypto-Handy an Kriminelle vermarktet.[15] Tatsächlich konnten die Ermittler von FBI, Europol und der australischen Bundespolizei die Mobiltelefone problemlos abhören und so 800 Verdächtige festnehmen.

In diese Kategorie fällt prinzipiell auch der Ansatz, in Standards und Implementierungen von Verschlüsselungssystemen versteckte oder offene Hintertüren für die Strafverfolgungsbehörden einzubauen. In der Cybersicherheitsforschung wird dieser Ansatz durchweg abgelehnt, da solche Hintertüren einerseits für die normalen Benutzer ein Sicherheitsrisiko darstellen und andererseits Cyberkriminelle diese Hintertüren umgehen können, indem sie andere Verschlüsselungsverfahren verwenden.

Aber auch ohne Hintertüren kann in Systeme von Angreifern eingedrungen werden, etwa mittels Passwörter, die man auf andere Weise ermittelt oder im Darknet gefunden hat, dank Fehlkonfigurationen in Systemen und Protokollen. veralteter Kryptographie oder unter Ausnutzung von Schwachstellen in der Soft- und Hardware. Erfahrungsgemäß finden sich in fast allen Organisationen solche

[14] Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities; The United States Department of Justice, April 13, 2021 (https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange).

[15] David Klaubert, Katharina Iskandar, Jan Schiefenhövel: Wer nicht spurt, stirbt; Frankfurter Allgemeine Zeitung FAZ, 27.3.2022 (https://www.faz.net/aktuell/rhein-main/anom-verfahren-bringen-deutsche-gerichte-an-ihre-grenzen-17910424.html)

Probleme. Die Verwendung von „Zero Days", also Schwachstellen, die dem Hersteller nicht bekannt sind und die deshalb auch nicht gepatcht sein können, braucht es deshalb tendenziell gar nicht.

Umgekehrt wird die Verwendung von „Zero Days" für die aktive Cyberabwehr oft kritisch gesehen. Die vorherrschende Meinung in der Cybersicherheitsforschung ist, dass „Zero Days" nicht für die aktive Cyberabwehr zurückgehalten, sondern möglichst rasch den Herstellern gemeldet und von diesen behoben werden sollten. Es gibt zwar Vorschläge für Prozesse, wie man den Nutzen einer bestimmten Schwachstelle für die aktive Cyberabwehr gegen das Risiko abwägen kann, dass diese Schwachstelle auch für Cyberangriffe ausgenutzt wird. Allerdings ist fraglich, wie zuverlässig diese Prozesse in der Praxis funktionieren, und wie realistisch die dahinterstehende Annahme ist, dass eine solche „Zero Day"-Schwachstelle auch tatsächlich nur den Strafverfolgungsbehörden bekannt ist. Tatsächlich wurden den amerikanischen Geheimdiensten NSA[16] und CIA[17] schon Hacking-Werkzeuge gestohlen, ebenso dem Sicherheitsdienstleister Gamma Group[18].

Ein aktuelles Beispiel für diesen Ansatz ist die Aktion des FBI gegen Darkside, jene Gruppe, die für den Ransomware-Angriff auf Colonial Pipeline im Jahr 2021 verantwortlich war.[19] Dem FBI gelang es, das Passwort für das Bitcoin-Wallet der Angreifer zu bestimmen, und so einen großen Teil des Lösegeldes zurückzuholen. Diese Art von Maßnahmen erfordert im Allgemeinen eine sehr umfangreiche Vorbereitung und ist nur in sehr geringem Ausmaß automatisierbar.

3 Aktive Cyberabwehr in Deutschland

Die öffentliche Diskussion zum Thema aktive Cyberabwehr ist in Deutschland durch eine Reihe von Missverständnissen belastet. Wie schon in Kapitel 2 erläutert, wird aktive Cyberabwehr oft mit Hackback im Sinne von digitalen Gegen- oder Vergeltungsangriffen gleichgesetzt. In Deutschland ist das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr unter gewissen Voraussetzungen und im Rahmen des Bundeswehrauftrags zu solchen Gegenangriffen befugt. Mit aktiver Cyberabwehr zur Unterstützung der Vereitelung oder Verfolgung von Straftaten hat dies allerdings nichts zu tun, und die Strafverfolgung gehört auch nicht zum Auftrag der Bundeswehr.

Ein weiteres Missverständnis beruht auf Unwissen über die technischen Möglichkeiten. Sehr häufig wird aktive Cyberabwehr darauf reduziert, dass Strafverfolgungsbehörden in die Server der Angreifer eindringen. Dies ist allerdings nur eine der in Abschnitt 2.4 genannten Methoden. Die Ablehnung dieser Methode wird begründet durch die vermeintliche Notwendigkeit von Zero Day Schwachstellen.

[16] Scott Shane, Nicole Perlroth, David E. Sanger, Security Breach and Spilled Secrets Have Shanken the NSA to Its Core; New York Times, Nov. 12, 2017 (https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html)

[17] Scott Shane, Matthew Rosenberg. Andrew W. Lehren: WikiLeaks Releases Trove of Alleged CIA Hacking Documents; New York Times, March 7, 2017 (https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html).

