August 2018 · Dr. Sven Herpig

Schwachstellen-Management für mehr Sicherheit

Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Von der Polizei über nationale Sicherheitsbehörden bis hin zum Militär: In den letzten Jahren nutzen Behörden immer öfter Schwachstellen in Hardware, Software und Online-Diensten, um etwa bei polizeilichen Ermittlungen Verdächtige digital abzuhören und Beweismittel zu sammeln oder um nachrichtendienstliche Operationen durchzuführen. Schwachstellen sind Fehler in Hardware oder Software, die als Einfallstor für diese Hacking-Operationen genutzt werden können. Die Schwachstellen halten Sicherheitsbehörden geheim, um zu verhindern, dass Hersteller sie schließen. Damit stellt die staatliche Nutzung von Schwachstellen, die Herstellern und der Öffentlichkeit unbekannt sind, eine drängende und schwerwiegende sicherheitspolitische Herausforderung dar. Zwar ist die Ausnutzung dieser "Zero-Day" genannten Schwachstellen manchmal die einzige Möglichkeit für Behörden, auf Informationen in modernen, gut gesicherten IT-Systemen oder Netzwerken zuzugreifen. Allerdings stellen offene Schwachstellen in millionenfach genutzter Soft- oder Hardware gleichzeitig ein Sicherheitsrisiko für die gesamte Wirtschaft, Gesellschaft und Behördenlandschaft dar. Denn Cyber-kriminelle Gruppen, ausländische Nachrichtendienste und Militärs können sich ebenfalls dieser Schwachstellen bedienen und sie gegen die Computer und Smartphones der Bürger:innen, IT-Systeme von Firmen und kritischen Infrastrukturen und deutsche Behörden-Netzwerke einsetzen. Dies passierte bereits im Fall der WannaCry-Schadsoftware, die 2017 weltweit IT-Systeme lahmlegte und Millionenschäden verursachte.

Will die Bundesregierung die Nutzung dieser Schwachstellen weiter erlauben und gleichzeitig die allgemeine Sicherheitsbedrohung dieser Praxis minimieren, bedarf es einem rechtlich verbindlichen Prozess für den staatlichen Umgang mit Zero-Day-Schwachstellen. Ziel dieses Prozesses muss es sein, bei der Nutzung einer Schwachstelle die Interessen der Sicherheitsbehörden und das Sicherheitsrisiko für die Allgemeinheit gegeneinander abzuwägen. Dieser Prozess sollte erstens auf dem Prinzip basieren, dass Zero-Day-Schwachstellen nur temporär zurückgehalten werden. Die Offenlegung der Schwachstellen hat immer Vorrang und muss über bereits international etablierte Verfahren in Abstimmung mit Herstellern bzw. Anbietern erfolgen. Zweitens wird ein transparentes, rechtlich verbindliches Verfahren mit Kontrollmechanismen benötigt, in dem darüber entschieden wird, ob Schwachstellen unmittelbar offengelegt oder temporär zur Nutzung durch die Sicherheitsbehörden zurückgehalten werden sollen. Die Effektivität des Verfahrens muss regelmäßig evaluiert werden. Drittens muss die Forschung zum besseren Verständnis vom staatlichen Umgang mit Schwachstellen,

zum Beispiel ihrer Beschaffung über spezialisierte Marktplätze oder ihrem adäquaten Schutz vor dem Zugriff Dritter, gefördert werden.

Des staatliche Management-Prozess von Zero-Day-Schwachstellen könnte dabei aus vier Elementen bestehen:

1. **Institutioneller Aufbau und Workflow**
   Beim institutionellen Aufbau ist zu berücksichtigen, dass das Verfahren bei einem staatlichen Akteur angesiedelt sein muss, der ressortübergreifend agieren kann. Stimmberechtigt sollten bei dem Verfahren alle in ihrem Aufgabengebiet betroffenen staatlichen Akteure sein. Dies kann neben den Sicherheitsbehörden und dem Bundesministerium des Innern, für Bau und Heimat auch das Bundesministerium für Wirtschaft und Energie, das Auswärtige Amt oder das Bundesministerium für Justiz und Verbraucherschutz sein. Der Workflow muss in geeigneter Art und Weise die übergeordneten Ziele des Grundrechtsschutzes, dem Schutz der Wirtschaft, der öffentliche Sicherheit und IT-Sicherheit berücksichtigen.

2. **Beurteilung der Schwachstellen**
   Um zu prüfen, ob es einen legitimen und gut belegbaren Grund dafür gibt, eine Schwachstelle nicht unmittelbar offenzulegen, muss die Schwachstelle unter Berücksichtigung verschiedener Aspekte beurteilt werden. Hierzu gehören der Verbreitungsgrad der Schwachstelle, der Schaden, der mit dieser Schwachstelle angerichtet werden kann, die Wahrscheinlichkeit der Zurverfügungstellung von Patches, die Wahrscheinlichkeit das bestehende Patches eingespielt werden, die Existenz von Mitigationsmaßnahmen, wirtschaftliche Interessen, Art und Umfang der betroffenen Produkte, die Wahrscheinlichkeit, ob und welche anderen Akteure die Schwachstelle ebenfalls finden könnten, ob eine Ausnutzung dieser Schwachstelle von Dritten durch deutsche Sicherheitsbehörden erkannt werden könnte und welchen operativen Nutzen die Sicherheitsbehörden und Militärs von der Ausnutzung dieser Schwachstelle hätten.

3. **Management der Schwachstellen**
   Dieser Bereich beschäftigt sich damit, wie eine Schwachstelle von den zuständigen Behörden gehandhabt werden muss, wann die Wiederholung ihrer Beurteilung ansteht, welchen Nutzen Mitigationsmaßnahmen haben und wie die Offenlegung stattfinden muss.

4. **Schutz- und Kontrollmaßnahmen**
   Der gesamte Beurteilungs- und Managementprozess sollte von drei Maßnahmen begleitet werden. Zum einen müssen nicht unmittelbar offengelegte Schwachstellen sicher verwahrt werden, damit Dritte sich nicht unautorisierten Zugriff darauf verschaffen können. Gleichzeitig muss sowohl eine Parlamentarische Kontrolle als auch ein Transparenzbericht etabliert werden, damit Rechtmäßigkeit und Effektivität des Prozesses sichergestellt und überprüft werden können.

Danksagung

Diese Analyse wurde von den Mitgliedern des Transatlantic Cyber Forums im Rahmen einer Online Zusammenarbeit und gemeinsamer Workshops in Washington D.C. und Berlin unterstützt. Das Transatlantische Cyber Forum ist ein intersektorales Netzwerk von Cyber-Sicherheitsexpert:innen das zu aktuellen Themen der internationalen Cyber-Sicherheitspolitik arbeitet.

Die vertretenen Meinungen und Positionen sind allein die des Autors und geben nicht notwendigerweise die Meinung der Mitglieder der Arbeitsgruppe oder deren jeweiligen Arbeitgebern wider. Besonderer Dank gilt:

1. Cathleen Berger, Mozilla
2. Ulf Buermeyer, Gesellschaft für Freiheitsrechte e.V. (GFF)
3. Betsy Cooper, Unabhängige Beraterin
4. Alan Duric, Wire
5. Marc Fliehe, Verband der TÜV e.V.
6. Sharon Bradford Franklin, New America's Open Technology Institute
7. Andrew Grotto, Stanford University
8. Trey Herr, Microsoft
9. Karsten-Kai König, CIPHRON
10. Andreas Kuehn, EastWest Institute
11. Susan Landau, Tufts University *(Zugehörigkeit lediglich zur Identifikation)*
12. Daniel Moßbrucker, Reporter ohne Grenzen Deutschland
13. Jan Neutze, Microsoft
14. Riana Pfefferkorn, Stanford Center for Internet and Society
15. Thomas Reinhold, cyber-peace.org / Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
16. Michelle Richardson, Center for Democracy and Technology
17. Volker Roth, Freie Universität Berlin
18. Julia Schuetze, Stiftung Neue Verantwortung
19. Ari Schwartz, Cybersecurity Coalition
20. Megan Stifel, Public Knowledge
21. Eric Wenger, Cisco Systems, Inc.
22. Jessica Zucker, Microsoft
23. Christoph Zurheide, Deutsche Post DHL Group

Inhalt

1. Einleitung

Disclaimer: Es handelt sich bei diesem Papier um eine Übersetzung aus dem englischen Original . Aufgrund der Komplexität des Sachverhalts kann es vereinzelt zu Unstimmigkeiten der beiden Versionen kommen – in diesem Fall gilt das englische Original.

Die Beschaffung, die Beurteilung und das Management von Schwachstellen in Hardware, Software und Online Diensten, die offensive Cyber-Operationen und eine breite Palette von Aufklärungsaktivitäten ermöglichen, ist aktuell eines der wichtigsten Themen der Cyber-Sicherheitspolitik. Schwachstellen bilden der Kern offensiver Aktivitäten im Cyber-Raum wie zum Beispiel Hacking durch Strafverfolgungsbehörden, staatlich sanktionierte „Hack-Back"-Aktivitäten privater Unternehmen, militärische Operationen und nachrichtendienstliche Aufklärung. Andererseits sind schadensbegrenzende Mechanismen und die Schließung von Schwachstellen von entscheidender Bedeutung zum Schutz privater und staatlicher IT-Systeme und Netzwerke. Behörden ziehen daher nicht nur Nutzen aus dem Zurückhalten von Schwachstellen, denn sie nutzen selbst die entsprechenden Systeme, die nicht mehr sicher sind, wenn erkannte Schwachstellen nicht behoben werden – dies gilt analog für kritische Infrastrukturen. Abgesehen von Behörden und den Betreibern kritischer Infrastrukturen hat auch die private Wirtschaft als Ganzes und nicht zuletzt die Öffentlichkeit ein berechtigtes Interesse an der unmittelbaren Schließung von Schwachstellen. Hardware und Software Anbieter sowie Anbieter von Online Diensten im Speziellen haben ein genuines Interesse daran, Schwachstellen schnellstmöglich zu identifizieren und zu patchen, um ein sicheres Produkt anbieten zu können und um wirtschaftlichen und Reputationsschaden abzuwenden. Wirtschaft und Öffentlichkeit erwarten sichere Geräte und Dienste, mit denen sie frei und vertraulich kommunizieren und arbeiten können ohne Gefahr zu laufen, Opfer von Cyber-Spionage und -Kriminalität zu werden[1]. Das Internet Ökosystem profitiert als Ganzes davon, wenn Schwachstellen geschlossen werden. Die Offenlegung von Schwachstellen - und das damit verbundene Schließen dieser - sollte daher das primäre Ziel der Politik sein. Nur in berechtigten Ausnahmefällen sollte diese Offenlegung verzögert und die Schwachstellen damit temporär zurückgehalten werden. Dies kann beispielsweise bei bestimmten Strafverfolgungsaktivitäten oder nachrichtendienstlichen Operationen der Fall sein. Der Ausbalancierung und dem Management der entstehenden Zielkonflikte und der notwendigen Werteabwägung kommt daher eine herausragende Bedeutung zu. Dabei sind Grundrechte, Interessen des Handels, die öffentliche Sicherheit und die Sicherheit der informations-

1 Kate Musgrave, In Repressive Countries Citizens Go ‚Dark' to Share Independant News

technischen Systeme in die Interessenabwägung einzubeziehen. Eine gute Beschreibung des zu Grunde liegenden Auftrages hat die US-Regierung in ihrem Vulnerability Equities Policy and Process (VEP) geliefert: "The primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG [amerikanische Regierung], absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes"[2].

