Zeitschrift für Praktische Philosophie
Band 10, Heft 1, 2023, S. 79–104
www.praktische-philosophie.org
https://doi.org/10.22613/zfpp/10.1.3

Forschende in der Angriffsrolle

Zum besonderen forschungsethischen Bedarf in der IT-Sicherheit

Researchers in the Role of Attackers

Research Ethical Challenges in Cyber Security

Sebastian Weydner-Volkmann, Bochum & Kaya Cassing, Bochum

Zusammenfassung: Infolge der tiefgreifenden Durchdringung unserer Lebenswelt mit digitalen Systemen hat sich die gesamtgesellschaftliche Anforderung formiert, diese Systeme gegen immer neue Formen von Angriffen absichern zu können. In diesem Beitrag zeigen wir, inwiefern der IT-Sicherheitsforschung hierbei eine zentrale Rolle zukommt, aber auch, dass im Rahmen dieser Rolle eine besondere forschungsethische Problematik entsteht. Weil IT-Sicherheitsrisiken strukturell neuartige Probleme für die gesellschaftliche Gewährleistung von Sicherheit aufwerfen, treten Forschende systematisch auch in die Rolle der Angreifenden. Dabei erhöhen Forschende durch den notwendigen Schritt der Veröffentlichung gefundener Lücken die Gefährdungslage von IT-Systemen. Zugleich zielt die Entwicklung von Angriffstechniken normativ auf eine Stärkung gesamtgesellschaftlicher Sicherheit: die Sicherheitslücken sollen geschlossen und die Robustheit von IT-Systemen vergrößert werden.
Hier wird ein Konflikt im Umgang mit IT-Sicherheitsrisiken deutlich, der einen Bedarf an ethischer Orientierung erzeugt. Im Beitrag zeigen wir, inwiefern sich in der Forschungspraxis auch bereits Anfänge einer systematischen ethischen Reflexion als Antwort auf diesen Bedarf herausgebildet und institutionalisiert haben. Da die Problematik im Umgang mit Sicherheitslücken aber noch nicht adäquat adressiert wird, vertreten wir die These, dass in der IT-Sicherheitsforschung der Schritt hin zu einer Bereichsethik für IT-Sicherheitsforschung ein Desiderat ist, um so adäquatere Orientierungsangebote für Forschende entwickeln und um die breitere gesellschaftspolitische Rolle der Sicherheitsforschung reflektieren zu können.

Schlagwörter: Informationstechnik, IT-Sicherheit, Angewandte Ethik, Forschungsethik, Sicherheitslücke, Risiko

Abstract: As a result of the proliferation of digital technology in our lifeworld, a societal need for protection of computer systems against ever new forms of attacks has emerged. In this contribution, we show that IT security research plays a central role in addressing this need, but also that this role raises certain problems from a research ethical perspective. IT security risks raise structurally new challenges for the societal production of security, which imply that researchers take on the role of attackers. When researchers make their findings on viable forms of attacks public, this increases the threat to IT systems. At the same time, the scientific publishing is normatively guided by the goal of strengthening societal security: the vulnerabilities are meant to be closed and the robustness of IT systems strengthened.
What becomes visible here are conflicts in dealing with IT security risks that imply a need for ethical orientation. In our contribution, we explore the beginnings of systematic ethical reflection that have emerged in the field and been institutionalized in an effort to answer this need. However, since the challenges have not been adequately addressed so far, we propose that IT security research should become a new field in applied ethics so as to provide more adequate orientation to researchers and to discuss its socio-political role at large.

Keywords: Information technology, cyber security, applied ethics, research ethics, vulnerability, risk

1 Einleitung

IT-Systeme[1] nehmen in nahezu allen gesellschaftlichen Lebensbereichen eine zentrale Rolle ein. Infolge dieser tiefgreifenden Durchdringung unserer Lebenswelt mit digitalen Systemen entstanden aber auch neue individuelle und gesellschaftliche Vulnerabilitäten, zu denen insbesondere auch sogenannte Sicherheitslücken in IT-Systemen zählen. Weil bei einem erfolgreichen Ausnutzen einer Sicherheitslücke je nach System gravierende Auswirkungen für Individuen, Unternehmen, Institutionen, Behörden bis hin zu ganzen Gesellschaften („kritische Infrastruktur", KRITIS) entstehen können, hat sich die Anforderung formiert, digitale Systeme gegen immer neue

1 Die in diesem Paper präsentierte Forschung wurde gefördert durch das Forschungskolleg „SecHuman – Sicherheit für Menschen im Cyberspace" des Landes NRW. Wir danken für die wichtigen Hinweise im Peer-Review-Verfahren.

Formen von Angriffen abzusichern: „Ein hohes IT-Sicherheitsniveau ist ein gesamtgesellschaftliches Anliegen“ (Wagner 2020, 116).

Neben geheimdienstlichen und militärischen Operationen (*cyber espionage, cyber warfare*) zählen kriminelle Angriffe bereits seit Jahren zu den zentralen Bedrohungen. Dabei haben sogenannte „Ransomware“-Attacken stark an Bedeutung gewonnen, bei denen Schadsoftware durch Ausnutzen einer Sicherheitslücke IT-Systeme kompromittiert. Zunächst werden dabei wichtige und sensible Daten auf den kompromittierten Systemen verschlüsselt und gegebenenfalls auch ausgeleitet. Anschließend kann dann Lösegeld für die Entschlüsselung der Systeme erpresst werden.

> „Ransomware zählte auch im Jahr 2020 zu den primären Bedrohungen für Unternehmen und öffentliche Einrichtungen. Von allen Modi Operandi im Phänomenbereich Cybercrime besitzt Ransomware das höchste Schadenspotenzial.“ (BKA 2020, 22)

Dabei zeigt sich insbesondere mit Blick auf KRITIS, „dass erfolgreiche Ransomware-Angriffe drastische Folgen für die Zivilbevölkerung nach sich ziehen und elementare Services des öffentlichen Geschehens sabotieren können“ (BKA 2020, 22). Dies wird anhand des Ransomware-Angriffs auf die Uniklinik Düsseldorf deutlich, bei dem nach Ausnutzung einer Sicherheitslücke die IT-Systeme für die Notfallversorgung abgeschaltet werden mussten (Heise online 2020; BKA 2020, 26). Daher mussten Patientinnen[2] in teils weiter entfernte Kliniken verlegt werden, wobei eine Patientin verstarb (Heise online 2020). Zwar ist ungeklärt, wie die verspätete Behandlung und der Tod der Patientin zusammenhängen, doch wird deutlich, wie existentiell der Schutz digitaler Systeme für die Sicherheitsproduktion moderner Gesellschaften ist. Auch wenn Polizeibehörden Ermittlungserfolge vorweisen können (BKA 2020, 33ff), steht eine effektive Repression cyber-krimineller Handlungen vor großen Hürden. Daher kommt der *Forschung* zu IT-Sicherheitslücken eine zentrale Rolle in der gesellschaftlichen Sicherheitsproduktion zu: „IT Sicherheitsforschung, die das Ziel der Aufdeckung von Sicherheitsschwachstellen verfolgt, ermöglicht oftmals erst die schnelle und lückenlose Schließung potentieller Angriffsmöglichkeiten“ (Wagner 2020, 116). Konsequenterweise wird bei staatlichen Investitionen in Forschungs-

2 Wir nutzen in diesem Text das generische Femininum wo immer uns eine geschlechtsneutrale Form (etwa „Forschende“) unpraktisch erscheint.

programme zur IT-Sicherheit dann auch deren gesellschaftliche Bedeutung betont (BMBF 2020).

In diesem Artikel werden wir für den akademischen Kontext zeigen, dass im Rahmen dieser Rolle in der gesellschaftlichen Sicherheitsproduktion ein besonderer forschungsethischer Bedarf entsteht. Wir werden zeigen, dass dies insbesondere deshalb der Fall ist, weil IT-Sicherheitsrisiken strukturell neuartige Probleme für die gesellschaftliche Gewährleistung von Sicherheit aufwerfen und Forschende deshalb systematisch auch in die Rolle der Angreifenden treten – wodurch sich dann aber eine besondere ethische Problematik im Umgang mit der Veröffentlichung ihrer Forschungsergebnisse ergibt, die aktuell nur unzureichend gelöst ist.

Hierzu werden wir zunächst den Sicherheitsbegriff der IT-Sicherheitsforschung skizzieren und dabei grob umreißen, inwiefern gängige Konzeptionen der geistes- und sozialwissenschaftlichen Sicherheitsforschung die IT-Sicherheitslücke als ein Kernphänomen moderner gesellschaftlicher Vulnerabilität bislang nur unzureichend reflektieren (Abschnitt 2). Anschließend werden wir in einem Exkurs argumentieren, dass dies mit einer Veränderung der typischen Risikostruktur bei IT-Sicherheitslücken zusammenhängt, weshalb IT-Sicherheitsforschende hier regelmäßig in eine Angriffsrolle treten (Abschnitt 3). Sodann werden wir zeigen, inwiefern dies im Kontext der wissenschaftlichen Veröffentlichung von Forschungsergebnissen eine inhärente ethische Problematik offenbart (Abschnitt 4). Anschließend werden wir deskriptiv darlegen, inwiefern sich im Kontext der IT-Sicherheitsforschung bereits Anfänge einer eigenen Bereichsethik als Antwort auf diese Problemlagen herausgebildet haben, die den besonderen forschungsethischen Bedarf aber noch nicht adäquat adressieren (Abschnitt 5). Wenn die IT-Sicherheitsforschung aber ihre (normativ geprägte) Rolle in der Sicherheitsproduktion erfüllen soll, dann stellt – so unser Fazit – eine weitere Professionalisierung im Sinne einer Bereichsethik für IT-Sicherheit ein Desiderat für Forschung und Gesellschaft dar.