[18] Steve Ragan: Hacking Team hacked, attackers claim 400GB in dumped data; CSO, July 6, 2015 (https://www.csoonline.com/article/2943968/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html).

[19] Nicole Perlroth, Erin Griffith, Katie Benner: Pipeline Investigation Upends Idea That Bitcoin Is Untraceable; ; New York Times, June 9, 2021 (https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html).

Wie in Abschnitt 2.4 erläutert, sehen auch wir die Zurückhaltung von Zero Day Schwachstellen durch staatliche oder andere Stellen kritisch. Allerdings sind Zero Day Schwachstellen in der Praxis für die in Abschnitt 2.4 genannten Methoden häufig überhaupt nicht notwendig.

Trotz der Vorbehalte gegen aktive Cyberabwehr beteiligten sich deutsche Behörden bereits erfolgreich an international durchgeführten Maßnahmen zur aktiven Cyberabwehr. Die bekannteste ist die Abschaltung des Emotet-Botnetz im Jahr 2021, an der das Bundeskriminalamt (BKA) und die Generalstaatsanwaltschaft Frankfurt am Main maßgeblich beteiligt waren; siehe auch Abschnitt 2.3.[13] Die Aktion beseitigte Schadsoftware von Opfersystemen im In- und Ausland. Allgemein wird die Aktion als Erfolg gewertet, aber zugleich kritisiert, BKA und Staatsanwaltschaft hätten dafür keine belastbare Rechtsgrundlage gehabt.[20,21]

Mit der Änderung des BSI-Gesetzes im Juni 2021 erhielt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in §§7b-d eine Reihe erweiterter Befugnisse zur aktiven Cyberabwehr.[22] Insbesondere kann das BSI danach selbst Netze scannen und so Schwachstellen und Angriffe möglicherweise schneller identifizieren, Internetverkehr eines Angreifers auf das BSI umleiten lassen und analysieren, und es kann Diensteanbieter und Anbieter von Telemediendiensten anweisen, Schwachstellen und Schadsoftware auf Systemen unter ihrer Kontrolle zu beseitigen. Zur Anwendung dieser Befugnisse gibt es allerdings noch keine uns bekannten Erfahrungen. Schon zuvor arbeitete das BSI mit Diensteanbietern im In- und Ausland zusammen und informierte diese z.B. über gefunden C2-Server, was diese typischerweise im Rahmen ihrer AGB dazu befugt, solche Server von der Kommunikation auszuschließen.

Die gesetzlichen Befugnisse des BSI gelten allerdings nur innerhalb Deutschlands. Um international tätig werden zu können, müssen sich die zuständigen Behörden in den betroffenen Ländern untereinander und entsprechend ihren jeweiligen rechtlichen Möglichkeiten und politischen Interessen koordinieren. Dies erfordert meist persönliche Kontakte, gelingt aufgrund unterschiedlicher politischer Interessen keineswegs immer, und benötigt einen Zeitaufwand, der sich selbst im besten Fall

[20] Andre Meister: BKA nutzt Emotet-Takedown als Türöffner für mehr Befugnisse und neue Gesetze; netzpolitik.org, 22.03.2021 (https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/).

[21] Sven Herpig: Active Cyber Defense Operations. Assessments and Safeguards; Stiftung Neue Verantwortung, Berlin, Nov. 4, 2021 (https://www.stiftung-nv.de/de/publikation/active-cyber-defense-operations-assessment-and-safeguards).

[22] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist:

- §7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (https://www.gesetze-im-internet.de/bsig_2009/__7b.html);
- §7c Anordnungen des Bundesamtes gegenüber Diensteanbietern (https://www.gesetze-im-internet.de/bsig_2009/__7c.html);
- §7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten (https://www.gesetze-im-internet.de/bsig_2009/__7d.html).

meist in Wochen und Monaten misst. Es gibt zudem kaum international etablierte Prozesse, mit denen z.B. Internet-Registrare schnell und rechtssicher auf entsprechende Anfragen nationaler Sicherheitsbehörden reagieren könnten.

4 Deutschland braucht eine sachliche Diskussion

Aktive Cyberabwehr ist ein wichtiges Instrument zur Erhöhung der Cybersicherheit. Laufende Angriffe können abgewehrt und künftige verhindert werden. Aktive Cyberabwehr kann und soll die klassische Cybersicherheit nicht ersetzen, aber sie ist eine unverzichtbare Ergänzung. Manche Angriffe können nur mittels aktiver Cyberabwehr verhindert werden, da sie sich komplett außerhalb des Einflussbereichs der Opfer abspielen.

