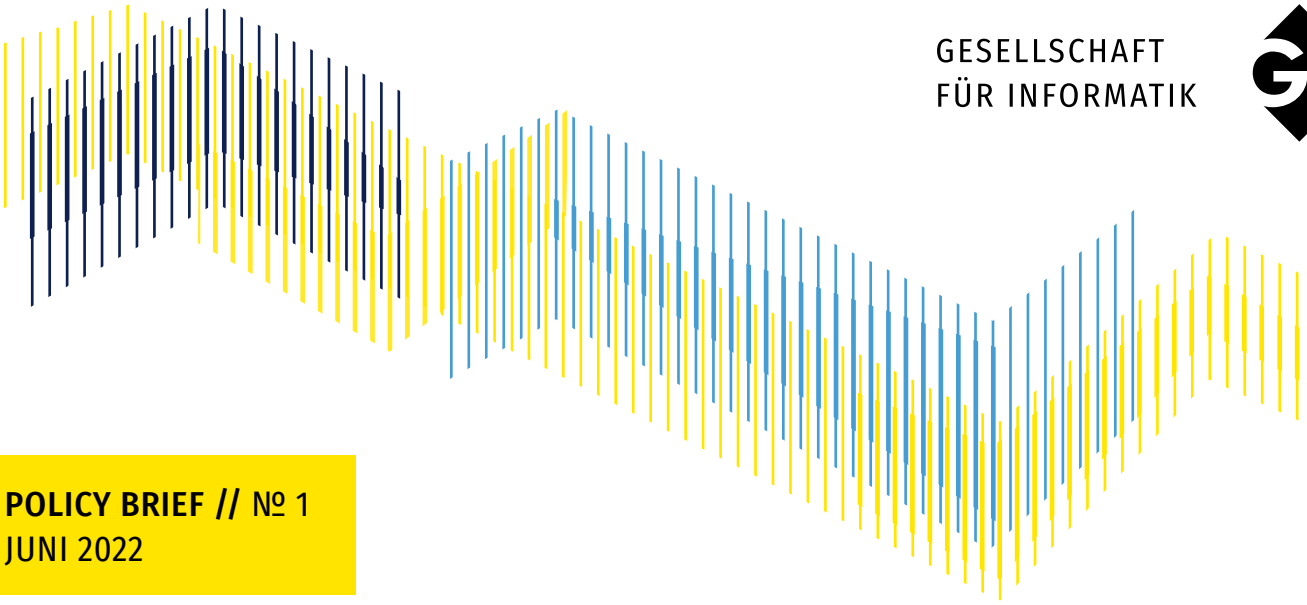

GESELLSCHAFT
FÜR INFORMATIK

POLICY BRIEF // № 1
JUNI 2022

Aktive Cyberabwehr im Angesicht einer sicherheitspolitischen Neuaufstellung

Hannes Federrath, Alexander von Gernler, Nikolas Becker

Mit dem russischen Angriff auf die Ukraine ist auch die Bedeutung von IT-Sicherheit wieder stärker in das Bewusstsein gerückt. Angriffe auf kritische Infrastrukturen, wie auf mehrere Unternehmen der Windenergie-Branche im April/Mai 2022, verdeutlichen die Dringlichkeit einer kurzfristigen Stärkung der europäischen IT-Sicherheit [1]. Auch wenn die Urheberschaft dieser Vorfälle bislang nicht abschließend geklärt ist, so gilt doch spätestens seit dem Angriff auf die IT-Infrastruktur des Deutschen Bundestags im Jahr 2015 als erwiesen, dass auch der russische Geheimdienst GRU entsprechende Cyber-Angriffe initiiert [2].