2 Der Sicherheitsbegriff der IT-Security

Dass die gesellschaftspolitische Relevanz des allgemeineren Begriffs „Sicherheit“ enorm gestiegen ist, ist kein Geheimnis. Wolfgang Bonß (2010, 36) spricht diesbezüglich auch von einer universalisierenden Vervielfältigung der Sicherheitsdiskurse seit den 1950er Jahren, welche alle Dimensionen des Sicherheitsbegriffs umfasst. Bis in die 1970er-Jahre hinein fanden sich

dennoch kaum Versuche, den Begriff „Sicherheit" einer tiefergehenden philosophischen Klärung zu unterziehen (Kaufmann 1973, 5). Für die geistes- und sozialwissenschaftliche Forschung hat sich diese Situation mittlerweile deutlich gewandelt. Hier ist „Sicherheit" zu einem zentralen Forschungsbegriff avanciert. Speziell seit den Anschlägen vom 11. September 2001 stehen (terroristische, aber auch allgemein kriminelle) Angriffe ebenso im Fokus ausgeprägter Forschungsdebatten wie die sich hierbei ergebenden Konflikte um die staatlichen Überwachungs- und Kontrollmaßnahmen auf der einen Seite und den Schutz von Freiheits- und Abwehrrechten auf der anderen (etwa Riescher 2010, 19–23; Koch 2014; Weydner-Volkmann 2018, 103–125). Mit Blick auf die Forschung zur Gestaltung technischer Innovationen spielt die Forderung nach sicherer Technik sogar noch länger eine zentrale Rolle. Was hierbei im Einzelfall aber konkret gefordert wird, ist keinesfalls immer eindeutig: Der Sicherheitsbegriff verweist vielmehr „immer auf ein komplexes Gefüge von Urteils- und Wertungszusammenhängen, die es im situativen Kontext […] zu explizieren gilt." (Weydner-Volkmann 2019, 332).

Dies gilt auch mit Blick auf „Sicherheitslücken" in IT-Systemen, deren Relevanz im Kontext der Technikfolgenforschung zuletzt betont und zu denen weitergehende Forschungsanstrengungen gefordert wurden (K. Weber et al. 2020). In den deutschsprachigen philosophischen und ethischen Debatten fehlen derzeit jedoch Publikationen, die sich eingehender mit „Sicherheitslücken" auseinandersetzen. Der Begriff wird vielmehr nur am Rande erwähnt oder im Rahmen von Beispielen angeführt. Ähnliches gilt für den englischsprachigen Kontext, wo zuletzt Diskussionen zu einer Cyberethik aufkamen (etwa Christen, Gordijn, und Loi 2020); auch hier fehlen aber reflektierende Ausführungen zu „*vulnerabilities*". Die wenigen Texte, die sich näher mit Sicherheitslücken auseinandersetzen, verbleiben bei technischen Definitionen, etwa Dunn Cavelty (2014, 704): „In computer security, a vulnerability is understood as the confluence of three elements […]: a system susceptibility or flaw, an attacker's knowledge of and access to the flaw, and an attacker's capability to exploit the flaw." Als Ausnahme können Joque und Haque (2020) gelten, die im Rahmen eines dekonstruktiven Ansatzes zu Cybersicherheit auch etwas näher auf Sicherheitslücken eingehen. Wir werden hierauf in Abschnitt 3 zurückkommen. Macnish und van der Ham (2020, 1) weisen zwar auf die eigenständige Relevanz forschungsethischer Fragen hin, eine weitergehende Diskussion fehlt aber auch hier.

Für eine erste Verortung von Sicherheitsfragen innerhalb situativer Handlungskontexte hat sich in den philosophischen und ethischen Debatten

zunächst ein Rückgriff auf die englischsprachige Differenzierung durchgesetzt, die auch hier hilfreich sein könnte: Sicherheitsaspekte lassen sich demzufolge danach unterscheiden, ob sie auf *safety*-Fragen (technische Betriebssicherheit, Ausfallsicherheit), *security*-Fragen (politisch-soziale Sicherheit, Sicherheit vor Angriffen) und *certainty*-Fragen (erkenntnisbezogene Gewissheit) bezogen sind (Bonß 2010, 35). Allerdings lassen sich „Sicherheitslücken" nicht gut in diese etablierte Differenzierung einfügen: Zwar geht es hier, ähnlich wie bei den *safety*-Fragen einerseits um technische Anforderungen für einen sicheren Betrieb, doch sind diese Anforderungen nicht im Sinne der klassischen Betriebssicherheit zu verstehen, also im Sinne eines ausfallsicheren Betriebs oder eines Schutzes vor Schäden durch Unfälle. Hier geht es um die Robustheit gegenüber *bewussten Angriffen* auf IT-Systeme. Anforderungen an die Betriebssicherheit (*safety*) eines IT-Systems beziehen sich hingegen auch in der Informatik auf idealerweise statistisch bestimmbare Verlässlichkeitsgrößen (*reliability*), die als Fähigkeit eines Systems verstanden werden, bis zu einem gewissen Zeitpunkt störungsfrei zu arbeiten (Eusgeld et al. 2008, 59). Im Gegensatz zu derartigen Fehlfunktionen lassen sich bewusste Angriffe ganz grundsätzlich nicht statistisch erfassen: Eine Angreiferin mag bewusst genau jene höchst selten auftretenden Fehlerbilder provozieren, die sie dann für ihre eigenen Zwecke verlässlich ausnutzen kann. In diesem Sinne zeigen sich „Sicherheitslücken" klar dem Bereich der *security*-Fragen zugehörig.

Andererseits lässt sich IT-Sicherheit auch nicht adäquat beschreiben, indem auf etablierte *security*-Ansätze aus der geistes- und gesellschaftswissenschaftlichen Sicherheitsforschung zurückgegriffen wird. Dies wird anhand der Zielvorstellung von IT-Security deutlich: Im Allgemeinen wird hierbei auf drei Aspekte rekurriert, nämlich auf (1) die Integrität, (2) die Vertraulichkeit und (3) die Verfügbarkeit der Datenverarbeitung (A. Weber et al. 2020, 30). Damit sind aber grundsätzlich andere Fragen adressiert als in der philosophischen und ethischen Forschung zu terroristischen und kriminellen Angriffen. Überspitzt formuliert geht es dort zumeist um die kritische Reflexion von (insbesondere staatlichen) Eingriffen in persönliche Freiheitsrechte im Rahmen von Überwachungs- oder Kontrollmaßnahmen, etwa in den Schutz der Privatheit oder das Diskriminierungsverbot (Zurawski 2015, 18–20, 37). Die Methoden der IT-Security zielen in aller Regel aber nicht auf Maßnahmen der Strafverfolgung oder der präventiven Abwehr eines Angriffs durch frühzeitige Erkennung von Verdachtsmomenten, sondern vielmehr auf die Robustheit von Systemen gegen Angriffe. Wie in Abschnitt 3

noch deutlich werden wird, hängt dies insbesondere auch mit der veränderten Struktur typischer Risiken bei Sicherheitslücken zusammen.

Dieser Fokus auf die Robustheit von IT-Systemen gegen Angriffe wird auch dadurch deutlich, dass Forschende sehr häufig in die Rolle der Angreifenden treten: „Ein Teil der IT-Sicherheitsforschung umfasst die Tests von Computerprogrammen auf Schwachstellen" (Wagner 2020, 111). Entsprechend gilt die *reproduzierbar demonstrierte Angreifbarkeit eines IT-Systems* gängiger Weise auch als *Ergebnis von Forschung*. Als solches muss es grundsätzlich auf eine Veröffentlichung ausgelegt sein, was besondere Probleme aufwirft, die wir in Abschnitt 4 noch genauer betrachten werden. An dieser Stelle ist zunächst von Bedeutung, dass es keineswegs trivial ist, Angriffe im Rahmen einer Sicherheits*forschung* von kriminellen Aktivitäten abzugrenzen. Entsprechend können Gesetze, die bestimmte Angriffe auf IT-Systeme unter Strafe stellen, auch Forschungsaktivitäten der IT-Sicherheit kriminalisieren. Hierauf wurde erst kürzlich in einem Whitepaper hingewiesen, in dem Forschende einen dringenden Reformbedarf formulieren (Balaban et al. 2021). Auch Wagner (2020, 111) schreibt in diesem Sinne: „Wenn IT-Sicherheitsforscherinnen und -forscher Produkte oder Systeme testen, führen sie in technischer Hinsicht exakt dieselben Angriffsmethoden durch wie Cyberkriminelle. Allerdings ist ihr Ziel und damit die Motivation eine völlig andere: Sie wollen die Allgemeinheit vor derartigen Schadensgefahren bewahren."

