Miha Creative/AdobeStock

# AKTIVE CYBERABWEHR

Impulspapier | März 2023

## Zusammenfassung

Unter aktiver Cyberabwehr verstehen wir eine Reihe von Technologien und Maßnahmen, die Behörden der Gefahrenabwehr und der Strafverfolgung dabei unterstützen können, Straftaten im Cyberraum abzumildern, zu verhindern oder zu verfolgen. Im Folgenden diskutieren wir vier Klassen solcher Maßnahmen: I) Manipulation des Internetverkehrs, II) Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerkressourcen, 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 sehr allgemein einen digitalen Gegenangriff, der auch rein auf Rache und Vergeltung angelegt sein kann. Hackbacks in dieser Allgemeinheit 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 Impulspapiers[1] 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 überwiegen 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 Prozent aller Unternehmen waren betroffen.[2] 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 oder die Lage im Iran führen alle zu mehr Spionage und vermutlich auch zu mehr Sabotage.

Die Ziele der Angreifenden 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. Initiiert werden Cyberangriffe von einzelnen Personen, kriminellen Gruppen, die Angriffe als Dienstleistung anbieten, oder auch von Gruppen, die im Auftrag fremder Staaten operieren und gezielt vorgehen.

Die Erfahrung der letzten Jahre zeigt: Mit ausreichend Zeit, Geld und Aufwand gelangen organisierte Cyberkriminelle und staatlich unterstützte Gruppen 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 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? Um diese Frage zu adressieren, werden zunehmend Technologien wie Zero-Trust-Architekturen eingesetzt, die die Ausbreitungsmöglichkeiten von Angriffen stark begrenzen, und Methoden aus dem Business Continuity Management, die speziell auf Cyberangriffe ausgerichtet sind. Die andere Konsequenz und unser Thema in diesem Impulspapier ist die Diskussion um aktive Cyberabwehr, also Methoden und Technologien, die Cyberangriffe blockieren und verhindern, indem sie in IT-Infrastrukturen außerhalb der Systeme der Opfer eingreifen.

## 2 Was ist aktive Cyberabwehr?

Für die meisten Cyberangriffe benötigen die Angreifenden Netze, Server und mehr, also eine eigene IT-Infrastruktur. Die Verteilung von Schadsoftware erfolgt oft durch von den Angreifenden aufgesetzte, gefälschte Webseiten. Um einmal installierte Schadsoftware zu kontrollieren, zu aktualisieren und gestohlene Daten abgreifen zu können, bauen die Angreifenden 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 Distributed-Denial-of-Service(DDoS)-Angriff durchzuführen und das Opfer mit Nachrichten zu fluten. Auch um Nachrichten im Internet über Server der Angreifer umzuleiten oder das Opfer ganz vom Internet abzukopplen, braucht es eine entsprechende Infrastruktur.

Wird ein Angriff entdeckt, so ist es in vielen Fällen möglich, diese IT-Infrastruktur der Angreifenden im Internet zu lokalisieren, also festzustellen, welche Netze, Internetdomänen, IP-Adressbereiche und Server für den Angriff genutzt werden. Mit etwas mehr Aufwand gelingt dies oft sogar dann, wenn die Angreifenden Anonymisierungsdienste verwenden.[3,4] 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 Angreifende 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.[5,6] Gelingt die Lokalisierung, so gehen die zuständigen Behörden vermehrt gegen solche Angriffsinfrastrukturen vor, allen voran das Federal Bureau of Investigation (FBI) in den Vereinigten Staaten. Beispielsweise gab das amerikanische Justizministerium im April 2022 bekannt, dass das dem russischen Geheimdienst Glawnoje Raswedywatelnoje Uprawlenije (GRU, zu Deutsch: Hauptverwaltung für Aufklärung) zugeschriebene Botnet „Cyclops Blink“ ausgeschaltet wurde.[7] Hierdurch wurden laufende Angriffe gestoppt und künftige Angriffe verhindert.