Im November 2017 veröffentlichte die US-Regierung ihre VEP Charta, in der sie die organisatorische Struktur, die Verfahren und jeweiligen Indikatoren und Interessen der verschiedenen Akteure, die zur Beurteilung von Schwachstellen herangezogen werden, darlegt. Details des Verfahrens sind zwar nach wie vor geheim, dennoch setzt die VEP Veröffentlichung einen neuen Standard in Bezug auf die Transparenz von Regierungshandeln rund um die Beurteilung, das Zurückhalten und die Offenlegung von Schwachstellen. Auch wenn zu großen Teilen hinter verschlossenen Türen[3] geführt, hat die langjährige Debatte um den VEP zusammen mit einer Diskussion über andere internationale Regelungsansätze[4], eine Fülle an Material für dieses Papier geliefert und sie ist für Regierungen in aller Welt von erheblicher Bedeutung.

Hauptanliegen der Arbeitsgruppe „Verschlüsselungspolitik und staatliches Hacking" des Transatlantic Cyber Forum (TCF) ist die rasche Verabschiedung öffentlich zugänglicher Verfahren zu Umgang, Zurückhaltung und Offenlegung von Schwachstellen im Rahmen der aktuell in Deutschland und der EU[5] geführten Diskussion. Gleichzeitig will die Arbeitsgruppe weitere Verbesserungen des in den USA existierenden Verfahrens identifizieren und voranbringen. Das vorliegende Papier beleuchtet Prinzipien und Kriterien für die Umsetzung entsprechender Policies in verschiedenen Ländern. Ein wichtiger Punkt ist die Notwendigkeit, staatlicherseits Verfahren zu entwickeln, die eine Offenlegung favorisieren und ein Zurückhalten nur unter bestimmten Bedingungen erlaubt sowie klar zeitlich beschränkt. Im Zentrum der jeweiligen Policies sollte das „wann" und „wie" der Offenlegung stehen, und nicht das „ob" und „wenn".

2 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

3 Konsolidiertes Material, z. B. Unterlagen, die die Electronic Frontier Foundation mittels einer Informationsfreiheitsanfrage zugänglich machen konnte

4 Aspen Institute, Cyber Breakfast:The View from the White House with Rob Joyce

5 Mirja Gutheil et al., Legal Frameworks for Hacking by Law Enforcemen,Identification, Evaluation and Comparison of Practices

2. Schwachstellen

Ein grundlegendes Verständnis des Begriffs muss der Beurteilung und dem Umgang mit „Schwachstellen“ vorangehen. Der ISO/IEC Standard 30111:2013 definiert Schwachstellen als „weaknesses of software, hardware, or online service that can be exploited [...]. Regardless of cause, an exploitation of such vulnerability may result in real threats of mission-critical information systems”[6]. Ähnlich formuliert es die United States National Telecommunications and Information Administration (NTIA): „vulnerabilities are weaknesses of software, hardware, or online services that can be used to damage the confidentiality, integrity, or availability of those systems or the data they store. Finding these vulnerabilities and informing affected parties is essential to protect our economy and citizens“[7]. Das National Security Council (NSC) des Weißen Hauses definierte Schwachstellen in einem Dokument aus dem Jahr 2017 als „a weakness in an information system or its components (e.g. system security procedures, hardware design, internal controls) that could be exploited or impact confidentiality, integrity, or availability of information“[8].

Im vorliegenden Papier wird der Begriff Schwachstelle daher wie folgt definiert: „Fehler in Hard- oder Software, die jeweils einzeln oder in Verkettung mit anderen Schwachstellen Dritten die Ausnutzung eines Systems ermöglichen, um unautorisiert, und vom Systeminhaber unter Umständen unbemerkt, ein oder mehrere Geräte oder Online Dienste zu manipulieren“. Eine weitere Differenzierung nach einer Reihe von Gesichtspunkten ist möglich, etwa danach, welche Software oder Hardware die Schwachstelle betrifft, nach dem möglichen Schadenausmaß[9] oder charakteristischen Eigenschaften[10]. Das grundlegendste Unterscheidungskriterium ist, ob es sich um Zero-Day-Schwachstellen (unbekannte Schwachstellen) oder N-Day-Schwachstellen (bekannte Schwachstellen) handelt.

6 ISO, ISO/IEC 30111:2013(en) Information technology — Security techniques — Vulnerability handling processes

7 National Telecommunications and Information Administration, Vulnerability Disclosure Attitudes and Actions

8 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

9 CVE Details

10 Kann beispielsweise die Schwachstelle per Internet Zugriff, also aus beliebiger Entfernung, ausgenutzt werden oder nur vor Ort, wenn der Angreifer in Besitz des Gerätes ist. Schweregrad und Charakteristika sind wichtige Aspekte für die Beurteilung einer Schwachstelle und werden daher in den entsprechenden Kapiteln dieses Papiers diskutiert.

Unbekannte Schwachstellen

Zero-Days sind Schwachstellen, die weder dem jeweiligen Betreiber oder Hersteller - hier als „Maintainer“[11] bezeichnet -, noch der Öffentlichkeit[12] bekannt sind. Damit steht kein „Patch“ – keine Abhilfe zur Behebung der Schwachstelle – und kein schadensbegrenzender Mechanismus, eine “Mitigation”[13], durch den jeweiligen *Maintainer* zur Verfügung. Dadurch ist die Schwachstelle äußerst potent für Angreifer und extrem gefährlich für entsprechend verwundbare Systeme. Mehrere Akteure (zum Beispiel Nachrichtendienste) können unabhängig voneinander Wissen von ein- und derselben Schwachstelle erhalten haben, ohne zu wissen, dass auch die andere Seite die Schwachstelle kennt. Gegnerische Nachrichtendienste oder Kriminelle können so parallel offene Zero-Day-Schwachstellen ausnutzen. Unabhängig davon, ob eine solche Schwachstelle ausgenutzt wird oder nicht, bleibt sie eine Zero-Day-Schwachstelle bis zu dem Zeitpunkt, an dem der betroffene *Maintainer* informiert ist.

Bekannte Schwachstellen

N-Days sind Schwachstellen, die dem *Maintainer* bekannt sind. Das bedeutet nicht, dass er bereits einen Patch zum Schließen der Schwachstelle entwickelt hat oder dass er grundsätzlich plant, sie zu schließen. Typischerweise tritt das letztgenannte Szenario auf, wenn ein Produkt bereits das Ende

11 Der Begriff „Maintainer“ stammt aus dem Bereich der Open Source Entwicklung und umfasst hier denjenigen Akteur, der einen Patch zur Schließung der Schwachstelle bereitstellen kann. Das kann sowohl der Hersteller oder Anbieter einer Hard- oder Software sein, der Anbieter eines Online Dienstes oder Personen oder die Community, die Open Source Software entwickelt und betreut. Siehe: David “cdlu” Graham, OLS: Kernel documentation, and submitting kernel patches

12 Besondere Werkzeuge der statischen Codeanalyse können genutzt werden, um zu bestimmen, ob eine unbekannte Schwachstelle vorliegt.
White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

13 Eine „schadensbegrenzende Maßnahme“ (Mitigation) bezeichnet laut radware, Attack Mitigation „[...] detection and protection strategy used to safeguard networks, servers and applications by IT administrators in order to minimize the effect of malicious traffic and intrusion attempts while maintaining functionality for users“; Diese Maßnahmen sind unabhängig davon, ob es einen Patch des *Maintainers* gibt, in dessen Soft- oder Hardware beziehungsweise Online Dienst die Schwachstelle steckt. Nicht immer gibt es solche Mitigationen, die die Effekte einer Schwachstelle abschwächen können. Ein Beispiel für eine Methode zur Schadensbegrenzung ist: gibt es eine Sicherheitslücke im Macro eines Textverarbeitungsprogramms (z. B. Microsoft Word oder Libre Office Writer), kann ein Administrator einer Windows Umgebung die entsprechenden Macros blockieren, indem er die entsprechende Policy für die Nutzergruppe anpasst. Damit wäre die Nutzung des infizierten Macros für keinen Nutzer im betroffenen Netzwerk mehr möglich, potenzielle Angriffe unter Ausnutzung dieser Schwachstelle wären jedoch ausgeschlossen. Damit ist kurzfristig für Abhilfe gesorgt, bis der eigentliche Patch für die Software zur Verfügung steht oder die Sicherheitssoftware entsprechend angepasst ist.

seines Lebenzyklus (EOL) erreicht hat, nicht mehr hergestellt wird, wenn es keinen hauptverantwortlichen *Maintainer* gibt, dieser nicht die Fähigkeit hat, einen Patch zu entwickeln, gar nicht mehr existiert[14], oder schlicht kein Interesse hat, die Schwachstelle zu schließen. All diese Konstellationen können dazu führen, dass es niemals einen entsprechenden Patch für das verwundbare Produkt gibt[15]. Selbst wenn ein Patch verfügbar ist, muss dieser getestet, an die betroffenen Geräte verteilt und außerhalb zentral betriebener IT-Umgebungen von den eigentlichen Endnutzer:innen selbst installiert werden. Die Zeit zwischen dem Bekanntwerden einer Schwachstelle und dessen Schließung mittels eines Patches, wird als "Window of Exposure"[16] bezeichnet.

Auswirkungen

Das Schließen einer Schwachstelle per Patch führt häufig zu nicht völlig konsistenten Ergebnissen, insbesondere wenn komplexe Systeme oder ältere Software betroffen sind. Besonders kompliziert wird es, wenn die zugrundeliegende Software von unterschiedlichen Anbietern kommt; ein Sicherheitsbericht von Google im Jahr 2016 stellte beispielsweise fest, dass nur die Hälfte der Top-50 Android Mobiltelefon-Modelle die aktuellsten Sicherheitsupdates eingespielt hatten[17]. Zieht man die vielen EOL-Modelle in die Betrachtung mit ein, ergibt sich eine beängstigend hohe Zahl nicht abgesicherter Geräte, die schon über bekannte Schwachstellen angreifbar sind. Noch problematischer ist die Situation in den Bereichen Internet der Dinge (IoT[18]), industrielle Steuerungssysteme (ICS[19]), Embedded-Systeme oder System-on-a-Chip-Architekturen[20]. Solche Systeme verfügen teilweise nicht einmal über Möglichkeiten und Kanäle, um Updates vorzunehmen und Patches einzuspielen.

14 Dan Geer empfahl bei der BlackHat Konferenz 2014 „[...] if Company X abandons a code base, then that code base must be open sourced". Damit könnten andere Akteure als *Maintainer* fungieren. Dan Geer, Cybersecurity as Realpolitik

15 Diese Situation tritt hauptsächlich bei proprietären Lösungen auf. Open Source Produkte kann theoretisch auch ein anderer, nicht nur der eigentliche *Maintainer*, patchen, weil der Quellcode öffentlich einsehbar ist.

16 Bruce Schneier, Full Disclosure and the Window of Exposure
Trend Micro, Maintaining Vulnerable Servers - What's Your Window of Exposure?