Als ein zentrales Unterscheidungsmerkmal lassen sich also insbesondere *normative* Maßstäbe ausmachen, die im Forschungsfeld der IT-Security situativ an den Umgang mit Sicherheitslücken gestellt werden. Insofern diese Maßstäbe für den Forschungskontext gelten, sind sie als *forschungsethische* Maßstäbe zu begreifen. In anderen Kontexten können sie gänzlich fehl am Platz sein, wie etwa die forschungsethische Forderung einer Meldung von Sicherheitslücken im Kontext nachrichtendienstlicher Informationsbeschaffung. Dieser normativ geprägte Umgang mit Sicherheitslücken zielt dabei auf das erwähnte gesellschaftspolitische Ziel, durch IT-Sicherheitsforschung IT-Systeme robuster gegen Angriffe zu machen (Balaban et al. 2021, 7; Wagner 2020, 111).

Bevor wir uns der Veröffentlichung von Sicherheitslücken im wissenschaftlichen Kontext zuwenden, soll als Exkurs zunächst noch genauer herausgearbeitet werden, warum klassische Sicherheitsmaßnahmen aus dem nicht-digitalen Bereich (etwa mit Blick auf die Kriminalitätsabwehr) in der IT-Sicherheit inadäquat erscheinen. Dabei werden wir argumentativ aufzei-

gen, dass aufgrund einer in verschiedenen Dimensionen veränderten Risiko-Struktur der Umgang mit Sicherheitslücken in IT-Systemen typischerweise einen anderen Umgang erforderlich macht.

3 Exkurs zur Neuartigkeit der Risikostruktur bei IT-Sicherheitslücken

Als Ausnahme der bislang weitgehend ausgebliebenen philosophischen Analyse von „Sicherheitslücken" darf Joque und Haques (2020, 104f.) gelten. Die Autoren betonen eine Kontinuität nicht-digitaler und digitaler Kontexte, die darin besteht, dass eine philosophisch hinterfragende Dekonstruktion von „Sicherheit" auch im IT-Kontext unbewusst vorausgesetzte Annahmen aufdecken kann – und somit immer auch auf fundamentale *Un*sicherheiten verweist. Ohne dem zu widersprechen soll im Folgenden ein anderer Weg eingeschlagen und stattdessen herausgestellt werden, inwiefern Cybercrime-Aktivitäten im Vergleich zu nicht-digitalen Kontexten typischerweise eine veränderte Risiko-Struktur implizieren, wenn hierbei Sicherheitslücken ausgenutzt werden. Dies soll verständlich machen, warum IT-Sicherheitsrisiken einen anderen Umgang erforderlich machen – wodurch dann aber neuartige ethische Problemstellungen entstehen.

Mit Blick auf den digitalen Kontext soll das Kompromittieren einer Alltagstechnik durch eine Angreiferin betrachtet werden: Durch das Ausnutzen einer Sicherheitslücke im E-Mail-Client erhält eine Angreiferin vollständigen Zugriff auf den Arbeitsrechner einer Nutzerin und installiert einen sogenannten Krypto-Trojaner, der die Nutzdaten auf dem Rechner verschlüsselt und diese so für die Nutzerin ohne einen Schlüssel unzugänglich macht. Zugleich weist der Trojaner die Nutzerin darauf hin, dass sie diesen Schlüssel nur gegen eine Bitcoin-Zahlung erhalten wird und leitet sie zu einem entsprechenden anonymen Zahlungsportal. Es handelt sich hierbei um einen technisch realisierten erpresserischen Angriff, der eingangs bereits unter dem Begriff „Ransomware" eingeführt wurde (BKA 2020, 22). Dieses Beispiel wird im Folgen entlang dreier Dimensionen (Räumlichkeit, Temporalität, Topologie) kontrastiv mit einem ähnlich strukturierten erpresserischen, aber nicht-digitalen Angriff verglichen, um Veränderungen der Risikostruktur herauszuarbeiten.

Zunächst (1) lässt sich kontrastiv mit Blick auf die *räumliche Dimension* feststellen, dass ein nicht-digitaler Angriff in aller Regel eine gewisse Nähe zwischen Angreiferin und Opfer impliziert. Nehmen wir an, eine Angreiferin

würde das Fahrrad einer Person stehlen,[3] um es anschließend gegen Geldzahlung wieder an die Besitzerin zurückzugeben, so setzt dies voraus, dass die Angreiferin tatsächlich physischen Zugriff auf das Fahrrad erhalten und eine Geldübergabe organisieren kann. Beide Male besteht durch die räumliche Anwesenheit ein wesentliches Risiko für die Angreiferin, entdeckt zu werden. Für die Fahrradbesitzerin hingegen ist das Risiko, tatsächlich Opfer eines solchen Angriffs zu werden, dadurch begrenzt, dass sie das Pech haben muss, in räumlicher Nähe zu einer Angreiferin zu sein, die dieses Risiko einzugehen gewillt ist. Angriffe auf Sicherheitslücken hingegen lassen sich global durchführen. Die räumliche Distanz zum Opfer ist dabei ein wesentlicher Faktor für die Angreiferin, das Risiko entdeckt zu werden gering zu halten; Cyberkriminelle agieren insbesondere global vernetzt (BKA 2020, 3).

Weiterhin (2) lässt sich kontrastiv mit Blick auf die *temporale Dimension* feststellen, dass es mit erheblichem zeitlichen Aufwand verbunden ist, ein Fahrrad zu stehlen und eine Geldübergabe zu organisieren. Angesichts des Risikos, hierbei entdeckt zu werden, muss dieser Aufwand also eine einigermaßen hohe Geldsumme versprechen. Entsprechend lässt sich für die Fahrradbesitzerin abschätzen, ob mit Blick auf das eigene Gefährt ein realistisches Risiko besteht, Opfer eines solchen Angriffs zu werden. Dabei ist zentral, dass Folgeangriffe nach dem gleichen Schema wieder den gleichen zeitlichen Aufwand nach sich ziehen würden. Zwar bedeutet auch das Auffinden und erstmalige Ausnutzen einer Sicherheitslücke für einen Ransomware-Angriff einen zeitlich hohen, vermutlich sogar deutlich höheren Aufwand. Allerdings lassen sich solche Angriffe in der Folge mit weniger Aufwand, gegebenenfalls sogar vollständig automatisiert massenhaft durchführen. Hier lohnt es sich, bei Privatpersonen in wirtschaftlich schwächeren Regionen auch kleinere Beträge zu erpressen, die sich dann durch häufiger geleistete Zahlungen aufsummieren (die Spannweite der Forderungen ist mit 10 bis 100.000.000 Euro enorm, BKA 2020, 23). Entsprechend ergibt für die Nutzerin eines IT-Systems eine zur Fahrradbesitzerin analoge Risiko-Abwägung keinen rechten Sinn, denn sie muss zu allen Zeiten annehmen, automatisiert

3 Es ist schwer, gute Parallelen zwischen nicht-digitalen und digitalen Angriffsszenarien zu konstruieren. Da der Diebstahl von Arbeitsdaten zumeist den Einbruch in Privatwohnungen implizieren würde, soll hier über das Beispiel des Fahrrads dahingehend eine Analogie geschaffen werden, dass ein IT-System über das Internet zwar grundsätzlich erreichbar ist, dabei aber Sicherungshürden überwunden werden müssen – so wie auch ein Fahrradschloss aufgebrochen werden muss.

durchgeführten, breiten Angriffswellen ausgesetzt zu sein – unabhängig vom konkreten Wert ihrer Daten. Freilich müssen große Unternehmen und KRITIS sich *zusätzlich* gegen gezielte Angriffe mit hohem Ressourceneinsatz wappnen (die dann auch mit höheren Lösegeldforderungen einhergehen), doch auch hier werden Tools in einer Art Wertschöpfungskette mehrfach genutzt (BKA 2020, 24).

Letztlich (3) lässt sich kontrastiv mit Blick auf die *topologische Dimension*[4] feststellen, dass bei nicht-digitalen Angriffen in aller Regel eine *direkte Beziehung* zwischen Angreiferin und Opfer angenommen werden kann. Aufgrund der vorauszusetzenden räumlichen Nähe und des vorausschauend zu rechtfertigenden zeitlichen Aufwands, können Strafermittlungsbehörden sich die Frage stellen, warum ausgerechnet diese Fahrradbesitzerin Opfer eines Erpressungsangriffs wurde – und wer umgekehrt überhaupt infrage käme, entsprechende Kenntnisse über die finanzielle Situation des Opfers zu besitzen. Im Unterschied dazu steht der Angreiferin im IT-Kontext, aufgrund der Möglichkeit zur Automatisierung und ihrer räumlichen Ungebundenheit, typischerweise offen, *beliebige* IT-Systeme anzugreifen, sofern die Systeme über das Internet *vernetzt* sind. Wie erwähnt erweist sich gerade bei einem massenhaften Angriff die Frage danach, warum diese, aber nicht jene Person Opfer wurde, als nicht zielführend. Entsprechend ist es hier nicht nur denkbar, sondern bei automatisierten Angriffen sogar typisch, dass die Angreiferin und die Nutzerin des IT-Systems beiderseitig in keinem direkten, sondern in einem vollständig anonymen Verhältnis stehen; die Angriffsbeziehung hat einen rein zufälligen Charakter.