Dieses Vorgehen ist ein typisches Beispiel für aktive Cyberabwehr. Während zum Beispiel die USA die aktive Cyberabwehr deutlich ausbauen wollen[8], ist diese 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 digitale Vergeltungsangriffe oder die Cyberfähigkeiten der Bundeswehr, sondern darum, die für Gefahrenabwehr und Strafverfolgung zuständigen Behörden dabei zu unterstützen, Straftaten zu vereiteln und zu verfolgen.

Es gibt viele Methoden der aktiven Cyberabwehr – unter Ausnutzung von 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 Angreifenden eingreifen. Dafür gibt es grundsätzlich vier Ansätze (siehe Abbildung 1), die im Folgenden ausführlicher dargestellt werden. Vorausgeschickt sei, dass die Anwendung dieser Ansätze einen entsprechenden Rechtsrahmen voraussetzt, der in Deutschland bislang nur teilweise existiert, und dass die

| | |
|---|---|
| **I. Internetverkehr manipulieren** → Abschnitt 2.1 | **II. Für Angriffe genutzte Netzwerkressourcen abkoppeln oder übernehmen** → Abschnitt 2.2 |
| **III. Schwachstellen und Schadsoftware auf den Systemen der Opfer beseitigen** → Abschnitt 2.3 | **IV. In für Angriffe genutzte Systeme eingreifen** → Abschnitt 2.4 |

Abbildung 1: Möglichkeiten aktiver Cyberabwehr

Entscheidung zum Einsatz einer bestimmten Maßnahme in einem bestimmten Fall stets nach rechtsstaatlichen Prinzipien erfolgen muss, beispielsweise auf richterliche Anordnung.

### 2.1 Internetverkehr manipulieren

Dieser Ansatz zur aktiven Cyberabwehr besteht darin, den Internetverkehr von oder zu Angreifenden zu manipulieren. Ist ein Netz identifiziert, von dem aus Angreifende agieren, können Verteidigende gezielt die Nachrichten aus diesem blockieren und dadurch den Angriff stoppen. Wird erkannt, dass Angreifende Nachrichten für ein bestimmtes Netz im Internet so umlenken, dass sie über von den Angreifenden kontrollierte Netze laufen, so können die Verteidigenden diese Verkehrsumlenkung ganz oder teilweise abwehren. Technisch gibt es eine Vielzahl an Möglichkeiten, den Angriffsverkehr zu manipulieren. Keine davon erfordert, in das Netz der Angreifenden einzudringen. Stattdessen greift man in die Kontrollmechanismen des Internets ein. Im Kern geht es immer darum, Konfigurationsdaten zu ändern, zum Beispiel in Routern, Internet Exchange Points (IXPs) wie DE-CIX in Frankfurt, bei Internetdienstleistern, Internet-Registries oder Internet-Registraren. Wie genau man das tut, hängt auch davon ab, welche Methoden die Angreifenden verwenden.[9]

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 zum Beispiel zwischen Sicherheits- und Strafverfolgungsbehörden einerseits und Internet Service Providern, Internet Registries oder Registraren andererseits.

### 2.2 Für Angriffe genutzte Netzwerkressourcen abkoppeln oder übernehmen

Zur aktiven Cyberabwehr kann man auch die für einen Angriff genutzten Netzwerkressourcen komplett übernehmen oder abschalten. Hierdurch lassen sich beispielsweise manche DDoS-Angriffe stoppen oder die Kommunikation zwischen einem Botnetz und seiner C2-Infrastruktur unterbinden, wodurch das Botnetz unschädlich wird. 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 Serverinfrastruktur des Botnetzes „Trickbot“ zu lokalisieren.[10] Nach einem Gerichtsbeschluss wurden alle genutzten IP-Adressen deaktiviert, sodass die Angreifenden den Zugriff auf ihre Infrastruktur verloren. Im Allgemeinen setzt ein solcher Vorgang die Kooperation einer Internet-Registry voraus, in Europa zum Beispiel des Réseaux IP Européens Network Coordination Centre (RIPE NCC).