> **„Expert*innen betonen seit vielen Jahren, dass IT-Sicherheit vor allem präventiv gestaltet werden sollte."**

Hinsichtlich möglicher Gegenstrategien betonen sowohl Expert*innen für Internationale Politik als auch aus dem Bereich Informatik/IT-Sicherheit seit vielen Jahren, dass IT-Sicherheit ausschließlich nicht-intrusiv und vor allem präventiv gestaltet werden sollte. Das heißt, dass insbesondere der Einsatz von Ende-zu-Ende-Verschlüsselung, die mehrseitig sichere Systemgestaltung sowie das koordinierte Schließen von Sicherheitslücken gefördert werden müssen [3, 4]. Diesen Erkenntnissen aus Forschung und Praxis wird auch im Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP von 2021 Rechnung getragen, in dem es heißt: „Wir führen [...] ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, und die Vorgaben ‚security-by-design/default' ein. [...] Wir verpflichten alle staatlichen Stellen, ihnen bekannte Sicherheitslücken beim BSI zu melden und sich regelmäßig einer externen Überprüfung ihrer IT-Systeme zu unterziehen. Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein" [5, S. 16].
Dennoch werden im Zuge der aktuellen Debatte (Mai 2022) auch die Rufe nach einer „aktiven Cyberabwehr" wieder lauter, welche auf das Aufkaufen und Ausnutzen von Sicherheitslücken setzt.
Im Folgenden sollen daher zunächst (1) der Begriff der aktiven Cyberabwehr erläutert und verschiedene Arten der aktiven Cyberabwehr differenziert werden, anschließend unter (2) Argumente gegen intrusive Maßnahmen („Hackbacks") bzw. für einen verantwortungsvollen Umgangs mit Sicherheitslücken vorgebracht werden, sowie schließlich unter (3) nicht-intrusive Handlungsalternativen für eine größere IT-Sicherheit dargelegt werden.

WAS BEDEUTET „AKTIVE CYBERABWEHR"?

Der Begriff der Cyberabwehr „umfasst alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyberangriffen zu verhindern oder abzuschwächen" [6, S. 133]. Dabei muss der Ruf nach einer aktiven Cyberabwehr als Versuch verstanden werden, neben einer defensiven Abwehr, die ausschließlich die eigenen Systeme betrifft, auch Offensivkapazitäten zu errichten.

→

„Nicht-intrusive Maßnahmen bewahren die IT-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit."

Innerhalb der offensiven Maßnahmen lässt sich wiederum zwischen intrusiven und nicht-intrusiven Maßnahmen unterscheiden [7, S. 3]. Nicht-intrusive Maßnahmen zielen lediglich auf die Informationsgewinnung zur Identifikation von möglichen Zielsystemen und deren Schwachstellen ab und beeinträchtigen die IT-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit nicht. So sind beispielsweise Portscans nicht-intrusive Maßnahmen. Intrusive Maßnahmen zielen hingegen auf Aufklärung und Wirkung und umfassen „Hackbacks", mit denen die Infrastruktur eines Angreifenden repressiv geschädigt werden soll. Eine besondere Rolle kommt hierbei den 0-Day-Schwachstellen zu, d. h. Sicherheitslücken, welche nur dem Entdeckenden, nicht aber den Nutzer*innen oder Hersteller*innen der Infrastrukturen bekannt sind. Konkret beinhalten intrusive Maßnahmen zum Beispiel die Übernahme der externen Angreifer-Infrastruktur mit der Möglichkeit deren Funktionen zu stören oder Daten extrahieren oder löschen zu können.

PROBLEME INTRUSIVER MASSNAHMEN: WARUM EIN VERANTWORTUNGSVOLLER UMGANG MIT SICHERHEITSLÜCKEN VONNÖTEN IST

„Das Nicht-Veröffentlichen bekannter Sicherheitslücken ist riskant."