Zusammengenommen entfalten diese drei Dimensionen eine „skalierende" Dynamik: Während wiederholte nicht-digitale Angriffe im Allgemeinen eine räumliche Nähe, eine gewisse direkte Beziehung und einen immer wieder neu entstehenden zeitlichen Aufwand erfordern, können Sicherheitslücken in IT-Systemen typischerweise global, anonym-vernetzt und mit ständig sinkendem Aufwand ausgenutzt werden. Im Gegensatz zu anderen Bereichen der Sicherheitsproduktion in modernen Gesellschaften, wo bei Angriffen zumeist die Angreifenden im Fokus der Sicherheitsproduktion stehen (etwa mit Blick auf die Prävention von Terrorangriffen oder die Repression von Kriminalität), führt dies in der IT-Sicherheit zu einem Fokus auf die *technische Robustheit der IT-Systeme* vor quasi persistent angenom-

4 Wir danken Estrid Sørensen für die Idee, eine topologische Dimension zu ergänzen.

menen Angriffen. Kriminelle Angriffsversuche werden für vernetzte Systeme als gegebene Kontextbedingung aufgefasst, denen nur zum Teil mit Maßnahmen der Kriminalitätsbekämpfung begegnet wird, insbesondere aber mit einer Erhöhung der technischen Hürden und der kontinuierlichen Schließung von bekannt gewordenen Sicherheitslücken, die diese Hürden zu umgehen erlauben.

Für die Forschenden der IT-Sicherheit bedeutet dies aber, dass sie häufig in die Rolle der Angreiferinnen treten, um Lücken aufzudecken. Ihre gesellschaftliche Rolle übernehmen die Forschenden, indem sie die Angreifbarkeit von IT-Systemen replizierbar demonstrieren, um so mittelbar zu sichereren Systemen beizutragen. Im Folgenden soll nun betrachtet werden, welche ethischen Konflikte sich mit Blick auf die wissenschaftliche Veröffentlichung von Sicherheitslücken ergeben.

4 Das Dilemma der Veröffentlichung von Sicherheitslücken

Weil die akademische IT-Sicherheitsforschung Teil des wissenschaftlichen Diskurses ist, ist die Publikation von Forschungsergebnissen ein wesentlicher Bestandteil des Arbeitsprozesses wie auch der Verfolgung wissenschaftlicher Karrieren – und daher ist sie auch grundsätzlich von der Forschungsfreiheit gedeckt. Weil hier unter anderem Sicherheitslücken als Forschungsergebnis gelten, stellt deren Veröffentlichung wegen eines möglichen Missbrauchs durch Dritte *per se* ein Risiko dar. Die Veröffentlichung von Informationen zu Sicherheitslücken wirft somit regelmäßig Dual-Use-Probleme auf. Die Entscheidung, ob, wann und wie eine gefundene Sicherheitslücke der (Fach-)Öffentlichkeit zugänglich gemacht werden sollte, ist von besonderer ethischer Relevanz: „[D]urchgeführte Forschung [muss] mit den in einer Gemeinschaft geltenden Gesetzen und anerkannten ethischen Normen vereinbar sein“ (Fenner 2010, 183), was Forschende in die Verantwortung nimmt, zu beurteilen, inwieweit die Veröffentlichung einer Lücke Risiken für die Gesellschaft aufwirft.

Diese Beurteilung der Dual-Use-Problematik trägt Züge einer Dilemma-Situation. So kann es in bestimmten Fällen geboten sein, relevante Akteurinnen oder die (Fach-)Öffentlichkeit darüber zu informieren, dass Sicherheitslücken bestehen. Andererseits kann es zugleich geboten sein, die Lücke unter Verschluss zu halten, bis sie über ein Update geschlossen wurde. So bleibt abzuwägen, ob jeweils die Zurückhaltung oder die Verbreitung von Informationen über die Lücke größere Risiken aufwirft. Im Dezember

2021 sah es etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI) als geboten an, die Öffentlichkeit vor den Risiken der Schwachstelle „Log4Shell“ zu warnen (BSI 2021b). Zwar gab es damals noch nicht für alle Systeme Updates, allerdings wurde die Lücke zu diesem Zeitpunkt bereits für kriminelle Angriffe ausgenutzt, weshalb die zusätzlichen Risiken als vertretbar galten.

Zu den beschriebenen Abwägungsproblemen zwischen Interessen von Forschenden und Gesellschaft treten zudem Interessenkonflikte mit Dritten: Bei Lücken in kommerziellen Systemen haben Unternehmen zwar ein Interesse daran, Kenntnis über die damit zusammenhängende Gefährdung zu erhalten, um die Lücke zu schließen. Andererseits werden Lücken und Angriffe oft auch bewusst unter Verschluss gehalten, um das Vertrauen der Kundschaft nicht zu schmälern (vgl. Dreißigacker et al. 2020, 150f.). Wie viele Lücken und Angriffe *nicht* öffentlich bekannt werden, ist schwer zu erheben. „Insbesondere das als sehr groß vermutete Dunkelfeld und eine als gering wahrgenommene Anzeigenbereitschaft erschweren die Einschätzung des Phänomens“ (Dreißigacker et al. 2020, 47).

Nach welchen Kriterien können Forschende Interessen und Risiken der Bekanntmachung einer Sicherheitslücke bewerten? Und wer trägt letztlich welche Verantwortung für die Konsequenzen der Entscheidung? Eine generelle Antwort auf diese Fragen kann es nicht geben. Für Forschende in der IT-Sicherheit ergibt sich hieraus ein Bedarf an forschungsethischer Orientierung, etwa im Sinne von Leitlinien, anhand derer die Entscheidung für oder wider eine Publikation begründet werden kann. Dieser Bedarf ist im IT-Bereich nicht unbekannt. In der Praxis haben sich unter anderem ethische Verhaltenskodizes und Best Practices entwickelt, die solche Leitlinien bereitstellen. Wir vertreten die These, dass sich hier (in Anerkennung der gesellschaftspolitischen Relevanz) als Antwort auf den forschungsethischen Bedarf erste Ansätze einer Bereichsethik herausbilden. Im Folgenden werden wir diese Ansätze deskriptiv darlegen und jeweils hinsichtlich ihrer Orientierungsleistung im Umgang mit Sicherheitslücken befragen.

5 Die Behandlung der Sicherheitslücken in der IT-Sicherheit

5.1 Ethische Verhaltenskodizes

Ethische Kodizes können als „systematische Sammlungen von Regeln und Normen [verstanden werden], die für eine Berufsgruppe oder eine Organisation gelten" (Maring 2013, 410). Im IT-Bereich gibt es diverse ethische Kodizes, die sich in ihrer Grundstruktur ähneln: Sie sind prinzipienethisch aufgebaut und weisen relativ allgemein gehalten auf die Verpflichtung der angesprochenen Zielgruppe hin, mit den eigenen Handlungen das Wohl der Gesellschaft beziehungsweise der Individuen zu fördern und Schädigungen zu unterlassen. Sie basieren zudem auf Selbstverpflichtung und besitzen somit keine direkte rechtliche Bindung. Ein solcher, für die IT-Sicherheit zentraler Kodex ist der Menlo-Report (Kenneally und Dittrich, 2012), auf den sich auch das in der Forschung zentrale Institute of Electrical and Electronics Engineers (IEEE), wie auch Forschungsarbeiten zur Ethik in der IT-Sicherheit beziehen (Macnish und van der Ham 2020; Narayaran und Zevenberg 2015). Im Folgenden werden wir uns bei den Ausführungen stellvertretend auf diesen Kodex beziehen.

Die Zielgruppe des Menlo-Reports umfasst verschiedene Berufsgruppen; Forschende werden aber explizit erwähnt: „This report offers guidance primarily for ICT [information and communication technologies] researchers (including academic, corporate, and independent researchers), professional societies, publication review committees, and funding agencies" (Kenneally und Dittrich 2012, 3). Dabei stützt sich der Kodex auf Prinzipien, die als Leitlinien bei ethischen Schwierigkeiten im Kontext der IT genutzt werden sollen. Explizit werden hierbei Respekt vor Personen (*respect for persons*), Wohltätigkeit (*beneficience*), Gerechtigkeit (*justice*) sowie Respekt vor dem Gesetz und dem öffentlichen Interesse (*respect for law and public interest*) genannt (Kenneally und Dittrich 2012, 5f.). Die Prinzipien schließen unter anderem die Gewährleistung von Sicherheit, Privatheit und Gesundheit der Individuen sowie der Gerechtigkeit, Transparenz und Ehrlichkeit der durchgeführten Forschung ein (Kenneally und Dittrich 2012, 7f.).