Eine andere, sehr häufig genutzte Methode ist es, Internetdomänen, die Angreifende zum Beispiel für eine C2-Infrastruktur verwenden, zu übernehmen und etwa auf Systeme von Gefahrenabwehr- oder Strafverfolgungsbehörden umzulenken. 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.[11]

### 2.3 Schwachstellen und Schadsoftware auf den Systemen der Opfer beseitigen

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. Stattdessen wehrt man solche Angriffe ab, indem bei möglichst allen Opfern zentral gesteuert die von Angreifenden 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 Server oft auch dazu verwenden, um die Bots zu deaktivieren. Auf diese Weise wurde 2021 das Emotet-Botnetz abgeschaltet, unter maßgeblicher Mitarbeit des Bundeskriminalamtes und der Generalstaatsanwaltschaft Frankfurt am Main.[12]

Eine weitere Möglichkeit wurde im April 2021 in den USA verwendet, um eine vermutlich von chinesischen Hackern der Gruppe „Hafnium“ in Microsoft-Exchange-Servern eingebaute Hintertür zu beseitigen: Das FBI verwendete diese Hintertür selbst, um die Server anzuweisen, sie zu schließen.[13]

Kooperieren die Hersteller der von einem Cyberangriff betroffenen 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 Botnetz „Cyclops Blink“ abgeschaltet. 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“ des russischen Geheimdienstes GRU die Kontrolle über ihr Botnetz verlor.

### 2.4 In für Angriffe genutzte Systeme eingreifen

Der vierte Ansatz zur aktiven Cyberabwehr besteht darin, in von Angreifenden genutzte Ressourcen – Endgeräte, Server, virtuelle Maschinen – einzugreifen. Kooperiert der Hersteller des für den Angriff verwendeten Systems, so kann dieser beispielsweise schon während der Produktion oder später über die Patch-Funktion eine Hintertür in das Angriffssystem 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 abhörsicheres Mobiltelefon an Kriminelle vermarktet.[14] Tatsächlich konnten die Ermittler von FBI, Europol und der australischen Bundespolizei die Mobiltelefone problemlos abhören und so 800 Verdächtige festnehmen.

Eine weitere Methode dieser Kategorie besteht darin, 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 Nutzenden ein Sicherheitsrisiko darstellen und andererseits Cyberkriminelle diese Hintertüren umgehen können, indem sie andere Verschlüsselungsverfahren verwenden.

Aber auch ohne Hintertüren kann in Systeme von Angreifenden 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 öffentlich bekannten Schwachstellen in der Soft- und Hardware. Erfahrungsgemäß finden sich in fast allen Organisationen solche Probleme. Der tatsächliche Eingriff setzt nicht unbedingt eine Lokalisierung voraus, meist genügt eine Kommunikationsbeziehung. Die Verwendung von „Zero Days“, also Schwachstellen, die dem Hersteller nicht bekannt sind und die deshalb auch nicht gepatcht sein können, braucht es deshalb häufig 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 Sicherheits- und Strafverfolgungsbehörden bekannt ist. Tatsächlich wurden den amerikanischen Geheimdiensten National Security Agency (NSA)[15] und Central Intelligence Agency (CIA)[16] schon Hacking-Werkzeuge gestohlen, ebenso den Sicherheitsdienstleistern Gamma Group[17] und Cellebrite[18].

Ein aktuelles Beispiel für den hier behandelten 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 Angreifenden 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 im vorigen Abschnitt erläutert, wird aktive Cyberabwehr oft fälschlicherweise mit Hackback im Sinne von digitalen Gegen- oder Vergeltungsangriffen gleichgesetzt. Auch werden im Zusammenhang mit aktiver Cyberabwehr häufig Fähigkeiten der Bundeswehr diskutiert. Zwar ist das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr zur Wahrnehmung des Verteidigungsauftrags befugt, Cyberoperationen durchzuführen, die Vereitelung und Verfolgung von Straftaten gehören jedoch nicht zum Auftrag der Bundeswehr.

Ein weiteres Missverständnis beruht auf Unwissen über die technischen Möglichkeiten. Sehr häufig wird aktive Cyberabwehr darauf reduziert, dass Sicherheits- und Strafverfolgungsbehörden in die Server der Angreifenden 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. Wie in Abschnitt 2.4 erläutert, sehen auch wir die Zurückhaltung solcher Schwachstellen durch staatliche oder andere Stellen kritisch. Allerdings sind „Zero Day“-

Schwachstellen in der Praxis für die in Abschnitt 2.4 genannten Methoden häufig gar nicht notwendig.