Damit ein Hackback gelingt, müssen die Schwachstellen bekannt sein und geheim gehalten werden. Das Nicht-Veröffentlichen bekannter Sicherheitslücken ist jedoch sehr riskant. Wenn Sicherheitslücken bestehen bleiben, können zum einen Datenschutz und Privatsphäre von vielen Menschen verletzt werden, zum anderen können die Schwachstellen auch gegen die eigene Wirtschaft und Verwaltung gerichtet ausgenutzt werden. Das Geheimhalten des Wissens um Schwachstellen ist zudem teuer. Staatliche Stellen verfügen meist nicht über genügend Wissen um Informationssicherheit. Daher muss dieses auf einem (Schwarz-)Markt erworben werden. Es gibt einen großen Schwarzmarkt für Cyberkriminalität, dessen Volumen auf mehrere Milliarden US-Dollar geschätzt wird [8]. Anstatt diesen kriminellen Schwarzmarkt über Ankäufe weiter zu fördern, sollte man ihn über das Aufdecken von Sicherheitslücken eindämmen.

Schließlich sind Realisierungschancen und tatsächlicher Nutzen von Hackbacks fraglich. Zum einen müssen Hackbacks zeitnah erfolgen, um eine gewünschte Wirkung zu erzielen. Dazu müssen IT-Störungen jedoch zeitnah erkannt werden, was leider selten der Fall ist. So werden schwerwiegende Cyber-Vorfälle in der Industrie erst nach durchschnittlich 200 Tagen bemerkt [3]. Zum anderen muss bekannt sein, gegen wen Hackbacks zu richten sind, um diese zu starten. Es ist allerdings schwierig herauszufinden, woher Cyber-Angriffe tatsächlich stammen. Angreifer*innen agieren in der Regel nicht direkt von ihrem Rechner aus, sondern anonym, über mehrere Rechner hinweg.

KONKRETE HANDLUNGSALTERNATIVEN

Cyberabwehr ist wichtig, sollte sich aus den genannten Gründen jedoch auf nicht-intrusive Maßnahmen beschränken. Intrusive Maßnahmen und die Geheimhaltung des Wissens über Schwachstellen bergen hingegen viele Gefahren und sind nicht unbedingt nützlich.

Ein wirksames Schwachstellenmanagement

„Ein verantwortungsvoller Umgang mit Schwachstellen kann nur darin bestehen, das Wissen darüber nach einer angemessenen Frist zu veröffentlichen."

Daher sollte an den Vereinbarungen des Koalitionsvertrages festgehalten werden und wie bereits in der Cybersicherheitsstrategie von 2021 formuliert, ein →

verbindliches Vorhaben für den verantwortungsvollen Umgang mit 0-Day-Schwachstellen und -Exploits etabliert werden. Dieser kann nur darin bestehen, das Wissen über eine Schwachstelle nach einer angemessenen Frist (Responsible Disclosure) vollständig zu veröffentlichen. Es sollte zudem ein koordinierter und transparenter Austausch über Sicherheitslücken innerhalb von Regierungsbehörden etabliert und der Umgang mit (Nicht-0-Day) Schwachstellen in einer Government Disclosure Policy festgehalten werden.

Stärkung der IT-Sicherheitsforschung

Die verantwortungsvolle Forschung an und Aufdeckung von Sicherheitslücken dienen dem Gemeinwohl. Ethische Hacker*innen müssen daher mit einer klaren Rechtslage gestärkt werden, die die strafrechtliche Verfolgung für Handlungen im Rahmen der Forschung ausschließt. Zum anderen sollte die IT-Sicherheitsforschung institutionell gestärkt werden, um IT-Systeme von vornherein robuster und sicherer zu gestalten.

Bekämpfung des Sicherheitslücken-Schwarzmarkes

Sobald Sicherheitslücken bekannt werden, können diese nicht mehr am Schwarzmarkt gehandelt werden. Um den Schwarzmarkt zu schwächen, sollte daher ein offener Umgang mit Sicherheitslücken unterstützt werden. Möglichkeiten hierfür sind Hackerwettbewerbe oder Bug-Bounty-Wettbewerbe, auf denen Hacker*innen Systeme nach möglichen Sicherheitslücken durchforsten. Hacker*innen bekämen so nicht nur legale finanzielle, sondern auch soziale Anerkennung. Es sollte außerdem ein institutioneller Rahmen geschaffen werden, in dem Sicherheitslücken gemeldet werden können [3].