In Hinblick auf den Umgang mit und die Veröffentlichung von Sicherheitslücken schlägt der Kodex wenig spezifisch vor, eine Risikoabwägung vorzunehmen:

> „From an equity standpoint, open public disclosure of system vulnerabilities demands that researchers consider how the burdens and

> benefits of publicizing newly discovered vulnerability balance out. The burdens might be borne by the developers, yet actually might benefit malicious actors more in the short-term than developers or users of those systems. The calculation of benefits is actually a function of time, where malicious actors may act faster at exploiting vulnerability information than benevolent actors can act in mitigating the vulnerabilities." (Kenneally und Dittrich 2012, 11)

Weitergehende Orientierungshinweise zur Abwägung oder zu Umständen, die für oder gegen eine Veröffentlichung sprechen, fehlen jedoch. Daher bietet der Kodex nur eine unzureichende Hilfestellung, um Dilemmasituationen adäquat zu begegnen: Der Menlo-Report hilft weder dabei, in konkreten Konfliktsituationen zu entscheiden, noch die Entscheidung für oder gegen eine Veröffentlichung gut zu begründen (Macnish und van der Ham 2020, 8).

Prinzipienethische Kodizes stellen ferner nur dann eine hilfreiche Orientierung dar, wenn die Adressatinnen für die Prinzipien sensibilisiert sind und Kompetenzen aufgebaut haben, das hohe Abstraktionsniveau auf konkrete Einzelfallentscheidungen zu beziehen. Dies bezieht sich sowohl auf die Forschenden selbst wie auch auf Gutachterinnen, etwa bei Peer-Reviews (Abschnitt 5.2). Verpflichtende Lehrveranstaltungen zur Ethik in der IT-Sicherheit gibt es an Universitäten im deutschsprachigen Raum jedoch typischerweise nicht, wenn sich auch vereinzelt Hochschulen finden lassen, die mit entsprechenden fakultativen Angeboten werben (etwa H-BRS; BHT Berlin).

Dass eine Kompetenzvermittlung zu prinzipienethischen Kodizes eine echte Lösungsperspektive darstellt, darf mit Blick auf die unbefriedigenden Erfahrungen der angewandten Ethik ohnehin als fraglich gelten: „Dies zeigt sich auch daran, dass sogar diejenigen Ethiker, die eine Moralkonzeption teilen, zu unterschiedlichen Einzelfallurteilen gelangen. Außerdem besteht die Gefahr, Probleme allein durch die Brille der abstrakten Theorie zu betrachten und sie dadurch zu schnell auf bestimmte Aspekte zu reduzieren" (Zichy 2008, 96–97).

5.2 Konferenzen und ethische Komitees

Wie sich in Gesprächen mit IT-Forschenden vielfach bestätigt hat, sind Konferenzbände die zentralen Veröffentlichungsmedien der Disziplin; reine Zeitschriftenpublikationen fallen weniger ins Gewicht. Konferenzen können somit als einflussreiche Kontrollinstanzen für die akademische Disziplin (aber auch für Forschungsaktivitäten der IT-Branche) gelten. Bei der

Beurteilung der Eignung von Konferenzbeiträgen geht es in erster Linie um die fachlich-technische Qualität, jedoch lässt sich aktuell vermehrt eine Auseinandersetzung mit ethischen Fragestellungen beobachten (vgl. Usenix 2021; NDSS 2022). So wurde 2021 eine Einreichung für eine IEEE-Konferenz auch in der Fachpresse kontrovers diskutiert: Eine Forschungsgruppe hatte die Nutzung von Open-Source-Entwicklungsprozessen dokumentiert, über die sie Schwachstellen in den Code des Betriebssystems Linux einbringen konnten („Hypocrite Commits Paper"; vgl. Salter 2021; Loschwitz 2021; Vaughan-Nichols 2021). Zwar wurden im Peer-Review ethische Bedenken hinsichtlich der Täuschung der Linux-Entwicklerinnen und der erzeugten Risiken durch das Einbringen von Schwachstellen geäußert, diesen wurde jedoch nicht weiter nachgegangen und die Einreichung angenommen (Holz und Opera 2021, nach öffentlicher Kritik zogen die Autorinnen ihre Einreichung letztlich zurück). Als Antwort auf diesen Fall wurde beschlossen, im Rahmen der wichtigen IEEE-Konferenzen verstärkt forschungsethische Aspekte in der IT-Sicherheit zu berücksichtigen. Ein Ethik-Komitee soll anhand vereinbarter Leitlinien künftig Fälle überprüfen, bei denen im Peer-Review-Verfahren ethische Bedenken angemeldet wurden: „New to Oakland 2022 is a research ethics committee (REC) that will check papers flagged by reviewers as potentially including ethically fraught research" (IEEE 2022).

Das Ethik-Komitee orientiert sich dabei am Menlo-Report (IEEE 2022), wodurch sich die oben skizzierten Probleme auf die Kontrollfunktion von Fachkonferenzen übertragen. Hinsichtlich des Umgangs mit Sicherheitslücken findet sich jedoch eine knappe Ergänzung:

> „Where research identifies a vulnerability (e.g., software vulnerabilities in a given program, design weaknesses in a hardware system, or any other kind of vulnerability in deployed systems), we expect that researchers act in a way that avoids gratuitous harm to affected users and, where possible, affirmatively protects those users." (IEEE 2022)

In ähnlicher Weise allgemein gehalten wie der Menlo-Report, bietet jedoch erst der Hinweis eine weitergehende Orientierung, dass es in beinahe allen Fällen im Sinne der Nutzerinnen sei, gefundene Sicherheitslücken an die Herstellenden zu melden und ihnen 45 bis 90 Tage bis zur Veröffentlichung der Lücke einzuräumen (IEEE 2022).

Dieses Vorgehen deckt sich mit dem derzeitigen Standard-Verfahren beim Fund einer Sicherheitslücke (Responsible Disclosure). Wir werden dieses Verfahren im nächsten Abschnitt (5.3) betrachten. Zuvor möchten

wir aber betonen, dass die Einrichtung eines Ethik-Komitees auf einer der einflussreichsten IT-Sicherheits-Konferenzen den grundsätzlichen Bedarf an Orientierung zu ethischen Fragen in der IT-Sicherheitsforschung unterstreicht. Ein ethisch reflektierter Umgang mit Sicherheitslücken ist somit zwar auch ein wichtiges *gesellschaftliches* Anliegen, aber keines, das bloß „von außen" an die Forschungsgemeinschaft herangetragen würde, sondern eines, das aus der Forschungsgemeinschaft selbst heraus formuliert wird.

5.3 Verfahren zur Bekanntmachung einer Schwachstelle

Neben Kodizes und forschungsethischen Begutachtungskriterien wurde in der IT-Sicherheit auch eine Verfahrenslösung entwickelt, um mit ethischen Dilemmata umzugehen. „Responsible Disclosure" (auch „Coordinated Vulnerability Disclosure", Balaban 2021, 27) beschreibt die Bekanntmachung einer Schwachstelle gegenüber der Öffentlichkeit nach Ablauf einer Frist, in der betreffende Unternehmen oder Verantwortliche zunächst informiert werden und ihnen Zeit eingeräumt wird, diese zu schließen. Dieses Verfahren ist von zwei möglichen Alternativen zu unterscheiden: „Non Disclosure" beschreibt die komplette Geheimhaltung der Schwachstelle; „Full Disclosure" beschreibt hingegen eine nach dem Fund sofortige Veröffentlichung der Schwachstelle (vgl. Arora und Telang 2005, 20). Insbesondere große Unternehmen haben sich fast ausnahmslos zum Responsible-Disclosure-Verfahren bekannt. So sind auf den Webseiten vieler Unternehmen Ansprechpartnerinnen und detaillierte Vorgaben für die Meldung von Sicherheitslücken zu finden (etwa Google o. J.; Microsoft o. J.; SAP o. J.).

Als Verfahrenslösung bietet Responsible Disclosure konkrete Handlungsanweisungen und überwindet damit die erwähnten Probleme prinzipienethischer Kodizes. Es lässt sich in unkritischen Situationen zudem gut anwenden, nämlich immer dann, wenn das Verfahren erlaubt, den Interessen aller Akteurinnen und gegebenenfalls auch aller Betroffenen zu entsprechen. Bei sog. Open-Source-Projekten können Forschende Verbesserungsvorschläge sogar selbst einbringen. In schwierigen Konstellationen gerät das Verfahren jedoch schnell an seine Grenzen. So kann die gängige Praxis der Nutzung bestehender Softwarekomponenten für neue Anwendungen zu komplexen Abhängigkeiten führen, die unklar machen, welche Organisationen konkret zu informieren sind (vgl. auch Herrmann und Pridöhl 2020, 34). Auch sind die organisatorischen Voraussetzungen längst nicht bei allen Unternehmen und verantwortlichen Betreiberinnen von IT-Systemen etabliert. Es kommt immer wieder vor, dass keine Ansprechpartnerin für das

Verfahren bereitsteht, keine detaillierte „Vulnerability Disclosure Policy" zur Vorgehensweise kommuniziert wird oder Open-Source-Komponenten nur noch unzureichend gepflegt werden. Den verbreiteten Mangel an strukturellen Voraussetzungen für ein Responsible-Disclosure-Verfahren kritisiert auch das BSI (2021a, 71) im aktuellen Lagebericht. Haben sich Unternehmen beziehungsweise die verantwortlichen Betreiberinnen des betreffenden Systems aber nicht schon im Vorhinein darauf eingestellt, dass Sicherheitslücken gefunden werden können, führt dies immer wieder dazu, dass diese sich nicht auf das Verfahren einlassen und stattdessen auf die Meldung mit einer Strafanzeige reagieren – wie erst kürzlich im Fall der Meldung einer Lücke in der CDU-Connect App durch Lilith Wittmann (Balaban et al. 2021, 11; Wittmann 2021).