Trotz der Vorbehalte gegen aktive Cyberabwehr beteiligten sich deutsche Behörden bereits erfolgreich an international durchgeführten Maßnahmen zur aktiven Cyberabwehr. Die bislang bekannteste ist die Abschaltung des Botnetzes „Emotet“ im Jahr 2021; siehe auch Abschnitt 2.3.[11] Die Aktion beseitigte Schadsoftware von Opfersystemen im In- und Ausland und wird allgemein als Erfolg gewertet. Jedoch wird zugleich kritisiert, BKA und Staatsanwaltschaft hätten für ihr Handeln keine belastbare Rechtsgrundlage gehabt.[20,21] Ein neueres Beispiel ist die „Operation Dawnbreaker“, an der Ermittlungsbehörden aus den USA und Europa beteiligt waren, darunter auch das BKA und die Kriminalpolizeidirektion Esslingen. Im Juli 2022 gelang es den Ermittlern, sich Zugang zur IT-Infrastruktur der Gruppe Hive zu verschaffen, was dann im Januar 2023 zur vollständigen Übernahme dieser IT-Infrastruktur führte. Hive war vor allem für Ransomware-Angriffe auf Krankenhäuser und andere öffentliche Einrichtungen bekannt. Laut FBI konnte durch die Operation in über 300 Fällen den Opfern geholfen und die Zahlung von rund 130 Millionen US-Dollar verhindert werden.[22,23]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhielt mit der Änderung des BSI-Gesetzes im Juni 2021 in §§7b-d eine Reihe erweiterter Befugnisse zur aktiven Cyberabwehr.[24] Insbesondere kann das BSI danach selbst Netze scannen und so Schwachstellen und Angriffe möglicherweise schneller identifizieren sowie Internetverkehr von Angreifenden auf das BSI umleiten lassen und analysieren. Zudem kann die Cybersicherheitsbehörde Diensteanbieter und Anbieter von Telemediendiensten anweisen, Schwachstellen und Schadsoftware auf Systemen unter ihrer Kontrolle zu beseitigen. Schon zuvor arbeitete das BSI mit Diensteanbietern im In- und Ausland zusammen und informierte diese zum Beispiel über gefundene C2-Server, was diese typischerweise im Rahmen ihrer Allgemeinen Geschäftsbedingungen 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 ihrer 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 meist in Wochen und Monaten misst. Es gibt zudem kaum international etablierte Prozesse, mit denen zum Beispiel Internet-Registrare schnell und rechtssicher auf entsprechende Anfragen nationaler Sicherheitsbehörden reagieren könnten.

## 4 Empfehlungen

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, und nicht darum, 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 darauf reduziert, 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 den Angreifenden auch unbeteiligte andere Nutzende getroffen werden könnten. Richtig ist, dass die Risiken immer gegeneinander abgewogen werden müssen. Diese Abwägung kann man aber nicht pauschal treffen.

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

1. Es braucht eine breite, sachliche Diskussion, welche Methoden aktiver Cyberabwehr wir prinzipiell wollen, und eine enge Zusammenarbeit zwischen den Behörden, Herstellern, Netzbetreibern sowie der Forschung, insbesondere der technischen und juristischen Cybersicherheitsforschung. Die Koordination der Zusammenarbeit unterschiedlicher Behörden im Bereich der Cybersicherheit gehört zu den Aufgaben des BSI. Die Aufgaben betreffen aber zum Beispiel auch die Kriminal- und Verfassungsschutzämter sowie die Staatsanwaltschaften des Bundes und der Länder. Darüber hinaus ist eine

internationale Abstimmung notwendig, da Maßnahmen aktiver Cyberabwehr sehr häufig grenzüberschreitend umgesetzt werden müssen. Es braucht also auch internationale Abkommen und Prozesse. All dies setzt einen gesetzlichen Rahmen voraus, der heute jenseits der sehr beschränkten Befugnisse für das BSI auf Bundesebene noch nicht ausreichend existiert.[20]