17 Android Security 2016 Year In Review

18 Mario Ballano Barcena and Candid Wueest, Symantec Security Response - Insecurity in the Internet of Things
hp, HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack

19 European Union Agency for Network and Information Security, Window of exposure... a real problem for SCADA systems?

20 Graz University of Technology, Meltdown and Spectre

Für staatliche Behörden, die sich selbst als Hacker betätigen wollen, sind das gute Nachrichten. Sie müssen nicht unbedingt Zero-Day-Schwachstellen beschaffen – was weitaus aufwändiger und teurer ist. Stattdessen können sie die zahlreichen nicht abgesicherten N-Day-Schwachstellen[21] ausnutzen. Würden sich Regierungen auf diese Angriffsmöglichkeit beschränken, wäre das durchaus auch von Vorteil für die Cyber-Sicherheit per se. Eine Studie kam jüngst zum Ergebnis, dass die überwiegende Zahl der Hacking-Angriffe im Jahr 2015 N-Day Schwachstellen ausnutzte, für die bereits ein Patch zur Verfügung stand[22]. Wenn Sicherheitsbehörden sich dieser Schwachstellen erfolgreich bedienen können, um ihre Ziele anzugreifen, steht der unmittelbaren Offenlegung von Zero-Day-Schwachstellen wenig entgegen, weil das Zurückhalten dieser Schwachstellen dann keinen zusätzlichen operativen Mehrwert bringt. Allerdings fehlt die empirische Grundlage zu der spezifischen Frage, wie häufig Regierungen, etwa Russland, Großbritannien, China, Israel, die USA, Deutschland oder andere, sich bei ihren Cyber-Operationen auf Zero-Day-Schwachstellen gestützt haben und wie häufig andere Mittel ebenso erfolgversprechend gewesen wären. Ohne entsprechende Daten sollten wir davon ausgehen, dass die Offenlegung von Zero-Day-Schwachstellen einen Nettogewinn an Sicherheit bedeutet. Dass die Möglichkeiten der Sicherheitsbehörden beim Angriff auf Zielsysteme sich durch Zurückhalten und Ausnutzung solcher Zero-Day-Schwachstellen verbessern, steht dem vorerst ohne Nachweis gegenüber.

Auf der Basis von Daten der MITRE Corporation gab es 2017 40 neue Schwachstellen pro Tag[23]. Forscher:innen fanden allerdings heraus, dass es für 77 Prozent der Schwachstellen keine bekannten *Exploits* (also Angriffskonzepte unter Ausnutzung der entsprechenden Schwachstelle) gab. Nur bei zwei Prozent aller veröffentlichten Schwachstellen entdeckten die Forscher:innen den Einsatz der jeweiligen *Exploits* in der Praxis[24]. Es ist daher sinnvoll, die Ausnutzung von Zero-Day-Schwachstellen in einen größeren Zusammenhang zu stellen. David Hogue, Senior Technical Director beim Cyber Security Threat Operations Center der NSA sagte im April 2018: „at NSA we have not responded to an intrusion response that's used a zero day vulnerability in over 24 months [...] The majority of incidents we see are a

21 CVE Details

22 Verizon, 2016 Data Breach Investigations Report

23 Fahmida Y. Rashid, Predict Which Security Flaws Will be Exploited, Patch Those Bugs

24 Fahmida Y. Rashid, Predict Which Security Flaws Will be Exploited, Patch Those Bugs

result of hardware and software updates that are not applying“[25]. Andreas Könen, Abteilungsleiter für Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat sagte im Juni 2018, dass lediglich bei fünf Prozent aller Schwachstellen, die für *Exploits* genutzt werden, Zero-Day-Schwachstellen zum Einsatz kommen. Der Rest sind laut Könen bereits bekannte Schwachstellen[26].

3. Verfahren

3.1 Prinzipien

Das im vorliegenden Papier vorgestellte Verfahren zu Beurteilung und Management von Schwachstellen basiert auf den folgenden Prinzipien und Handlungsempfehlungen:

1. Eine Regierung, die für begrenzte Zeit Schwachstellen in Hardware, Software, oder bei Online Diensten zurückhalten und zum Zwecke der Strafverfolgung, der nachrichtendienstlichen Aufklärung oder militärischer Operationen ausnutzen will, muss ein offenes und transparentes Verfahren zu Beurteilung und Management von Schwachstellen etablieren, im Idealfall in Übereinstimmung mit den in diesem Papier empfohlenen Maßnahmen.

2. Das Verfahren muss gesetzlich geregelt und einer unabhängigen rechtlichen Evaluierung bezüglich Angemessenheit und Wirksamkeit unterworfen, beziehungsweise mit einer *Sunset*-Klausel von fünf (5) Jahren versehen werden.

3. Das hier vorgestellte Beurteilungs- und Managementverfahren findet bei allen Zero-Day-Schwachstellen[27] Anwendung, die von einer staatlichen Stelle beschafft werden; dies beinhaltet auch staatlich beschaffte Hacking-Werkzeuge und -Dienstleistungen die Zero-Day-Schwachstellen ausnutzen.

---

25 Chris Bing, Nation-state hackers attempted to use Equifax vulnerability against DoD, NSA official says

26 Podiumsdiskussion bei der Konferenz „Cyber-Sicherheitspolitik in Deutschland“ am 06.06.2018 in Berlin. Die Konferenz wurde gemeinsam von der Bundesakademie für Sicherheitspolitik und der Stiftung Neue Verantwortung organisiert.

27 Schwachstellen, die für rein defensive Zwecke beschafft werden (also zur Absicherung der informationstechnischen Systeme) werden nicht von diesem Verfahren erfasst, müssen aber allein für den vorgesehenen Zweck genutzt werden.

4. Schwachstellen werden niemals dauerhaft zurückgehalten gehalten. Ihre Offenlegung kann lediglich verzögert werden. Sie werden also gegebenenfalls zeitweise zurückgehalten und müssen letztlich immer in enger Abstimmung mit dem *Maintainer* offengelegt werden.

5. Grundprämisse des Verfahrens muss sein, dass die Offenlegung von Schwachstellen im Interesse der Grundrechte, der Wirtschaft, der öffentlichen Sicherheit und der IT-Sicherheit ist.

6. Eine Regierung, die Schwachstellen temporär zurückhalten will, muss die Notwendigkeit nachweisen und darlegen, dass der durch eine unmittelbare Offenlegung zu erwartende Sicherheitsgewinn aufgewogen wird. Sie muss darlegen, wie sie mögliche Schäden minimieren will, und demonstrieren, wie Schwachstellen sicher verwahrt und während dieses Zeitraums gegen unberechtigte Zugriffe durch Dritte geschützt werden sollen. Die Schutzmaßnahmen sollten auch darauf zielen, die Offenlegung für den Fall zu beschleunigen, dass Dritte Kenntnis von der Schwachstelle erlangen.

7. Regierungen, die solche Verfahren für den Umgang mit Schwachstellen eingeführt haben, sollten in den zuständigen internationalen Gremien und Kooperationen für eine entsprechende internationale Norm[28] werben.

8. Regierungen sollten die Erforschung zu Kollisionsraten[29] finanziell fördern, um das Zurückhalten von Schwachstellen auf der Basis des operativen Nutzens rechtfertigen zu können, ohne dabei Grundrechte, Handel, öffentliche Sicherheit und IT Sicherheit[30] zu gefährden.

9. Ein besseres Verständnis von Beschaffung (zum Beispiel Transparen-

28 Kate Charlet, Sasha Romanosky and Bert Thompson, It's Time for the International Community to Get Serious about Vulnerability Equities
Shaun Waterman, Responsible vulnerability disclosure is becoming an international norm
Centre for European Policy Studies (CEPS), Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges https://www.cyberscoop.com/vep-international-responsible-disclosure-canada-uk-netherlands/

29 Kollisionsraten bieten ein empirisches mathematisches Modell, mit dem kalkuliert werden kann, wie lange es dauert, bis zwei oder mehr Akteure dieselbe Schwachstelle unabhängig voneinander entdecken.

30 Ein volkswirtschaftlicher Überblick zur Frage, zu welchem Zeitpunkt eine Schwachstelle bevorzugt veröffentlicht werden soll, liefert Tristan Caulfield, Christos Ioannidis and David Pym, The U. S. Vulnerabilities Equities Process : An Economic Perspective

zanforderungen für den Schwachstellenhandel) und Offenlegung (zum Beispiel Umsetzung bestehender Richtlinien zur koordinierten Offenlegung von Schwachstellen [*Coordinated Vulnerability Disclosure*]) von Schwachstellen muss entwickelt werden.

3.2 Ziel und Abgrenzung

Regierungen stehen vor schwierigen Abwägungsprozessen: sollen sie Schwachstellen offenlegen oder zurückhalten. Beide Entscheidungen sind möglicherweise riskant. Daher brauchen staatliche Stellen klare Richtlinien, Verfahren und Verantwortlichkeiten, und möglicherweise negative Anreize, um deren Durchsetzung zu forcieren. Im vorliegenden Papier wird ein Verfahren vorgestellt, das die entsprechenden Entscheidungsprozesse für Regierungen erleichtern soll. Das Verfahren sieht vier Schritte und drei übergeordnete Schutzmaßnahmen im Prozess vor. Die Schritte sind nicht zwingend linear, insbesondere, wenn die Schwachstellen in den „Beurteilung-Management-Offenlegung" Kreislauf eingetreten sind.

Schritt eins ist die Beschaffung der Schwachstelle. Dabei hat eine Regierung Zugriff auf eine Schwachstelle erlangt, die zu Zwecken der Strafverfolgung, der nachrichtendienstlichen Aufklärung oder für militärische Operationen ausgenutzt werden soll. Schritt zwei ist das institutionelle Konzept des Verfahrens, gefolgt von der Beurteilung der Schwachstellen. Diese steht im Zentrum des Prozesses. An vierter Stelle kommt das Management der erworbenen Schwachstellen: entweder werden sie offengelegt, zurückgehalten oder zurückgehalten und mitigiert. Die technischen und rechtlichen Schutz- und Kontrollmaßnahmen: Schutz der Schwachstellen vor dem Zugriff Dritter, Transparenz und (parlamentarische) Kontrolle flankieren das gesamte Verfahren.

Bei der Beschaffung geht das vorgestellte Modell nur kurz, aber nicht im Detail darauf ein, wie die staatliche Stelle in den Besitz der Schwachstelle gelangt. Dies kann zum Beispiel im Rahmen der internationalen Zusammenarbeit zwischen Geheimdiensten, durch eigene Forschung oder über den entsprechenden Markt geschehen, auf dem Schwachstellen gehandelt werden. Vorarbeiten in diesem Bereich liegen vor[31]; Mehr Aufmerksamkeit für

31 Luca Allodi, Economic Factors of Vulnerability Trade and Exploitation
Nicole Perlroth and David E. Sanger, Nations Buying as Hackers Sell Flaws in Computer Code
Lillian Ablon and Andy Bogart, Zero Days and Thousands of Nights
Joseph Cox and Lorenzo Franceschi-Bicchierai, How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of

technische, ethische, politische, wirtschaftliche und gesetzgeberische Gesichtspunkte sind allerdings dringend erforderlich. Die Beschaffungsfrage ist allerdings ein eigenes Thema, das zusätzlich zum Umgang mit Schwachstellen ausführlich betrachtet werden sollte.