Das Verfahren ist zudem immer dann nicht sinnvoll anwendbar, wenn sich die gefundene Schwachstelle nicht beheben lässt und somit feststeht, dass die Lücke auch nach der Veröffentlichung Bestand haben wird. Exemplarisch kann hier die Sicherheitslücke „Spectre" genannt werden, die bei Intel-Prozessoren seit Jahren zu immer neuen Problemen führt, über die in der Fachpresse wie auch in der wissenschaftlichen Fachliteratur berichtet wird (vgl. Haas 2020; Goodin 2021; Mantel 2022). Derartige Sicherheitslücken beruhen auf ganz grundsätzlichen Schwierigkeiten in der Rechnerarchitektur; die Einräumung des üblichen Zeitkorridors von 45 bis 90 Tagen reicht hier schlicht nicht aus, um den durch die Veröffentlichung entstehenden Risiken zu begegnen. Entsprechend wirft der Umgang mit Forschungsergebnissen, die keine Lösung für das aufgeworfene Sicherheitsproblem beinhalten (können), komplexe ethische Fragen auf, die über diese Verfahrenslösung nur unzureichend beantwortet werden.

In anderen Fällen bietet Responsible Disclosure aber einen eleganten Lösungsweg, indem konfliktbehafteten Entscheidungen mit einem kooperativen Verfahren begegnet wird. Wann und wie eine Sicherheitslücke veröffentlicht werden darf, ergibt sich aus den Handlungsanweisungen der betreffenden Unternehmen oder System-Verantwortlichen. Hierin wird allerdings auch die dominante Rolle der Unternehmen deutlich: Sie *agieren* im Verfahren durch Vorgaben, die Forschenden *reagieren* darauf. Dies hängt auch mit der in Abschnitt 3 herausgearbeiteten veränderten Risikostruktur bzw. der darauf antwortenden Rolle der Forschenden zusammen: Dadurch, dass die Forschenden in eine bisweilen rechtlich unklare Angriffs-Rolle treten, um die Lücke überhaupt entdecken zu können, sind sie in gewisser Weise auch angreifbar. Weil Responsible-Disclosure-Verfahren – wie schon die Verhal-

tenskodizes – keinen rechtlich bindenden Standard darstellen, können sich Forschende im Streitfall nicht auf allgemeingültige Verfahrensabläufe berufen. „Eine anhaltende rechtliche Unsicherheit in der praktischen Durchführung von CVD [Coordinated Vulnerability Disclosure, synonym für Responsible Disclosure] führt zu einem Abschreckungseffekt [bei der Meldung von Sicherheitslücken], der die Gemeinschaft der Forschenden betrifft" (Balaban et al. 2021, 61). Diese Tatsache spiegelt abermals die bisher noch faktisch inadäquate normative Klärung des Umgangs von Forschung und Gesellschaft mit Sicherheitslücken.

5.4 Institutionelle Meldung von Sicherheitslücken

Unabhängig von Verfahrenslösungen zur Meldung der Lücke bei Unternehmen und Verantwortlichen (und von der erwarteten Schließung durch Updates) steht es Forschenden frei, einen Eintrag in eine Liste von identifizierten Sicherheitslücken zu beantragen. Entsprechende Listen beziehungsweise Datenbanken systematisieren und beschreiben Sicherheitslücken anhand bestimmter Kriterien und weisen jeder Lücke eine Erkennungsnummer zu. Das Verzeichnis „Common Vulnerabilities and Exposures" (CVE) ist eine der verbreitetsten Datenbanken, die auch mittels Stichwortkatalog durchsucht werden kann (CVE o.J.). Für Forschende (wie auch andere Akteurinnen) liegen die Vorteile einer systematisierten Auflistung von Lücken auf der Hand: Sie ermöglicht einen Überblick über gegebenenfalls bereits gefundene Lücken im Zielsystem oder über ähnlich geartete Lücken. Zudem werden einige grundlegende Informationen über die Lücke und ihre Umgebung zur Verfügung gestellt, wenngleich diese nicht umfangreich sind. Der Eintrag einer Lücke in die Liste bedeutet zunächst nur, dass die Lücke identifiziert wurde, sagt aber beispielsweise nichts darüber aus, welches Risiko von der Lücke ausgeht.

Hierzu dienen Industriestandards wie das Common Vulnerability Scoring System (CVSS), mittels derer sich der Schweregrad von Sicherheitslücken erfassen lässt (First o. J., 1). CVSS erfasst quantitativ das Gefahrenpotenzial einer Sicherheitslücke anhand verschiedener Charakteristika, die auf einer Skala bewertet und in eine qualitative Bewertung übersetzt werden (none, low, medium, high, critical; First o. J., 16). In diesem System werden verschiedene Aspekte der Lücke abgefragt, die insbesondere technischer Natur sind, jedoch auch Informationen über den Kontext, in dem die Sicherheitslücke zu bewerten ist, beinhalten. Hierzu zählt etwa die Information, ob die Schwachstelle per Update schließbar ist, ob eine Schwachstelle tat-

sächlich ausnutzbar ist und welches Potenzial die Lücke hat, wirtschaftlichen Verlust zu verursachen (First o. J., 14).

Die Meldung, Systematisierung und Klassifizierung von Lücken ist Teil eines institutionalisierten Umgangs mit Lücken, in den auch nationale und europäische Behörden eingebunden sind. So erstellt etwa das deutsche BSI auch auf dieser Basis regelmäßige Lageberichte, betreibt eine eigene Meldestelle für Lücken und Angriffe und warnt vor akuten Bedrohungslagen. Für KRITIS ergeben sich daraus auch gesetzliche Pflichten, eigene Sicherheitslücken zu melden und Schutzmaßnahmen nach dem State of the Art zu implementieren (Schlehan 2020, 210). Für Forschende ergibt sich daraus zwar keine rechtliche, eventuell aber eine ethische Pflicht, über die Meldung von Lücken eine gesellschaftspolitische Aufgabe in der Sicherheitsproduktion zu erfüllen – ohne dass dies aber eine weitergehende Orientierung hinsichtlich des Veröffentlichungsdilemmas erlauben würde.

Sowohl für einen Überblick über die Bandbreite von bereits identifizierten Lücken wie auch für die Beschreibung einer konkreten Lücke und ihres Kontextes können die Melde-Standards diesbezüglich einen Ansatzpunkt für weitere, normativ ausgerichtete Überlegungen liefern. Allerdings sind zumindest CVE und CVSS aus *technisch-industriellen* und *unternehmerischen* Bedarfen heraus entstanden, was in den Spezifizierungen zu den Kriterien (etwa das Potential für wirtschaftlichen Schaden) auch ein Stück weit deutlich wird. Für eine ethische Bewertung müssten weitere Aspekte zu Risiken für einzelne Nutzerinnen oder gesamtgesellschaftliche Gefahren stärker berücksichtigt werden.

5.5 Inadäquate Abdeckung des forschungsethischen Bedarfs

Aus den obigen Ausführungen wurde deutlich, dass es im Feld der IT-Sicherheit auf verschiedenen Ebenen Normen im Umgang mit Sicherheitslücken gibt. Diese zeigen, dass auch aus der Forschungsgemeinschaft heraus ein Bedarf an ethischer Orientierung besteht. Bei der Betrachtung wurde auch deutlich, dass diese Normen hierfür zwar erste, wichtige Ansätze bieten, sie den Bedarf an konkreter normativer Orientierung im Umgang mit Sicherheitslücken im wissenschaftlichen Kontext jedoch noch nicht adäquat abdecken. So stellen prinzipienethische Kodizes eine grundlegende normative Ausrichtung bereit, die mit Blick auf eine anwendungsbezogene Orientierung aber in ihrer aktuellen Form zu abstrakt bleiben. Ethische Komitees auf den Konferenzen des Feldes können als Kontrollinstanz für die Einhaltung der formulierten ethischen Prinzipien in der Forschungspraxis

verstanden werden, jedoch befinden sich diese noch im Entstehungsprozess. Die besprochene Neugründung eines Ethik-Komitees im Rahmen der IEEE orientiert sich zudem am einschlägigen, aber prinzipienethisch ausgerichteten Kodex des Menlo-Reports. Entsprechend ist zu erwarten, dass in der Arbeit des Komitees der Mangel an anwendungsbezogener Handlungsorientierung für die wissenschaftliche Veröffentlichung von Sicherheitslücken im Forschungsfeld ein Problem darstellen wird. Konkrete Vorgaben, wie Forschende im Fall des Funds einer Lücke vorgehen sollen, sind im Rahmen des Responsible-Disclosure-Verfahrens gegeben, aber dieses ist gerade in konfliktbehafteten Fällen oft unzureichend. Zwar sind nicht zuletzt die Verwaltung identifizierter Lücken mittels standardisierter Datenbanken sowie die behördliche Arbeit technisch sinnvolle und gesellschaftspolitisch wichtige Instrumente im Umgang mit Lücken. Sie lassen aus Sicht der Forschenden derzeit aber (noch) Aspekte außer Acht, die für eine ethische Orientierungsleistung notwendig wären.