Stärkung der Softwaresicherheit

> **„Hersteller müssen noch stärker für die IT-Sicherheit ihrer Produkte in Haftung genommen werden."**

Die Entwicklung und Instandhaltung sicherer Softwareprodukte müssen gestärkt werden, da Angriffe besonders dann gefährlich sind, wenn sie auf eine schlecht gewartete Infrastruktur treffen. Das bedeutet zum einen, dass Unternehmen stärkere IT-Sicherheitsstandards, insbesondere Ende-zu-Ende-Verschlüsselung und die mehrseitig sichere Systemgestaltung [9], etablieren beziehungsweise bereits im Entwicklungsprozess berücksichtigen und in den kompletten Lebenszyklus ihrer Produkte integrieren müssen (security by design). Zum anderen müssen Hersteller noch stärker für die IT-Sicherheit ihrer Produkte in Haftung genommen werden.

Förderung von Offenheit und Transparenz in der Softwareentwicklung

Zum anderen sollten offene und transparente Entwicklungsprozesse gefördert werden, um die Sicherheit von Software zu erhöhen. Die Entwicklung von Open-Source-Software sollte gestärkt werden und die Auditierung wichtiger Open-Source-Projekte im Sinne der allgemeinen Daseinsvorsorge staatlich gefördert werden.

→

LITERATUR

[1] S. Frost, “Windstrom im Visier von Cyberkriminellen - Tagesspiegel background,” Tagesspiegel.de. [Online]. Verfügbar unter: *https://background.tagesspiegel.de/energie-klima/windstrom-im-visier-von-cyberkriminellen. [Abgerufen am 7.6.2022].*

[2] C. Grozev, “Who is Dmitry Badin, the GRU hacker indicted by Germany over the Bundestag hacks?,” bellingcat, 06-May-2020. [Online]. Verfügbar unter: *https://www.bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/. [Abgerufen am 7.6.2022].*

[3] M. Schulze, Stiftung Wissenschaft und Politik, “Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik.” Deutsches Institut für Internationale Politik und Sicherheit, 2019.

[4] Gesellschaft für Informatik, „Stellungnahme zum Entwurf für die Cybersicherheitsstrategie,“. Gesellschaft für Informatik e.V., 2021. *https://gi.de/fileadmin/GI/Allgemein/PDF/2021-06-16_GI-StN_CSS_2021.pdf*

[5] SPD, Bündnis 90 / Die Grünen, FDP, „Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021— 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP)“, 2021. *https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf*

[6] Bundesministerium des Inneren, für Bau und Heimat, „Cybersicherheitsstrategie für Deutschland 2021“, 2021. *https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1*

[7] S. Herpig, „Stellungnahme im Nationalen Cyber-Sicherheitsrat“, Deutscher Bundestag. Stellungnahme von Dr. Sven Herpig. Drs. 19(12)985., 2021 *https://www.bundestag.de/resource/blob/823368/9f80169c43d2b3106b6db6b6247d51ee/stellungnahme-Dr-Sven-Herpig_15-03-2021-data.pdf*

[8] V. Blue, “Hackonomics: ‚cyber black market‘ more profitable than illegal drug trade,” ZDNet, 26. März 2014. [Online]. Verfügbar unter: *https://www.zdnet.com/article/hackonomics-cyber-black-market-more-profitable-than-illegal-drug-trade/. [Abgerufen am 7.6.2022].*

[9] G. Müller, K. Rannenberg (Hg.), Multilateral Security in Communications, Addison-Wesley-Longman, 1999.

ÜBER DIE GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik.

GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Geschäftsstelle Berlin im
Spreepalais am Dom
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Ansprechpartner:
Nikolas Becker
Teamleiter Politik & Wissenschaft

Mail: nikolas .becker@gi.de
Tel: +49 (0)1767 322 404 3
Web: www.gi.de