Ausgeschlossen von der Betrachtung in diesem Papier sind überdies Details der *Coordinated Vulnerability Disclosure* (CVD). CVD „is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public“[32]. Regierungen sollten also Schwachstellen an den *Maintainer* melden und mit diesen das weitere Vorgehen in Übereinstimmung mit den in der CVD festgelegten Vorgaben koordinieren. Regierungen müssen daher ein entsprechendes CVD-Verfahren implementiert haben, damit sie Informationen über Schwachstellen in ihren eigenen IT-Systemen erhalten können. Zugleich sollen Regierungen natürlich selbst Schwachstellen an *Maintainer* melden, also auch die Rolle des “Finders” von Schwachstellen im CVD-Verfahren[33] übernehmen können.

32 Allen D. Householder, Garret Wassermann, Art Manion and Chris King, The CERT® Guide to Coordinated Vulnerability Disclosure
Mehr Informationen zu CVD:
FIRST, Multi-Party Coordination and Disclosure
NTIA, Vulnerability Disclosure Attitudes and Actions
Bundesamt für Sicherheit in der Informationstechnik, Handhabung von Schwachstellen
ISO, ISO/IEC Standard 29147:2014
ISO, ISO/IEC Standard 30111:2013

33 CEPS Task Force, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

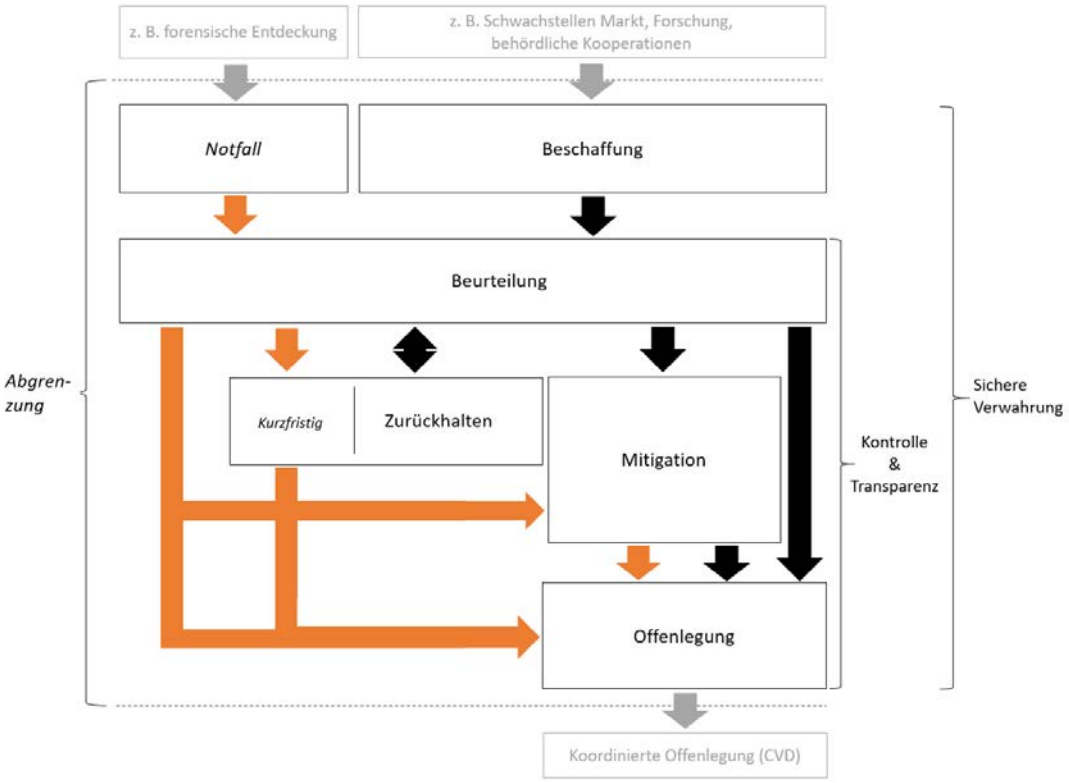

Abbildung 1: Visualisierung des Verfahrens

3.3 Beschaffung

3.3.1 Quellen und Umgang mit Schwachstellen

Regierungen können durch eigene Forschung, forensische Untersuchungen, über befreundete Nachrichtendienste oder über spezialisierte Firmen an Schwachstellen gelangen. Die Art und Weise der Beschaffung kann einen Einfluss auf die Art der Evaluierung einer Schwachstelle haben und sollte in dieser Phase auf jeden Fall berücksichtigt werden. Wurde eine Schwachstelle durch eigene Forschung entdeckt, kann es sein, dass kein anderer Akteur von der Schwachstelle Kenntnis hat. Damit verringert sich (temporär) das Risiko, dass die entsprechende Schwachstelle durch Dritte gegen IT-Systeme im eigenen Staat angewendet wird. Wurde die Schwachstelle aber über forensische Analysen, im Rahmen des Austauschs mit einem internationalen Partner oder von privaten Anbietern erworben, haben andere Akteure naturgemäß Kenntnis von der Schwachstelle, und können sie im Zweifel selbst für Angriffe ausnutzen, beziehungsweise tun dies bereits. In diesen Fällen ist die Gefährdung, zum Beispiel der öffentlichen Sicherheit, deutlich höher als im vorherigen Beispiel. Dies gilt analog zur Kenntnis einer Schwachstelle,

auch für das Kaufen oder Mieten von Hacking-Werkzeugen und -Dienstleistungen welche Zero-Day-Schwachstellen ausnutzen.

Jede einzelne Zero-Day-Schwachstelle, in deren Besitz eine staatliche Stelle gelangt, muss dieses hier skizzierte Verfahren zur Offenlegung durchlaufen. Davon ausgenommen sind Schwachstellen, welche staatlichen Stellen für den singulären Zweck übermittelt werden, damit diese sie in das CVD-Verfahren einspeisen. Diese Schwachstellen dürfen nicht zurückgehalten werden und müssen unmittelbar über den CVD-Prozess an den *Maintainer* gemeldet werden. Diese Vorgehensweise ist zwingend erforderlich, damit das CVD-Verfahren nicht unterlaufen wird und staatliche Akteure ihrer vertrauenswürdigen Rolle als Koordinator im CVD gerecht werden können. Nur so wird gewährleistet, dass bei Problemen mit der direkten Kommunikation zwischen Findern von Schwachstellen und betroffenen *Maintainern* diese die entsprechenden Informationen erhalten.

In Notfällen ist das reguläre Zurückhalten bzw. Zurückhalten und Mitigation (Langzeit-Mitigation mit verzögerter Offenlegung) keine Option. In diesen Fällen müssen Schwachstellen entweder unmittelbar mitigiert und offengelegt werden, oder allenfalls für kurze Zeit zurückgehalten (kurzfristige s Zurückhalten) und dann mitigiert und offengelegt werden. Ein Notfall liegt zum Beispiel dann vor, wenn eine forensische Untersuchung staatlicher IT-Systeme oder kritischer Infrastrukturen eine Zero-Day-Schwachstelle zu Tage fördert, die aktiv durch Dritte ausgenutzt wird. Ein Grund für das kurzfristige Zurückhalten der Schwachstelle wäre hierbei, dass sich entgegenstehende Interessen berücksichtigt werden müssen. Eine unmittelbare Offenlegung der Schwachstelle könnte beispielsweise laufende forensische Ermittlungen zur Identifikation der Angreifer behindern (Attribution).

3.3.2 Vereinbarungen mit Dritten

Eine Kritik an dem Schwachstellenmanagement-Prozess der US-Regierung ist, dass er keine Regelung enthält, die Geheimhaltungsvereinbarungen (*Non-Disclosure Agreements*, NDAs)[34] als Vorbedingungen Dritter ausschließen. Wenn eine Regierung von einem Dritten (einer anderen Regierung, einem privaten Unternehmen, einem:r unabhängigen Sicherheitsforscher:in) eine Schwachstelle beschafft, kann es vorkommen, dass sie verpflichtet wird, ein NDA zu unterschreiben, das sie daran hindert, diese Schwachstelle dem normalen Beurteilungs- und Offenlegungsverfahren zuzuführen. NDAs können so dazu genutzt werden, diesen Prozess weitgehend auszu-

34 Robert Knake, Grading the New Vulnerabilities Equities Policy: Pass

hebeln, abgesehen von Schwachstellen, die aus der eigenen Forschung und forensischen Arbeit des jeweiligen Staates kommen. Die Beschaffung von Schwachstellen darf aus diesem Grund keinen NDAs unterworfen sein[35]. Das schließt die Beschaffung von Hacking-Werkzeugen und -Dienstleistungen die Zero-Day-Schwachstellen ausnutzen mit ein. Dies könnte dazu führen, dass Regierungen die keine NDAs unterzeichnen, durch eine solche harte Linie benachteiligt sind. Firmen verkaufen ihre Hacking-Werkzeuge und -Dienstleistungen präferiert an Akteure, die NDAs unterzeichnen, da dies ansonsten zur Offenlegung der Schwachstelle führen kann und dadurch wirtschaftlicher Schaden für die Firma entsteht. Besteht ein Nachfragemonopol, können Regierungen, die NDAs im Prinzip ablehnen, jedoch immer noch Schwachstellen bei Dritten einkaufen - möglicherweise zu einem höheren Preis. Um den Druck auf die Verkäufer zu erhöhen, auf NDAs als Vorbedingung zu verzichten, könnten gleich gesinnte Regierungen davon überzeugt werden, NDAs ebenfalls abzulehnen.

3.4 Struktur

3.4.1 Interessenvertretung

Bei der Schaffung der institutionellen Strukturen für ein staatliches Verfahren zur Beurteilung und zum Management von Schwachstellen, müssen die Rollen und Verantwortlichkeiten für die beteiligten Institutionen denen entsprechen, die ihnen auch im jeweiligen politischen System zukommen. Das institutionelle Design ist eine der schwierigsten Aufgaben bei der Gestaltung eines solchen Verfahrens. Um die Kommunikation zu erleichtern und Ressort-übergreifende Aktivitäten zu organisieren, sollte es eine zentrale Plattform, ein Sekretariat, ähnlich dem „VEP Executive Secretariat“ in den USA[36],

35 Eine Alternative wäre statt eines grundsätzlichen Verbotes, NDAs als absolute Ausnahme und letztes Mittel zuzulassen. Klare Dokumentationspflichten wären dabei notwendig, in denen dargelegt wird, warum man zu diesem letzten Mittel gegriffen und den NDA unterzeichnet hat. Die mit dem Schwachstellen-Management betraute Behörde müsste die entsprechenden Dokumente jährlich prüfen und entscheiden, ob die geltende Regelung noch tragbar ist oder ob weitere Verschärfungen oder ein Verbot der NDAs angezeigt sind.