Es ist augenscheinlich, dass die Angewandte Ethik einen nützlichen Beitrag zu den aktuellen Entwicklungen innerhalb der IT-Sicherheit leisten kann. Auch kann sie im Sinne der Gewinnung eines neuen Forschungsfeldes profitieren, in dem neuartige ethische Problematiken der Digitalisierung manifest werden. In dieser Hinsicht ist es misslich, dass die philosophische Ethik nicht bereits tiefer in die aktuellen Formierungsprozesse der IT-Sicherheit involviert ist. Ein möglicher Zugang eröffnet sich beispielsweise über die Klärung des Verantwortungsbegriffs im Rahmen des zentralen Verfahrens des *Responsible* Disclosures sowie der konkret in den bestehenden Verfahren etablierten oder normativ erwarteten Verantwortlichkeiten im Umgang mit Sicherheitslücken. Es läge nahe, hier insbesondere an die verantwortungsethischen Debatten in der Technikethik anzuschließen. Alternativ läge mit Blick auf den für die Abwägungsproblematik zentralen Risikobegriff auch ein Zugang über die Risikoethik nahe. Auch die Forschung zu Dual-Use-Problemen könnte sinnvolle Impulse setzen. Eine *Bereichsethik für IT-Sicherheit* könnte sich der besonderen Problemlagen und Dilemmata dezidiert annehmen und dabei deren Vielschichtigkeit ggf. auch durch Kombination von Ansätzen berücksichtigen. Wenn wir hier für die Formierung einer neuen Bereichsethik plädieren, dann also nicht in *Abgrenzung* zu anderen Teilbereichen der Angewandten Ethik, sondern im Sinne einer *Öffnung und Professionalisierung* der aktuell noch fast ausschließlich innerfachlichen Diskussionen der IT-Sicherheit für die Expertise der Angewandten Ethik in ihrer Breite.

6 Fazit

Die Sicherheit von IT-Systemen ist aufgrund der Eingriffstiefe der Systeme in die Lebenswelt der Menschen mittlerweile eine gesamtgesellschaftliche Angelegenheit, die jedoch, wie wir gezeigt haben, nicht auf die gleiche Weise wie in nicht-digitalen Kontexten gewährleistet werden kann. So obliegt die Gewährleistung von IT-Sicherheit nicht alleine den Strafverfolgungsbehörden; der IT-Sicherheitsforschung wird hier eine zentrale Rolle zugeschrieben. Wir haben gezeigt, dass hierdurch auch ein besonderer forschungsethischer Bedarf mit Blick auf das akademische Feld der IT-Sicherheit entsteht, der bislang nur unzureichend adressiert wird.

Etablierte Ansätze aus der insbesondere auf Überwachungs- und Kontrollpraktiken zugeschnitten Sicherheitsforschung bieten sich weniger an, um dieser Herausforderung zu begegnen. Ein Grund dafür ist, dass sich digitale und nicht-digitale Sicherheitsprobleme typischerweise in mehreren Dimensionen unterscheiden. In einem Exkurs wurde gezeigt, dass wiederholte nicht-digitale Angriffe eine räumliche Nähe, eine gewisse direkte Beziehung und einen immer wieder neu entstehenden zeitlichen Aufwand erfordern. Digitale Angriffe auf IT-Systeme sind hingegen global, anonym-vernetzt und mit ständig sinkendem Aufwand durchführbar. Die sich hieraus ergebende skalierende Dynamik führt dazu, den Fokus der IT-Sicherheit auf die Robustheit der IT-Systeme vor quasi permanent angenommenen Angriffen zu legen. Für Forschende bedeutet dies, der gesellschaftlich zugeschriebenen Aufgabe in der Produktion von IT-Sicherheit (auch) dadurch gerecht zu werden, dass sie in eine Angriffs-Rolle schlüpfen.

Die gewissermaßen paradoxale Praxis, gesellschaftliche Risiken zu verringern, indem (unter explizit anderen normativen Vorzeichen) öffentlich demonstriert wird, wie IT-Systeme attackiert werden können, führt gerade mit Blick auf die Veröffentlichung von Sicherheitslücken zu forschungsethisch problematischen Situationen: Die Publikation ist als wesentlicher Bestandteil der Forschungsarbeit zu verstehen, erhöht aber auch das Risiko, dass die Lücke missbraucht wird. So erhöhen Forschende durch einen (notwendigen) Schritt ihres Arbeitsprozesses die Gefährdungslage von IT-Systemen. Zugleich forschen sie normativ auch im Sinne einer Stärkung gesamtgesellschaftlicher Sicherheit an der Robustheit von IT-Systemen. Dadurch entsteht eine dilemmatische Konstellation, anhand derer ein konkreter forschungsethischer Bedarf in der IT-Sicherheit deutlich wird.

Ansätze, die auf diesen Bedarf antworten, sind bereits vorzufinden. Ethische Kodizes und ihre Anwendung auf wichtigen Konferenzen bilden

einen allgemeinen prinzipienethischen Rahmen, der jedoch in der aktuellen Form keine *anwendungsbezogenen* Entscheidungshilfen mit Blick auf den Umgang mit Sicherheitslücken bietet. Das Standard-Meldeverfahren „Responsible Disclosure" bietet dabei zwar klare Vorgaben, erweist sich jedoch unter anderem bei Interessenskonflikten als inadäquat. Auch bestehende institutionalisierte Strukturen werden dem forschungsethischen Orientierungsbedarf derzeit nicht gerecht. Eine Anpassung der Kodizes und Verfahren an die wissenschaftlichen Bedürfnisse und Sonderfälle könnte helfen, die bestehenden Grundlagen auszubauen und die Bedarfe besser zu adressieren. Damit die IT-Sicherheitsforschung ihrer gesellschaftspolitischen Rolle in der Sicherheitsproduktion gerecht werden kann, sehen wir es als Desiderat an, den Schritt hin zu einer Professionalisierung des Feldes im Sinne einer Bereichsethik für IT-Sicherheitsforschung zu gehen und sich so auch stärker für die Expertise der Angewandten Ethik zu öffnen. Es ist anzunehmen, dass die Angewandte Ethik hier wertvolle Beiträge leisten kann – einerseits um die Forschungsgemeinschaft dabei zu unterstützen, adäquatere Orientierungsangebote zu entwickeln, andererseits aber auch, um deren gesellschaftspolitische Rolle in der Sicherheitsproduktion zu reflektieren.

Literatur

Arora, Ashish und Rahul Telang. 2005. „Economics of Software Vulnerability Disclosure." *IEEE Security and Privacy Magazine* 3 (1), 20–25. https://doi.org/10.1109/MSP.2005.12.

Balaban, Silvia, Franziska Boehm, Dominik Brodowski, Roman Dickmann, Fabian Franzen, Niklas Goerke, Sebastian Golla, u. a. 2021. *Whitepaper zur Rechtslage der IT-Sicherheitsforschung. Reformbedarf aus Sicht der angewandten Sicherheitsforschung*. www.sec4research.de. https://sec4research.de/assets/Whitepaper.pdf.

BHT Berlin. o.J. „IT-Sicherheit Online (B.Sc.): BHT Berlin." Abgerufen 17. Mai 2022, https://www.bht-berlin.de/b-its-o.

BKA. 2020. *Cybercrime Bundeslagebild 2020*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf.

BMBF. 2020. „Digital, sicher und souverän in die Zukunft." Abgerufen 17. Mai 2022, https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/it-sicherheit/it-sicherheit_node.html.

BSI. 2021a. *Die Lage der IT-Sicherheit in Deutschland 2021*. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

———. 2021b. "Update: Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage." Bundesamt für Sicherheit in der Informationstechnik, 16 Dezember 2021. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html;jsessionid=31C02769B9E3132B8C098B18EDE52188.internet471?nn=520690.

Bonß, Wolfgang. 2010. „(Un-)Sicherheit als Problem der Moderne." In *Handeln unter Risiko, Gestaltungsansätze zwischen Wagnis und Vorsorge*, herausgegeben von Herfried Münkler, 33–64. Bielefeld.

Christen, Markus, Bert Gordijn, und Michele Loi, Hrsg. 2020. *The Ethics of Cybersecurity*. Cham: Springer. https://doi.org/10.1007/978-3-030-29053-5.