Um die Diskussion zur aktiven Cyberabwehr zu versachlichen, ist es wichtig, sich zu vergegenwärtigen, dass es in der aktiven Cyberabwehr einzig darum geht, Straftaten im Cyberraum zu vereiteln und zu verfolgen, nicht Angriffe auf Einrichtungen eines fremden Staates zur Vergeltung oder Abschreckung durchzuführen. Der Begriff „Hackback" passt gut zu Vergeltung; dass er in der Diskussion oft mit dem Begriff der aktiven Cyberabwehr gleichgesetzt wird, führt aber in die Irre. In vielen Diskussionen wird aktive Cyberabwehr darüber hinaus reduziert darauf, Schwachstellen in IT-Systemen auszunutzen, um in angreifende Server einzudringen. Es gibt viele gute Argumente, weshalb der Staat ihm bekannte „Zero-Day"-Schwachstellen stets den Herstellern melden und dadurch unterstützen sollte, dass sie diese schnell schließen. Diese Feststellung hat aber mit aktiver Cyberabwehr nur sehr wenig zu tun – denn die meisten Maßnahmen der aktiven Cyberabwehr benötigen überhaupt keine Schwachstellen. Ein häufiger, pauschaler Einwand gegen aktive Cyberabwehr besteht schließlich darin, dass neben dem Angreifer auch unbeteiligte andere Nutzer getroffen werden könnten. Richtig ist, dass die Risiken immer gegeneinander abgewogen werden müssen. Diese Abwägung kann man aber nicht pauschal machen.

Was braucht es nun, um in Deutschland eine Strategie zur aktiven Cyberabwehr zu entwickeln und umzusetzen?

Erstens, es braucht eine sachliche Diskussion, welche Methoden aktiver Cyberabwehr wir prinzipiell wollen, und eine enge Zusammenarbeit zwischen den Behörden, Herstellern, Netzbetreibern und der Cybersicherheitsforschung. Die Koordination solcher Zusammenarbeit gehört zu den Aufgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), die Aufgaben betreffen aber auch z.B. die Kriminal- und Verfassungsschutzämter sowie die Staatsanwaltschaften des Bundes und der Länder. Darüber hinaus ist eine internationale Abstimmung notwendig, da Maßnahmen aktiver Cybersicherheit sehr häufig grenzüberschreitend umgesetzt werden müssen. Es braucht also auch internationale Abkommen und Prozesse.

Zweitens braucht es sehr viel technischen Sachverstand – die aktive Cyberabwehr war bislang in Deutschland eher Gegenstand politischer und juristischer, aber selten technischer Forschung. Hier

herrscht hoher Nachholbedarf. Dies betrifft die Entwicklung gezielter Methoden gegen verschiedene Angriffsszenarien wie auch die Risikobewertung konkreter Maßnahmen. Beispielsweise bergen Eingriffe in die Internet-Infrastrukturen oft das Risiko unerwünschter Seiteneffekte, die nur durch umfangreiche Simulationen abgeschätzt werden können.

Drittens müssen, um Angriffe abwehren zu können, diese möglichst frühzeitig erkannt und lokalisiert werden. Oft passiert die Erkennung innerhalb weniger Stunden, nach Schätzung des Unternehmens Mandiant dauert dies aber im weltweiten Durchschnitt 21 Tage.[23] Je kürzer diese Zeit ist, desto effektiver wird auch die aktive Cyberabwehr. Viertens erfordern viele der oben genannten Maßnahmen Prozesse über mehrere Organisationen hinweg, die man proaktiv vorbereiten muss. Die Entscheidung, die Maßnahmen durchzuführen, muss aber natürlich individuell, unter Abwägung der Risiken und nach einem rechtsstaatlichen Verfahren getroffen werden.

Der Koalitionsvertrag der aktuellen Bundesregierung kündigt eine Weiterentwicklung der Cybersicherheitsstrategie an. Wie wir lehnt die Koalition Hackbacks als Mittel der Cyberabwehr ab. Es ist aber wichtig zu klären, welche Mittel der aktiven Cyberabwehr genutzt werden sollen, und die Entwicklung dieser Mittel voranzutreiben. Äußerungen der Bundesministerinnen Faeser und Baerbock lassen hoffen, dass die Bundesregierung Fortschritte in dieser Richtung machen möchte, sowohl national als auch international.

[23] M-Trends 2022,Special Report, Mandiant 2022 (https://www.mandiant.com/m-trends).

Autoren

Prof. Dr. Haya Shulman ist Professorin für Cybersicherheit am Institut für Informatik der Goethe-Universität Frankfurt am Main, Abteilungsleiterin am Fraunhofer-Institut für Sichere Informationstechnologie SIT und für die Goethe-Universität Mitglied im Direktorium des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE.

Prof. Dr. Michael Waidner ist Professor für Sicherheit in der Informationstechnologie am Fachbereich Informatik der Technischen Universität Darmstadt, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie SIT und CEO des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE.

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt

Web: https://www.sit.fraunhofer.de

Email: {vorname.nachname}@sit.fraunhofer.de

ATHENE

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft unter Mitwirkung der Fraunhofer-Institute SIT und IGD sowie der Hochschulen TU Darmstadt, Goethe-Universität Frankfurt und Hochschule Darmstadt. ATHENE ist das größte Forschungszentrum für Cybersicherheit in Deutschland. Es wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK). Die Aufgabe von ATHENE ist es, die digitale Transformation von Wirtschaft, Gesellschaft und Staat aus Sicht der Cybersicherheit und des Privatsphärenschutzes mit anwendungs-orientierter Spitzenforschung und Entwicklung zu begleiten.

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt

Web: https://www.athene-center.de