36 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

geben. Jede beteiligte Behörde, die bestimmte Interessen vertritt[37], sollte gegenüber dem Sekretariat eine Kontaktperson (POC) benennen - analog zur Struktur in der VEP Charta[38]. Komplizierter ist die Verortung des Sekretariats. Die VEP Charta hat diese Aufgabe der National Security Agency (NSA) übertragen. Deren Rolle als militärischer Auslandsgeheimdienst, der eigene Cyber-Operationen durchführt, macht die NSA zu einer weniger geeigneten Kandidatin für diese Aufgabe, da sie aufgrund ihrer Rolle das Zurückhalten von Schwachstellen favorisieren dürfte[39]. Mögliche andere Kandidat:innen sind mit der Cyber- und Informationssicherheit betraute Behörden. In Deutschland kommt etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Frage. Wie im Fall der NSA könnte auch diese Behörde bestimmte Entscheidungen favorisieren, im Fall des BSI in Richtung Offenlegung der Schwachstellen. Zusätzlich ist Vertrauen ein kritischer Aspekt der Cyber-Sicherheit. Macht man eine Cyber-/IT-Sicherheitsbehörde für das Management von Schwachstellen verantwortlich, von denen dann einige nicht unmittelbar offengelegt werden, leidet zwangsläufig deren Reputation bei internationalen Partnern (zum Beispiel CERTs), aber auch bei privaten, zivilgesellschaftlichen Akteuren und anderen Behörden im jeweiligen Land. Andere Akteure verlassen sich auf die Sicherheitsrichtlinien und -Standards, die diese Behörde herausgibt. Das Vertrauen in genau diese Richtlinien wird aber unterminiert, die Bereitschaft zur Umsetzung von Empfehlungen nimmt ab, und letztlich könnte die Cyber-Sicherheit eines Landes massiv leiden, wenn das Sekretariat bei einer Behörde wie dem BSI angesiedelt wird[40]. Ein anderer Nachteil einer solchen Konstruktion sind Schwierigkeiten bei Ressort-übergreifenden Absprachen, vor allem bei der Abwägung der verschiedenen Interessen. Gerade wegen der Ressort-übergreifenden Natur des Verfahrens und dessen Bedeutsamkeit sowie der Abwägung der verschiedenen

37 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF
Beteiligte Behörden als Vertreter verschiedener Interessen können etwa sein die Ressorts für Wirtschaft, Justiz, Außenpolitik sowie Strafverfolgungsbehörden, Geheimdienste, Streitkräfte, Verbraucherschutz-, Cybersicherheit- und weitere spezialisierte Behörden (wie die Federal Communication Commission in den USA oder das Bundesinstitut für Arzneimittel und Medizinprodukte).

38 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

39 Ari Schwartz and Rob Knake, Government's Role in Vulnerability Disclosure - Creating a Permanent and Accountable Vulnerability Equities Process

40 Ein ähnliche Diskussion entstand durch die widersprüchliche Rolle, die das US National Institute of Standards and Technology (NIST) bei der Standardisierung von Verschlüsselungsalgorithmen spielte, die die NSA knacken konnte, siehe Nicole Perlroth, Government Announces Steps to Restore Confidence on Encryption Standards

Werte und Interessen rät das vorliegende Papier dazu, das Sekretariat bei einer hochrangigen Regierungsstelle anzusiedeln, die an der Schnittstelle zwischen Digitalisierungspolitik einerseits und öffentliche Sicherheit andererseits sitzt. Beispielhaft genannt seien hier der Cyber-Sicherheitskoordinator des Weißen Hauses in den Vereinigten Staaten oder, für Deutschland, der Chef des Bundeskanzleramtes.

3.4.2 Struktur des Sekretariats

Für die Beurteilung und das Management von Schwachstellen entsenden die beteiligten Behörden ihre jeweiligen POCs zu regelmäßigen Treffen. Zusätzlich zu den POCs und einem kleinen Management-Team, sollten im Bedarfsfall auch externe Expert:innen, einschließlich technischer Fachleute, hinzugezogen werden (möglicherweise aus einem Pool von Personen, die vorab die etwaige Sicherheitsüberprüfung durchlaufen haben). Dadurch lässt sich die in den Beratungen notwendige Fachkompetenz beiziehen[41], die Vor- und Nachteile von Offenlegung und Zurückhalten der Schwachstellen aufzeigen[42] und auch die Akzeptanz und das Vertrauen der Öffentlichkeit in das Verfahren stärken. Das Sekretariat übernimmt auch die notwendigen Dokumentations- und Berichterstattungspflichten und sorgt für Transparenz; es organisiert und unterstützt öffentliche und private Forschung zum Thema Schwachstellenanalyse; es macht regelmäßig Bestandsaufnahmen zu der in Regierungsnetzen und kritischer Infrastruktur eingesetzten Hard- und Software und von der öffentlichen Hand genutzten Online Diensten und anderen sensiblen Bereichen. Diese Informationen können in das Verfahren einfließen und die Beurteilung von Schwachstellen verbessern.

3.4.3 Workflow

Eine Behörde, die eine Schwachstelle beschafft, versorgt unmittelbar nach dem Erwerb das Sekretariat mit Detailinformationen über die Sicherheitslücke, anhand der Kriterien, die unten aufgelistet sind. Das gesamte Sekretariat, samt der POCs und ggf. technischer Expert:innen, trifft sich einmal im

41 Abgesehen von der technischen Expertise sind Einschätzungen zur Wahrscheinlichkeit von Patches und auch deren Akzeptanz und Einspielung hilfreich.

42 Vergleichbar den Amicus Gutachten bei den FISA Verfahren in den USA, siehe U.S. Congress, UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015

Monat[43], bei Bedarf auch kurzfristig, und entscheidet über die Offenlegung der neu vorgelegten, so wie bereits zurückgehaltenen und zur Re-Evaluierung anstehenden Schwachstellen. Das Ergebnis kann jeweils lauten: Offenlegung, Zurückhalten zur etwaigen Ausnutzung oder Zurückhalten und Mitigation (wenn es mitigierende Maßnahmen zu dieser Schwachstelle gibt). Nur POCs haben Stimmrecht. Um einer Tendenz zugunsten des Zurückhaltens der Schwachstellen entgegenzuwirken, und nicht in eine reine Zahlenarithmetik zu verfallen (etwa durch die größere Präsenz von Sicherheits- und Nachrichtendiensten gegenüber anderen Behörden), ist ein Ansprechpartner, der die Offenlegung von Schwachstellen favorisiert (voraussichtlich aus den Ressorts Außen- oder Wirtschaftspolitik oder aus der für Cyber- und IT-Sicher-

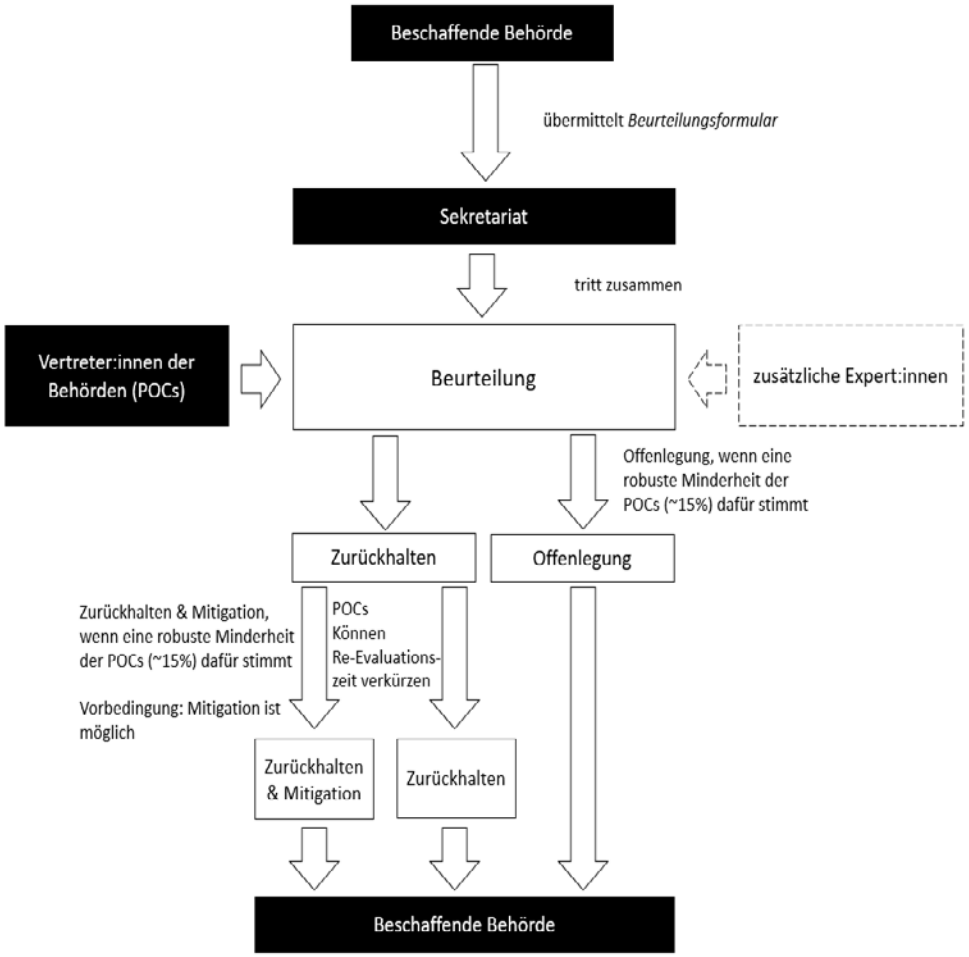

Abbildung 2 Visualisierung des institutionellen Aufbaus und des Workflow

43 Die deutsche G10 Kommission trifft sich beispielsweise monatlich.
Bundesministerium der Justiz und für Verbraucherschutz, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) § 15 G 10-Kommission

heit zuständigen Behörde), gehalten, eine "robuste Minderheit" (ungefähr 15 Prozent) für die Offenlegung zu gewinnen. Sofern keine robuste Minderheit für die Offenlegung zustande kommt, aber es mitigierende Maßnahmen gibt, kommt es zu einer zweiten Abstimmungsrunde.

In diesem Durchlauf bedarf es einer robusten Minderheit für das Zurückhalten und Mitigation. Kommt auch hier keine robuste Minderheit zustande, so wird die Schwachstelle temporär zurückgehalten. Eine zurückgehaltene Schwachstelle wird nach einem Jahr re-evaluiert. Die POCs haben bei der Beurteilung der Schwachstelle die Möglichkeit diesen Zeitraum zu verkürzen. Die jeweilige Entscheidung des Gremiums wird an die Behörde übermittelt, die die Schwachstelle beschafft hat. Sie ist weiter für das Management der Sicherheitslücke verantwortlich und hat Entscheidungen des Sekretariats bezüglich der betreffenden Schwachstelle umzusetzen.