CVE. o. J.. „Overview." Abgerufen 17. Mai 2022. https://www.cve.org/About/Overview.

Dreißigacker, Arne, Bennet von Skarczinski und Gina Rosa Wollinger. 2020. *Cyberangriffe gegen Unternehmen in Deutschland Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V., 2020.

Dunn Cavelty, Myriam. 2014. „Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20 (3): 701–15. https://doi.org/10.1007/s11948-014-9551-y.

Eusgeld, Irene, Bernhard Fechner, Felix Salfner, Max Walter, Philipp Limbourg, und Lijun Zhang. 2008. „Hardware Reliability." In *Dependability Metrics: GI-Dagstuhl Research Seminar, Dagstuhl Castle, Germany, October 5 – November 1, 2005, Advanced Lectures*, herausgegeben von Irene Eusgeld, Felix Freiling, und Ralf Reussner, 59–103. Berlin, Heidelberg: Springer.

First. o.J. „Common Vulnerability Scoring System v3.1: Specification Document." Abgerufen 17. Mai 2022. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Fenner, Dagmar. 2010. *Einführung in die Angewandte Ethik*. Tübingen: Francke.

Goodin, Dan. 2021. „New Spectre attack once again sends Intel and AMD scrambling for a fix. Ars Technica." Abgerufen 17. Mai 2022. https://arstechnica.com/gadgets/2021/05/new-spectre-attack-once-again-sends-intel-and-amd-scrambling-for-a-fix/.

Google. o. J.. „About Google's App Security." Google. Abgerufen 17. Mai 2022. https://about.google/appsecurity/

Haas, Werner. 2020. „Sicherheit auf Sand gebaut? Wie Meltdown und Spectre unsere Sicht auf Mikroprozessoren veränderten." *Datenschutz und Datensicherheit – DuD* 44: 441–445. https://doi.org/10.1007/s11623-020-1302-4.

H-BRS. o. J.. „Cyber Security & Privacy (B.Sc.)." Abgerufen 17. Mai 2022. https://www.h-brs.de/de/inf/studienangebot/bachelor/cybersecurity-und-privacy.

Heise online. 2020. „Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau." *Heise Online*, 17.09.2020. https://www.heise.de/news/Hackerangriff-auf-Uniklinik-Duesseldorf-Ermittlungen-wegen-fahrlaessiger-Toetung-4904134.html.

Herrmann, Dominik, und Henning Pridöhl. 2020. „Basic Concepts and Models of Cybersecurity.“ In *The Ethics of Cybersecurity*, herausgegeben von Markus Christen, Bert Gordijn, und Michele Loi, 11–44. Cham: Springer. https://doi.org/10.1007/978-3-030-29053-5.

Holz, Thorsten und Alina Opera. 2021. „IEEE S&P'21 Program Committee Statement Regarding 'The Hypocrite Commits' Paper.“ Abgerufen 17. Mai 2022. https://www.ieee-security.org/TC/SP2021/downloads/2021_PC_Statement.pdf.

IEEE. 2022. „43rd IEEE Symposium on Security and Privacy 2022.“ Abgerufen 17. Mai 2022. https://www.ieee-security.org/TC/SP2022/cfpapers.html.

Joque, Justin und S M Taiabul Haque. 2020. „Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity“. In *New Security Paradigms Workshop 2020*, 99–110. Online. https://doi.org/10.1145/3442167.3442170.

Kaufmann, Franz-Xaver. 1973. *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Stuttgart: Enke.

Kenneally, Erin, David Dittrich und andere. 2012. „The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.“ Abgerufen 17. Mai 2022. https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

Koch, Heiner. 2014. „Freiheit und Sicherheit.“ In *Sicherheitsethik*, herausgegeben von Regina Ammicht Quinn, 135–144. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-03203-6.

Loschwitz, Martin Gerhard. 2021. „Bugs mit Vorsatz: Linux Foundation legt Analyse der Kernel-Patches vor.“ *Heise Online*, 17.09.2020. https https://www.heise.de/news/Bugs-mit-Vorsatz-Universitaet-legt-Bericht-zur-Analyse-der-Kernel-Patches-vor-6041701.html.

Macnish, Kevin und Jeroen van der Ham. 2020. „Ethics in cybersecurity research and practice.“ *Technology in Society*, 63, 101382. https://doi.org/10.1016/j.techsoc.2020.101382.

Mantel, Mark. 2022. „CPU-Sicherheitslücke: Spectre V2 ist auch bei Intel und ARM zurück.“ *Security*, 10.03.2022. Abgerufen 17. Mai 2022. https://www.heise.de/news/Spectre-V2-ist-auch-bei-ARM-und-Intel-zurueck-Angriff-auf-Branch-History-Buffer-6545263.html.

Maring, Matthias. 2013. „Ethikkodizes.“ In *Handbuch Technikethik,* herausgegeben von Armin Grunwald, 410–415. Verlag J.B. Metzler.

Microsoft. o. J.. „Microsoft's Approach to Coordinated Vulnerability Disclosure.“ *Microsoft Response Centre*. Abgerufen 17. Mai 2022. https://www.microsoft.com/en-us/msrc/cvd.

NDSS. 2022. „Call for Papers – NDSS Symposium.“ Abgerufen 17. Mai 2022. https://www.ndss-symposium.org/ndss2022/call-for-papers/.

Riescher, Gisela. 2010. „Demokratische Freiheit und die Sicherheit des Leviathan." In *Sicherheit und Freiheit statt Terror und Angst: Perspektiven einer demokratischen Sicherheit*, herausgegeben von Gisela Riescher, 1. Aufl, 11–24. Baden-Baden: Nomos.

Salter, Jim. 2021. „Linux kernel team rejects University of Minnesota researchers' apology." *Ars Technica*, 27.04.2021. Abgerufen 17. Mai 2022. https://arstechnica.com/gadgets/2021/04/linux-kernel-team-rejects-university-of-minnesota-researchers-apology/.

SAP. o. J.. „Report a Security Issue." *SAP Security Management*. Abgerufen 17. Mai 2022. https://www.sap.com/about/trust-center/security/incident-management.html.

Schlehahn, Eva. 2020. „Cybersecurity and the State." In *The Ethics of Cybersecurity*, herausgegeben von Markus Christen, Bert Gordijn, und Michele Loi, 205–25. Cham: Springer. https://doi.org/10.1007/978-3-030-29053-5.

USENIX Security Symposium 2021. „USENIX Security Publication Model Changes." Abgerufen 17. Mai 2022. https://www.usenix.org/conference/usenixsecurity22/publication-model-change.

Vaughan-Nichols, Steven. 2021. „Linux's Technical Advisory Board reports on the UMN 'Hypocrite Commits' patches." *ZDNet*, 05.05.2021. Abgerufen 17. Mai 2022. https://www.zdnet.com/article/linuxs-technical-advisory-board-reports-on-the-umn-hypocrite-commits-patches/.

Wagner, Manuela. 2020. „IT-Sicherheitsforschung in rechtlicher Grauzone. Lizenz zum Hacken." In *Datenschutz und Datensicherheit – DuD* 44: 111–120.

Weber, Karsten, Markus Christen, und Dominik Herrmann. 2020. „Bedrohung, Verwundbarkeit, Werte und Schaden." *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 29 (1): 11–15. https://doi.org/10.14512/tatup.29.1.11.

Weber, Arnd, Gernot Heiser, Dirk Kuhlmann, Martin Schallbruch, Anupam Chattopadhyay, Sylvain Guilley, Michael Kasper. 2020. „Sichere IT ohne Schwachstellen und Hintertüren." *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 29 (1): 30–36. https://doi.org/10.14512/tatup.29.1.30.

Weydner-Volkmann, Sebastian. 2018. *Moralische Landkarten der Sicherheit: Ein Framework zur hermeneutisch-ethischen Bewertung von Fluggastkontrollen im Anschluss an John Dewey*. Ergon Verlag. https://doi.org/10.5771/9783956503788.

———. 2019. „Sicherheitsfragen in der Mensch-Maschine-Interaktion." In *Mensch-Maschine-Interaktion*, herausgegeben von Kevin Liggieri und Oliver Müller, 332–337. Berlin: J.B. Metzler. https://doi.org/10.1007/978-3-476-05604-7_61

Wittmann, Lilith. 2021. „Die Staatsanwaltschaft sagt, ich habe die CDU nicht gehackt." *Medium*, 16.09.2021. Abgerufen 17. Mai 2022. https://lilithwittmann.medium.com/die-staatsanwaltschaft-sagt-ich-habe-die-cdu-nicht-gehackt-86c1ebf83f63.

Zichy, Michael. 2008. „Gut und praktisch. Angewandte Ethik zwischen Richtigkeitsanspruch, Anwendbarkeit und Konfliktbewältigung.“ In *Praxis in der Ethik: zur Methodenreflexion in der anwendungsorientierten Moralphilosophie*, herausgegeben von Michael Zichy und Herwig Grimm, 87–116. Berlin ; New York: Walter De Gruyter.

Zurawski, Nils. 2015. *Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung*. Berlin: Forschungsforum Öffentliche Sicherheit.