2. Es braucht sehr viel technischen Sachverstand – die aktive Cyberabwehr war bislang in Deutschland eher Gegenstand politischer Diskussion, aber selten technischer Forschung. Selbst IT-Sicherheitsexpertinnen und -experten verfügen in den seltensten Fällen über das für die aktive Cyberabwehr notwendige Fachwissen. Hier herrscht hoher Nachholbedarf. Dies betrifft die Entwicklung gezielter Methoden gegen verschiedene Angriffsszenarien wie auch die Risikobewertung konkreter Maßnahmen. Beispielsweise bergen Eingriffe in die Internetinfrastrukturen oft das Risiko unerwünschter Seiteneffekte, die nur durch umfangreiche Simulationen abgeschätzt werden können.
3. Angriffe müssen möglichst frühzeitig erkannt und lokalisiert werden, um sie abwehren zu können. Oft gelingt dies auch innerhalb weniger Stunden nach Schätzung des Unternehmens Mandiant dauert dies aber im weltweiten Durchschnitt 21 Tage.[25] Je schneller Angriffe bemerkt werden, desto effektiver wird auch die aktive Cyberabwehr. Die zur Angriffserkennung notwendige Datenerfassung betrifft häufig auch personenbezogene oder -beziehbare Daten, was eine rechtliche Abwägung zwischen den Zielen „Datenschutz“ und „Angriffserkennung“ notwendig macht.
4. Viele der oben genannten Maßnahmen erfordern 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.

1 Dieses Impulspapier basiert auf dem Artikel „Der Weg zur aktiven Cyberabwehr“ von Haya Shulman und Michael Waidner, erschienen am 25. April 2022 in der Frankfurter Allgemeinen Zeitung FAZ
2 https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
3 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).
4 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).
5 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/).
6 Es gibt aber auch Beispiele erfolgreicher Attribution, z. B. https://interaktiv.br.de/elite-hacker-fsb/en/index.html.
7 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).
8 Fred Kaplan: When It Comes to Cybersecurity, the Biden Administration Is Getting Much More Aggressive; SLATE, January 17, 2023 (https://slate.com/news-and-politics/2023/01/biden-cybersecurity-inglis-neuberger.html).
9 Etwas ausführlicher beschrieben ist dies in Haya Shulman, Michael Waidner: ATHENE Whitepaper Aktive Cyberabwehr; 10.10.2022 (https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf).
10 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/).
11 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/).
12 Infrastruktur der Emotet-Schadsoftware zerschlagen; Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main -ZIT- und des Bundeskriminalamtes vom 27. Januar 2021
13 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).
14 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)
15 Scott Shane, Nicole Perlroth, David E. Sanger, Security Breach and Spilled Secrets Have Shaken the NSA to Its Core; New York Times, Nov. 12, 2017 (https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html)
16 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).
17 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).
18 Claudia Glover: Hacktivists leak data apparently from digital forensics vendors Cellebrite and MSAB; Tech Monitor, January 17, 2023 (https://techmonitor.ai/technology/cybersecurity/spyware-data-leak-hacktivist-msab-cellebrite).
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).
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 Linda Qiu: Justice Dept. Dismantles a Major Ransomware Operation; New York Times, Jan 26, 2023 (https://www.nytimes.com/2023/01/26/us/politics/justice-department-ransomware-hive.html)
23 Volker Briegleb: Polizei übernimmt IT-Infrastruktur der Ransomware-Gruppe „Hive“; Heise News, 27.01.2023 (https://www.heise.de/news/Cybercrime-Polizei-zerschlaegt-Ransomware-Gruppe-Hive-7472192.html)
24 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).
25 M-Trends 2022, Special Report, Mandiant 2022 (https://www.mandiant.com/m-trends).

**Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat**

Die Wissenschaftliche Arbeitsgruppe wurde im Oktober 2018 gegründet und ist Mitglied des Nationalen Cyber-Sicherheitsrats. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner

Hauptautor des Impulspapiers „Aktive Cyberabwehr“: Prof. Dr. Michael Waidner zusammen mit Prof. Dr. Haya Shulman