3.5 Beurteilung

Basis des Beurteilungsverfahrens für Schwachstellen ist der Grundsatz, dass das gesamte Internet Ökosystem von der Offenlegung und dem Schließen der Schwachstellen profitiert. Ziel des Regierungshandelns sollte daher stets die Offenlegung von Schwachstellen sein, es sei denn, es gibt spezielle, legitime und gut belegbare Gründe für das Zurückhalten und den späteren Einsatz einer Schwachstelle durch die Strafverfolgungsbehörden, die Nachrichtendienste oder das Militär. Der Akteur, der die Schwachstelle vorlegt, (beispielsweise ein Nachrichtendienst) soll nicht die Schwachstelle selbst, sondern ein Formular zur Beurteilung vorlegen. Darin wird eine Bewertung bezüglich der unten aufgeführten Kriterien[44] vorgenommen. Diese Art der Darstellung erleichtert das Verständnis, denn die Schwachstelle selbst, also der Code, wäre schwerer bzw. unmöglich für die POCs nachzuvollziehen. Die Kriterien ermöglichen eine Beurteilung der technischen Beschreibung und dienen als Entscheidungsgrundlage dafür, ob die Schwachstelle unmittelbar offengelegt werden soll oder nicht. Faktoren für die Entscheidung, ob ein überragendes Interesse der Regierung an dem Zurückhalten und späteren Ausnutzung einer Schwachstelle besteht, sind:

1. Verbreitungsgrad
2. Zurverfügungstellung von Patches
3. Ausrollen von Patches
4. Mitigation

44 Der Kritierienkatalog berücksichtigt die VEP's "Defensive Equity Considerations", siehe White House, Fact Sheet: Vulnerabilities Equities Process https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20White%20House%20Fact%20Sheet%20on%20VEP%20-%20FINAL%2011152017.PDF

5. Technologische Souveränität
6. Nutzung der betroffenen Produkte
7. Entdeckung von Ausnutzungen
8. Schweregrad
9. Kollisionsraten
10. Operativer Nutzen

3.5.1 Verbreitungsgrad

Je mehr Akteure (zum Beispiel fremde Nachrichtendienste, kriminelle Hackergruppen) Kenntnis von einer Schwachstelle haben, desto höher ist die Wahrscheinlichkeit, dass die Schwachstelle auch gegen die eigenen staatlichen IT-Systeme, kritische Infrastrukturen oder die eigene Bevölkerung zum Einsatz kommen wird. Ein wichtiger Anhaltspunkt für die Beurteilung ist daher, ob nur die Behörde, die die Schwachstelle erworben hat, exklusiv über die Information zu der Schwachstelle verfügt. Dies hängt unmittelbar mit der Art und Weise der Beschaffung zusammen. Wurde die Schwachstelle von Dritten gekauft oder übernommen, stammt das Wissen aus forensischen Untersuchungen zu einem voran gegangenen Angriff, weiß zumindest der Verkäufer, beziehungsweise der damalige Angreifer darüber Bescheid. Je höher der Verbreitungsgrad, desto zwingender wird es, den *Maintainer* über die Schwachstelle zu informieren. Einerseits nimmt der operative Wert für Strafverfolger, Nachrichtendienste und Militärs ab, zugleich wächst aber auch das Risiko, dass die Lücke von Dritten genutzt wird, um die eigenen IT-Systeme anzugreifen.

3.5.2 Zurverfügungstellung von Patches

Ein anderer Aspekt bei der Offenlegung ist die Frage, wer überhaupt über eine Schwachstelle informiert werden kann, und ob die betroffene Software oder Hardware noch von einem verantwortlichen *Maintainer* betreut wird. Verwaiste Codefamilien oder Hardware, für die kein Support mehr zur Verfügung steht, erschweren die zeitnahe Bereitstellung von Patches. In anderen Fällen hat ein Produkt EOL erreicht und wird daher nicht mehr gepflegt und mit Updates auf dem aktuellsten Stand gehalten wie Nachfolgeprodukte. Produkte, die die EOL Phase bereits überschritten haben oder deren *Maintainer* nicht mehr existiert, werden selten mit einem Patch nachgesichert. In dieser Situation hilft die Offenlegung einer Schwachstelle wenig. Bei EOL Szenarien hängt allerdings viel vom betroffenen Hersteller (und letztlich dem Schweregrad der Schwachstelle) ab. Microsoft stellte beispielsweise Patches für eigene Produkte auch jenseits der EOL zur Verfügung, als die

WannaCry Schadsoftware 2017[45] die unter EternalBlue/DoublePulsar bekannt gewordenen Schwachstellen ausnutzte.

Die Akteure, die am Verfahren zur Beurteilung von Schwachstellen beteiligt sind, sollten jeweils in Erfahrung bringen, ob es einen *Maintainer* gibt, der bereit und in der Lage ist, einen Patch zu konzipieren, zu entwickeln und zu verbreiten. Je unwahrscheinlicher die Schließung per Patch ist, desto gerechtfertigter wäre es, wenn der Staat die Schwachstelle zurückhält. Die Behörden können Unternehmen und Privatnutzer:innen allerdings trotzdem warnen und zu erhöhter Vorsicht im Umgang mit der entsprechenden Hardware, Software oder Online Dienstleistung aufrufen. Das erlaubt Wirtschaft und Bürger:innen ihr jeweiliges Risiko selbst zu verringern, zum Beispiel durch den Verzicht auf die Nutzung bestimmter Geräte oder Dienste.

3.5.3 Ausrollen von Patches

Abgesehen davon, wie wahrscheinlich die Verfügbarkeit eines Patch ist, empfiehlt sich auch, dass die Verfahrensbeteiligten erörtern, wie kompliziert das Einspielen eines Patches zur Schließung der Schwachstelle ist[46]. Zwar ist eine bis ins letzte Detail gehende Bewertung hier schwierig, von einer abstrakteren Warte aus aber erlaubt dies eine erste Abschätzung, wie lange es dauert, bis sich ein Patch verbreitet: ist beispielsweise der Rückruf von Hardware notwendig oder kann ein Patch durch ein Software Update per Fernzugriff eingespielt werden. Die Einschätzung, ob und wie schnell sich ein Patch verbreitet, ist überaus sinnvoll für eine entsprechende Beurteilung[47]. Ähnlich wie beim Kriterium zur Verfügbarkeit eines Patches muss die mangelnde Verbreitungswahrscheinlichkeit dabei nicht automatisch dazu führen, dass die Schwachstelle zurückgehalten wird. In seltenen Fällen mit extrem großen Risiken kann eine Regierung durch eine allgemeine öffentliche Warnung die Bereitschaft zum Einspielen des Sicherheitsupdates verbessern oder aber andere Vorsichtsmaßnahmen treffen, beispielsweise die

45 Steve Ragan, Microsoft patches Windows XP and Server 2003 due to WannaCrypt attacks

46 Akzeptanz und Verbreitung von Patches ist eine komplizierte Angelegenheit, nicht zuletzt, weil es mehr als einen *Maintainer* und Endnutzer gibt. Original Equipment Manufacturers (OEM) können beispielsweise einen Patch zur Verfügung stellen, aber er muss über zwischengeschaltete Akteure an den:die Endnutzer:in durchgereicht werden. Außerdem sind große IT-Infrastrukturen komplex und heterogen. Patches müssen intensiv getestet werden bevor sie ausgerollt werden können, um sicherzustellen, dass sie keine unerwarteten Probleme hervorrufen.

47 Enthält ein Patch nützliche Information zu einer Schwachstelle für einen potentiellen Angreifer, wird aber nicht eingespielt und es existiert keine mitigierende Maßnahme, kann eine Offenlegung mehr Schaden anrichten als das Zurückhalten der Schwachstelle.

Empfehlung aussprechen, die betroffene Software, Hardware oder den entsprechenden Online Dienst nicht mehr zu nutzen.

3.5.4 Mitigation

Die Möglichkeit zur Begrenzung des Schadens durch mitigierende Maßnahmen ist ein weiterer wichtiger Parameter. Ist eine Mitigation möglich, können Regierungsstellen und andere ausgewählte Akteure diese entsprechenden Vorsichtsmaßnahmen treffen, ohne zwangsläufig die Schwachstelle offen zu legen. In Deutschland könnten diese „ausgewählten Akteure" diejenigen sein, die von besonderem staatlichen Interesse sind, beispielsweise Vertragspartner der Streitkräfte oder Betreiber kritischer Infrastrukturen. Man spricht von „Institutionen von besonderem staatlichen Interesse" (INSI[48]). Nur weil eine Mitigation möglich ist, muss eine Schwachstelle nicht zwangsläufig zurückgehalten werden, denn alle anderen Akteure bleiben weiterhin angreifbar. Diese Option senkt lediglich das Risiko derer, die die entsprechenden mitigierenden Maßnahmen treffen. In seltenen Fällen kann es sinnvoll sein eine Schwachstelle kurzfristig zurückzuhalten und gleichzeitig mitigierende Maßnahmen zu implementieren. Sollte eine Mitigation nicht möglich sein, bleiben nur das unmittelbare Offenlegen der Schwachstelle und das temporäre Zurückhalten als Optionen übrig.

3.5.5 Technologische Souveränität

Bei der Beurteilung einer Schwachstelle von Produkten eines inländischen Unternehmens müssen ökonomische Überlegungen in die Bewertung einbezogen werden. Um die Sicherheit nationaler Hardware, Software oder Online Dienste nicht zu untergraben, hat die Beurteilung dieser Schwachstellen besondere Bedeutung. Die Nutzer:innen der entsprechenden Produkte könnten überproportional aus dem eigenen Land stammen, einschließlich eigener Behörden. Das Ansehen der Firma könnte ebenfalls leiden, wenn die Regierung die Offenlegung der Schwachstelle verzögert, und damit die Möglichkeit zur Mitigation oder zum Einspielen von Patches hinauszögert. Es muss den zuständigen Regierungsstellen bewusst sein, dass sich entsprechende Effekte für die Vertrauenswürdigkeit heimischer Marken insgesamt negativ auf die Sicherheit der Wirtschaft auswirken können, die Teil der nationalen Sicherheit ist.

48 Bundesamt für Sicherheit in der Informationstechnik, Allianz für Cybersicherheit Jahresbericht 2012/2013

3.5.6 Nutzung der betroffenen Produkte

Von großer Bedeutsamkeit für die Beurteilung einer Schwachstelle ist das Wissen darüber, wo die betroffene Hardware, Software oder die jeweiligen Online Dienste eingesetzt werden und wie weit verbreitet sie sind. Kommen sie zum Beispiel bei den eigenen Streitkräften oder bei befreundeten Armeen zum Einsatz, in Regierungsnetzwerken, kritischen Infrastrukturen, Firmen von besonderem Interesse für den Staat, in der Sicherheitsindustrie, der privaten Wirtschaft oder ist es ein in der Bevölkerung weit verbreitetes Produkt. Dabei ist mit zu bedenken, dass letztere auch von Regierungs- und Unternehmensangestellten zu Hause und außerhalb des Landes benutzt werden (etwa von Militärs oder Botschaftspersonal), und auch im Rahmen besonders vertraulicher Kommunikation (zum Beispiel von Journalisten oder Anwälten) zum Einsatz kommen. Dies kann das Bedrohungsszenario verändern.

3.5.7 Entdeckung von Ausnutzungen

Je niedriger die Wahrscheinlichkeit, dass Sicherheitsbehörden und Militärs einen laufenden Angriff unter Ausnutzung der zu beurteilenden Schwachstelle detektieren können, desto vordringlicher wird die Notwendigkeit zur Offenlegung der Schwachstelle. Kann die Schwachstelle unentdeckt von eigenen nationalen Sicherheitsbehörden durch Dritte ausgenutzt werden, wäre das Zurückhalten der Schwachstelle kontraproduktiv für die öffentliche Sicherheit. In einem solchen Fall sollte die Entscheidung bezüglich des Umgangs mit der Schwachstelle in Richtung Offenlegung gehen.

Die Bedrohungslage ist nicht zwingend symmetrisch; die Ausnutzung einer Schwachstelle kann für einen gegnerischen Akteur schwer und gleichzeitig einfach für die eigenen Sicherheitsbehörden sein; oder sie kann zu schwierig sein, um vom Gegner überhaupt ausgenutzt zu werden, nach dem Motto

„Nobody, but us“ (NOBUS[49]), also „Niemand, außer uns“.

3.5.8 Schweregrad

Eine Reihe von Faktoren bestimmen den Schweregrad einer Schwachstelle. Ein Aspekt zum Beispiel ist, ob sie aus der Ferne (zum Beispiel über das Internet) ausgenutzt werden kann, oder nur in räumlicher Nähe zum jeweiligen Gerät (zum Beispiel über WLAN oder Bluetooth) oder ob sogar der direkte physische Zugriff auf das Gerät notwendig ist. Eine Schwachstelle, die per Fernzugriff ausgenutzt werden kann, muss als schwerwiegender klassifiziert werden als eine, die den direkten Zugriff auf das Gerät erfordert. Darüber hinaus spielt es eine elementare Rolle, ob zur Ausnutzung der Schwachstelle eine Interaktion des:r Nutzers:in (zum Beispiel das Öffnen eines Anhangs oder das Anklicken eines Links) erforderlich ist oder nicht. Ein weiterer Aspekt ist, ob die Schwachstelle allein ausreicht, um Hardware, Software oder einen Online Dienst zu kompromittieren, oder ob eine Kombination von Schwachstellen hierzu notwendig ist. Der Umstand, dass die Schwachstelle allein nicht für einen Exploit ausreicht oder dass der mögliche Angriff weniger gravierend ist als bei einer Kombination mit anderen, macht ein Zurückbehalten der betreffenden Schwachstelle nicht unbedingt weniger problematisch: hier ist jeweils die Gesamtschau der aktuell im Umlauf befindlichen Schwachstellen zu berücksichtigen. Mit einzukalkulieren ist darüber hinaus die Art des möglichen Schadens: kann durch Ausnutzung der Schwachstelle ein Dienst unterbrochen werden oder erlaubt sie via Hintertür den Zugriff auf den gesamten Datenbestand eines Systems, einschließlich der Möglichkeiten, laufenden Datenverkehr zu überwachen und Sensoren zu manipulieren? Diese unterschiedlichen Aspekte müssen berücksichtigt werden, denn die Unterbrechung eines Emaildienstes stellt eine andere Art von Bedrohung dar als ein umfänglicher Zugriff auf den gleichen Dienst, durch den der:die Angreifer:in alle aktuellen und vergangenen Emails lesen kann. Das Common Vulnerability Scoring System (CVSS[50]) ist ein Beispiel dafür, wie die Schwere von Schwachstellen eingestuft werden kann.

---

49 „The premise of the NOBUS approach is simple: when there is tension between offense and defense, the United States aspires to secure communications against all forms of signals intelligence collection—except those forms of interception that are so complex, hard, or inaccessible that only the United States uses them“, Ben Buchanan, Nobody But Us Michael Hayden, 2013: „If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers in the basement in order to work it you kind of think 'NOBUS' and that's a vulnerability we are not ethically or legally compelled to try to patch — it's one that ethically and legally we could try to exploit in order to keep Americans safe from others“, Andrea Peterson, Why everyone is left less secure when the NSA doesn't help fix security flaws cited in Tristan Caulfield, Christos Ioannidis and David Pym, The U.S. Vulnerabilities Equities Process: An Economic Perspective

50 FIRST, Common Vulnerability Scoring System SIG

Alle hier genannten Aspekte zur Beurteilung einer Schwachstelle sind gemeinsam zu betrachten. Die Schwere einer Schwachstelle zusammen mit der Art und dem Umfang der betroffenen Produkte führt jedoch zu einer besonders kritischen Kombination. Eine Schwachstelle, die eine Abschaltung von Windows Rechnern aus der Ferne erlaubt, ist beispielsweise ein Kandidat für die Offenlegung, weil die Software weit verbreitet ist, auch wenn der erwartbare Schaden gegebenenfalls nicht so groß ist. Eine Schwachstelle bei einem Herzschrittmacher, der hundertfach verkauft wurde, empfiehlt sich ebenfalls zur Offenlegung, wenn die Schwachstelle eine Fernabschaltung erlaubt. Eine Schwachstelle in einem Online-Dienst hingegen, der nur von ausländischen Militärs genutzt wird, empfiehlt sich eher zum Zurückhalten, unabhängig davon, welcher Schaden damit angerichtet werden kann.

Der Faktor Schweregrad gewinnt zusätzliche Bedeutung, wenn er unter dem Gesichtspunkt des potenziellen Versagens der eigenen Sicherungsvorkehrungen betrachtet wird. Beispielhaft für dieses Szenario ist die Entwendung und Veröffentlichung der EternalBlue-Schwachstelle, die von der NSA zurückgehalten wurde, mutmaßlich durch die Gruppierung *The Shadow Brokers*[51].

3.5.9 Kollisionsraten

Werden Schwachstellen parallel von zwei oder mehreren Akteuren entdeckt, wie beim Heartbleed Bug in OpenSSL oder, in jüngster Zeit, bei Spectre und Meltdown, spricht man von einer Kollision. Das Kalkulieren von Kollisionsraten verschiedener Schwachstellentypen in verschiedener Software kann einen Hinweis liefern, wie groß die Wahrscheinlichkeit ist, dass ein Dritter die gleiche Schwachstelle in der Zukunft entdeckt, oder sie bereits entdeckt hat. Je höher die Kollisionsrate, desto wahrscheinlicher ist, dass ein anderer Akteur die Schwachstelle findet und anschließend auch ausnutzen kann. Das macht das Zurückhalten dieser Schwachstelle wiederum riskanter. Regierungen sollten Kollisionsraten für zur Beurteilung anstehende Sicherheitslücken so gut wie möglich kalkulieren oder auf der Basis vergleichbarer Schwachstellen ermitteln. Die Forschung in diesem Bereich steht noch am

51 Check Point IPS Research Team, BROKERS IN THE SHADOWS: Analyzing vulnerabilities and attacks spawned by the leaked NSA hacking tools

Anfang und kommt zu widersprüchlichen Ergebnissen[52]. Ohne weitergehende Forschungsanstrengungen, bleiben empirische Daten für spezifische Schwachstellen(-arten) Mangelware. Unabhängige Forschung zu Kollisionsraten sollte daher von der Regierung gefördert werden. Bis zum Vorliegen entsprechender Ergebnisse sollten Kollisionsraten in die Beurteilung von Schwachstellen einfließen, sie sollten aber kein zentraler Aspekt sein.

3.5.10 Operativer Nutzen

Ein weiteres, entscheidendes Kriterium betrifft den operativen Nutzen einer Schwachstelle für die Sicherheitsbehörden, Nachrichtendienste und Militärs. Das schließt Aspekte wie den geplanten Anwendungsbereich (Nachrichtengewinnung, militärische Operationen im Cyber-Raum oder Ermittlungen der Strafverfolgungsbehörden), ob vergleichbare Schwachstellen bereits zurückgehalten und/oder eingesetzt werden, so wie die operative Effektivität der Schwachstelle mit ein. Zur Bestimmung der Effektivität gehört eine Einschätzung darüber, ob es weniger invasive Alternativen gibt, um zum Beispiel an die Informationen über eine Zielperson zu gelangen, wie entscheidend der Beitrag der Schwachstelle für eine Operation ist und wie wichtig die Operation selbst für die nationale Sicherheit ist. Wie bereits ausgeführt, profitiert das Internet Ökosystem grundsätzlich von der Schließung von Schwachstellen und Ziel der Politik sollte daher die unmittelbare Offenlegung von Schwachstellen sein, abgesehen von den Fällen, in denen spezielle, legitime Gründe für das Zurückhalten einer Schwachstelle vorliegen.

3.6 Management

3.6.1 Handhabung und Aufbewahrung

Staatliche Stellen können nur dann gefahrlos Schwachstellen handhaben, wenn sie über die Fähigkeit verfügen, diese korrekt abzusichern (siehe „Schwachstellen sicher verwahren“). Behörden, die Schwachstellen nicht absichern können, dürfen diese nicht handhaben bzw. aufbewahren. Behörden, denen aufbewahrte Schwachstellen gestohlen werden, müssen sich einem Sicherheitsaudit unterziehen, bevor sie erneut mit dem Management von Schwachstellen betraut werden können.

52 Trey Herr, Bruce Schneier and Christopher Morris, Taking Stock: Estimating Vulnerability Rediscovery
Lillian Ablon and Andy Bogart, Zero Days Thousands of Nights
Katie Moussouris and Michael Siegel, The Wolves of Vuln Street:The 1st System Dynamics Model of the 0day Market presented at RSA Conference 2015

3.6.2 Re-Evaluierung

Aufgrund möglichen Veränderungen in der Beurteilung einer Schwachstelle, müssen diese regelmäßig re-evaluiert werden – und zusätzlich jedes Mal, wenn sie zum Einsatz kommen. Standardmäßig findet die Re-Evaluierung nach einem Jahr statt[53], es sei denn, die POCs haben sich im Rahmen des Beurteilungsverfahrens auf eine kürzere Zeitspanne geeinigt. Wie erwähnt, muss auch die Nutzung der Schwachstelle eine erneute Evaluierung auslösen, da davon ausgegangen werden muss, dass der Einsatz einer Schwachstelle zur Entdeckung dieser durch Dritte führen kann.

3.6.3 Kurzfristiges Zurückhalten

Alle Schwachstellen werden grundsätzlich nur für eine bestimmte Zeit zurückgehalten und müssen irgendwann offengelegt werden: die Frage ist lediglich, zu welchem Zeitpunkt. Das kurzfristige Zurückhalten einer Schwachstelle ist ein Sonderfall, der Behörden ein sehr kurzes Zeitfenster öffnet, innerhalb dessen sie bestimmte Schwachstellen für operative Zwecke zurückhalten können, während sie parallel Mitigationsmaßnahmen in Kraft setzen. Dies kann nur unter folgenden Bedingungen erfolgen:

- die Schwachstelle wurde durch forensische Ermittlungen aufgedeckt
- eine kurzfristig einsetzbare Mitigation steht zur Verfügung
- die Mitigation wird so schnell wie möglich ausgerollt
- das Beurteilungsgremium entscheidet auf Zurückhalten der Schwachstelle
- das Zurückhalten dient einem spezifischen singulären Zweck (der Ermittlung eines Angreifers in einer laufenden forensischen Untersuchung[54])
- das kurzfristige Zurückhalten endet, wenn der spezifische Zweck erfüllt ist, zum Beispiel die entsprechende Ermittlung abgeschlossen ist. Eine kurzfristig zurückgehaltene Schwachstelle muss bei jeder anstehenden Beurteilung (jeden Monat) erneut evaluiert werden.

53 White House, Vulnerabilities Equities Policy and Process for the United States Government (UNCLASSIFIED) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

54 Ende 2017/Anfang 2018 hielten die deutschen Sicherheitsbehörden Informationen über einen gegen das Auswärtige Amt gerichteten Angriff zurück, um Tatmethoden, Technik, Tatmotiv und Identität des Angreifers zu ermitteln. taz, Cyberangriff auf Ministerien Hacker noch im Bundesnetz

3.6.4 Mitigation

Mitigation ist die „detection and protection strategy used to safeguard networks, servers and applications by IT administrators in order to minimize the effect of malicious traffic and intrusion attempts while maintaining functionality for users“[55]. Das Vorgehen ist unabhängig davon, ob ein Patch vom *Maintainer* zur Verfügung steht, dessen Software, Hardware oder Online Dienst die Schwachstelle aufweist. Nicht immer steht ein solcher Mechanismus zur Schadensbegrenzung im Fall einer Schwachstelle zur Verfügung. Im hier vorgeschlagenen Verfahren sollten Mitigationsmaßnahmen in Zusammenarbeit mit oder federführend durch die nationale IT-/ Cyber-Sicherheitsbehörde entwickelt und verbreitet werden.

Kurzfristige Mitigation bei verzögerter Offenlegung
Die Verzögerung der Offenlegung einer Schwachstelle kann manchmal notwendig werden, weil sonst laufende Untersuchungen durch die Offenlegung behindert werden könnten. Ein Anwendungsbereich für Mitigationsmaßnahmen ist daher das kurzfristige Zurückhalten einer Schwachstelle. Das Risiko eines Angriffs mittels der Schwachstelle wird dabei etwas länger in Kauf genommen, um den Abschluss der laufenden Untersuchungen (zum Beispiel forensische Aufklärung/ Ermittlung von Angreifern) zu gewährleisten. Wird die Offenlegung einer Schwachstelle zugunsten eines solchen kurzfristigen Zurückhaltens wegen des operativen Nutzens für die anstehende/ laufende Operation verzögert, kann gleichzeitig die Implementierung von Mitigationsmaßnahmen Bestandteil der in diesem Sinn getroffenen Entscheidung sein. Zwar steigt damit das Risiko, dass im Rahmen der Mitigationsmaßnahmen die zurückgehaltene Schwachstelle offengelegt wird, gleichzeitig aber wird der Schutz für die eigenen Systeme (Regierungsnetzwerke, INSI, usw.) gegenüber der Ausnutzung der Schwachstelle damit erhöht.

Langzeit Mitigation mit verzögerter Offenlegung
Eine weitere Anwendung von Mitigationsmaßnahmen kann darin bestehen, diese auf Dauer einzusetzen, während man eine Schwachstelle zurückhält. Wird im Beurteilungsverfahren das Zurückhalten einer Schwachstelle befürwortet und Mitigation ist möglich, können die POCs auf Zurückhalten der Schwachstelle mit Mitigation entscheiden. Die Schwachstelle wird dann zurückgehalten, zugleich wird jedoch die Mitigation bei einer beschränkten Anzahl von Akteuren, zum Beispiel die als kritisch für die nationale Sicherheit betrachtet werden (siehe INSI), eingeleitet. Auf diese Weise lässt sich der operative Wert einer Schwachstelle mit einem gegenüber einer soforti-

55 radware, Attack Mitigation

gen Offenlegung verringerten Risiko der Entdeckung kombinieren. Allerdings erhöht Mitigation auch die Wahrscheinlichkeit, dass die Schwachstelle bekannt wird.

Regierungen haben sowohl bei kurzfristigem als auch langfristigem Zurückhalten mit Mitigation weniger Möglichkeiten entsprechende Mechanismen zu entwickeln als die dazugehörigen *Maintainer*. Maßnahmen wie das Blockieren des Zugangs zum Netz oder Anweisungen an Nutzer, bestimmte Features nicht zu benutzen, greifen allenfalls für kurze Zeit, beheben aber nicht das zugrunde liegende Problem des verwundbaren Codes.

3.6.5 Offenlegung

Sobald entschieden wurde, eine Schwachstelle offenzulegen, muss sie von der Behörde übergeben werden, die für den CVD zuständig ist. Meist wird dies die nationale Behörde für IT- und Cybersicherheit sein. Der Prozess der Offenlegung sollte den Bestimmungen des CVD folgen.

3.7 Schutz- und Kontrollmaßnahmen

3.7.1 Schwachstellen sicher verwahren

Die sichere Verwahrung von Schwachstellen ist entscheidend und zieht sich durch den gesamten Prozess, von der Beschaffung bis hin zur Offenlegung. Fehler bei dieser Absicherung können katastrophale Konsequenzen haben. EternalBlue hat dies beispielhaft illustriert. Die EternalBlue Schwachstelle wurde von der NSA entwendet und dann für die WannaCry- und NotPetya-Malware ausgenutzt[56]. Aktuelle Ansätze greifen hier noch zu kurz. Wie hoch der Prozentsatz der von Regierungen gehorteten Schwachstellen im Stil von EternalBlue ist, lässt sich auf der Basis der veröffentlichten Informationen unmöglich feststellen; aber schon eine sehr kleine Zahl ist besorgniserregend. Die Schwierigkeit, Schwachstellen zu jeder Zeit perfekt gegen unbefugten Zugriff abzusichern, unterstreicht die Gefahren eines massenhaften Zurückhaltens von Schwachstellen. Ziel muss sein, jeden nicht autorisierten Zugriff auf die Schwachstelleninformation durch Dritte zu verhindern. Ein Aspekt, der für sich genommen noch nicht zur sicheren Verwahrung von Schwachstellen geführt hat, ist die Einstufung dieser und damit verbunden Anwendung entsprechender Sicherheitsmechanismen. Wenn selbst mächtige Geheimdienstorganisationen wie die NSA Schwierigkeiten hat, zurückgehaltene Schwachstellen angemessen gegen einen Zu-

56 Lily Hay Newman, Why Governments Won't Let Go of Secret Software Bugs

griff durch Dritte zu schützen, müssen Regierungen gänzlich neue Konzepte dafür entwickeln. Dazu sollte entsprechende Forschung unterstützt und die Erfahrungen anderer Bereiche berücksichtigt werden.

3.7.2 Parlamentarische Kontrolle

Da das Zurückhalten von Schwachstellen erhebliche Auswirkungen auf die Wirtschaft, auf Grundrechte, IT Sicherheit und die öffentliche Sicherheit mit sich bringt, ist die parlamentarische Kontrolle über das Verfahren von elementarer Bedeutung[57]. Das Sekretariat sollte jährlich einen eingestuften Bericht an entsprechende Gremien übersenden (USA zum Beispiel: House of Representatives Homeland Security Committee, Senate Homeland Security and Governmental Affairs Committee, House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence[58] oder in Deutschland zum Beispiel: Verteidigungsausschuss, Ausschuss für Inneres und Heimat, Ausschuss Digitale Agenda, Parlamentarisches Kontrollgremium). Für den Bericht erforderlich sind folgende Datenpunkte:

- Zahl der zurückgehaltenen Schwachstellen
- durchschnittliche Aufbewahrungszeit
- operativer Nutzen abgeschlossener Operationen
- Effektivität der Mitigationsmaßnahmen
- Bewertungsbögen aller zurückgehaltenen Schwachstellen, die inzwischen offengelegt wurden

3.7.3 Transparenz

Transparenzberichte sind jährlich anzufertigen und in einer Form zu präsentieren, die externen Experten eine eigene Einschätzung erlaubt, ob Beurteilungsverfahren und Management der zurückgehaltenen Schwachstellen sich positiv auf die generelle Sicherheit des Internet Ökosystems ausgewirkt haben, indem die Offenlegung priorisiert und das Zurückhalten von Schwachstellen auf wohlbegründete Fälle beschränkt wurde. Ausführliche Beschreibungen aller aktuell gehaltenen Schwachstellen gehen nicht in den

57 Auch wenn der US-amerikanische Vulnerability Equities Process zum Zeitpunkt der Abfassung der Studie keine parlamentarische Kontrolle vorsieht, sind erste Schritte in diese Richtung bereits unternommen worden.
U.S. House of Representatives Permanent Select Committee on Intelligence, AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 6237 OFFERED BY MR. NUNES OF CALIFORNIA
U.S. Congress, A BILL To authorize appropriations for fiscal years 2018 and 2019 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purpose.

58 Chase Gunter, House passes vulnerability disclosure oversight bill

Transparenzbericht ein. Der Bericht wird vom Sekretariat vorbereitet, online veröffentlicht und soll folgende Datenpunkte enthalten:

- Zahl der Schwachstellen, die beschafft und direkt offengelegt wurden
- Zahl der Schwachstellen, die beschafft, mitigiert und aufbewahrt wurden
- Zahl der Schwachstellen, die beschafft und aufbewahrt wurden
- Zahl der Schwachstellen, die aufbewahrt und eingesetzt wurden
- durchschnittliche Aufbewahrungszeit
- Zahl der Schwachstellen, die aufbewahrt wurden und während der Zurückhaltung von Dritten erfolgreich ausgenutzt wurden

4. Zusammenfassung

Staaten stehen bei den unterschiedlichen offensiven Strategien im Cyber-Raum, von klassischer Spionagetätigkeit, strafrechtlichen Ermittlungen und Konzepten der Kriegsführung im Wettbewerb. Die Beurteilung und das Management von Schwachstellen durch den Staat wird angesichts dieser Entwicklung zu einer zentralen Herausforderung. Regierungen müssen herausfinden, wie sich die unterschiedlichen Interessen (Grundrechte, Wirtschaft, öffentliche Sicherheit und IT-Sicherheit) sinnvoll abwägen lassen. Die Vereinigten Staaten haben bereits eine Reihe wichtiger Schritte in die richtige Richtung unternommen, indem sie ein Verfahren zur Schwachstellenbewertung umgesetzt und in ersten Ansätzen vorgestellt haben. Es ist nun die Aufgabe der übrigen Staaten[59], diesen Prozess nachzuvollziehen und vergleichbare Mechanismen zu beschließen und weiter zu entwickeln, und dabei transparent Einblick zu gewähren, was sie in diesem Bereich machen. Auch das aktuelle US-Verfahren kann von weiteren Verbesserungen profitieren, etwa von verpflichtenden Auflagen zur Berichterstattung gegenüber dem US-Kongress und der Öffentlichkeit.

Die vorliegende Studie basiert auf dem bestehenden US-Verfahren zur Beurteilung und zum Management von Schwachstellen durch staatliche Stellen. Wertvolle Hinweise lieferten die Diskussionen und kritische Auseinandersetzungen, die in den vergangenen Jahren über dieses Verfahren geführt wurden, sowie Stellungnahmen und Einschätzungen aus dem Cybersicherheitsexpert:innen-Netzwerk des Transatlantic Cyber Forums. Der hier vorgeschlagene Mechanismus mit seinen Einzelelementen soll die Debatte über den Umgang von Regierungen mit Schwachstellen bereichern und mögliche Lösungsvorschläge für die bestehenden Herausforderungen anbieten.

59 Centre for European Policy Studies (CEPS), Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

Über die Stiftung Neue Verantwortung

Cyber-Sicherheitspolitik wird zunehmend ein elementares Feld nationaler und internationaler Politik. Hierzu gehören unter anderem die institutionelle Aufstellung, die Ressourcenlage und -verteilung, Prozesse und rechtliche Rahmenbedingungen, sowie die Auswirkungen nationaler Politik auf die internationalen Beziehungen ("Spillover-Effekte").

Auch wenn vieler dieser Herausforderungen subsidiär auf nationaler Ebene begegnet werden muss, so ist es zwingend notwendig international voneinander zu lernen und zusammen gute Lösungen, sogenannte Best Practices, zu entwickeln und diese weiterzuverbreiten. Zu diesem Zweck wurde das Transatlantic Cyber Forum, kurz: "TCF", von der Stiftung Neue Verantwortung gegründet.

Das TCF besteht derzeit aus mehr als 100 amerikanischen, deutschen und weiteren EU-Expert:innen, welche in Zivilgesellschaft, Wissenschaft und Privatwirtschaft tätig sind.

Das Transatlantic Cyber Forum wird von der Robert Bosch Stiftung und der William and Flora Hewlett Foundation gefördert.

Über den Autor

Sven Herpig ist Leiter des Transatlantic Cyber Forums (TCF) und bringt dort die Expert:innen von beiden Seiten des Atlantiks zu allen Facetten der Innen-, Sicherheits- und Verteidigungspolitik im Cyber-Raum zusammen.

So erreichen Sie den Autor

Dr. Sven Herpig
Projektleiter Internationale Cyber-Sicherheitspolitik
sherpig@stiftung-nv.de
+49 (0)30 81 45 03 78 91

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de