»Die Benutzer sind das Problem, nicht das System«
Verantwortung, Vertrauen und Vulnerabilität in IT-Sicherheitsdiskursen

Alexander Wentland und Nina Klimburg-Witjes

Einleitung: Das »Hacking menschlicher Schwächen«

Während wir diesen Artikel geschrieben haben, sind wir beide mehrfach Ziele von Social Hacking Angriffen geworden – so wie täglich Millionen Menschen, die von falschen Absender*innen per Email gebeten werden, auf einen Link zu klicken oder eine Datei zu öffnen. In einem unserer Fälle kam die E-Mail von einem Account, der jenem der IT-Abteilung der Universität Wien täuschend ähnlichsah. Die Nachricht enthielt die dringende Aufforderung, das Passwort für den Universitätszugang an den Absender zu schicken, damit dieser ein technisches Problem mit dem Zugang lösen könne. In einer anderen fingierten E-Mail wurde jemand von uns gebeten, einen vermeintlichen Bericht einer Regierungsorganisation zu kommentieren – zum Thema international cybersecurity. Anbieter*innen von Sicherheitsdienstleistungen schätzen, dass 90 Prozent aller Hackerangriffe Gebrauch von manipulativem Social Hacking machen (Kaspersky 2019; PurpleSec 2020).

Social Hacking (SH) im Kontext der IT-Sicherheit bezeichnet eine Angriffsart, bei der Hacker*innen sowohl auf die technischen als auch die soziale Komponenten eines IT-Sicherheitssystems abzielen (Abraham und Chengalur-Smith 2010). Das Ziel von Hacker*innen ist dabei, Benutzer*innen so zu manipulieren, dass sie vertrauliche Informationen preisgeben, mittels derer sich Hacker*innen dann Zugang zu Daten und Netzwerken verschaffen. Im Bereich der IT-Sicherheit hat sich mit der verbreiteten Nutzung des Internets Anfang der 1990er Jahre die Bezeich-

nung SH bzw. *Social Engineering*[1] für diese Art der Manipulation etabliert (Coleman 2012; Thomas 2002).

Mit der zunehmenden kommerziellen Relevanz des Internets und der Digitalisierung der meisten Lebens- und Wirtschaftsbereiche hielt der Begriff dann Einzug in IT-Sicherheitsdiskurse und mittlerweile auch in die Nachrichtenberichterstattung. Wie die Anschuldigungen über das angebliche Hacking des Demokratischen Nationalkomitees während der Kampagne der Demokratischen Partei für die US-Präsidentschaft 2017 oder der Twitter Bitcoin Betrug 2020[2] gezeigt haben, rufen SH-Angriffe nicht nur ein großes mediales Echo hervor, sondern können auch politische Implikationen nach sich ziehen.

Als besonders gefährlich und problematisch gilt SH im Kontext der IT-Sicherheit von Unternehmen, die besonders lukrative Ziele für Angriffe darstellen. Selbst kleine Unternehmen verfügen in der Regel über eine Dateninfrastruktur, auf der sämtliche internen und externen unternehmerischen Aktivitäten basieren. Die Kompromittierung solcher Netzwerke kann dazu führen, dass sensible Daten ausgespäht, manipuliert oder gelöscht werden. Derartige Einbrüche können massive wirtschaftliche Schäden mit sich bringen – für das Unternehmen selbst, aber auch für Kund*innen und Zulieferer, zum Beispiel durch den Zugang zu sensiblen Daten oder Betriebsgeheimnissen. IT-Verantwortliche in Unternehmen – aber auch in anderen Organisationen – sehen sich vor diesem Hintergrund vor der Herausforderung, kontinuierlich wirksame Gegenmaßnahmen zu entwickeln, die sowohl auf technischer als auch sozialer Ebene greifen müssen, da SH grundlegende menschliche Eigenschaften wie Unaufmerksamkeit, Neugier, Angst oder Gier als Einfallstor in die vermeintlich nach rein technischer Logik operierenden IT-Systeme ausnutzt (Hadnagy 2010; Krombholz et al. 2015).

Mitarbeiter*innen von Unternehmen und anderen Organisationen wiederum stehen mittlerweile im Zentrum eines Wettrüstens zwischen externen

---

1 *Social Hacking* wird insbesondere im angelsächsischen Raum häufig als *Social Engineering* bezeichnet. Eine Verbindung zu der Verwendung des Begriffes in den Sozialwissenschaften im Sinne einer Beeinflussung der Gesellschaft durch Planung und Steuerung ist dabei nicht beabsichtigt. Aus diesem Grund verwenden wir in diesem Text ausschließlich die Bezeichnung »Social Hacking« (SH), auch wenn in den meisten Dokumenten und Interviews von »Social Engineering« gesprochen wird. Beide Formen gelten als synonym.

2 Beim Hackerangriff auf Twitter 2020 wurden am 15. Juli bei dem populären Mikroblogging-Dienst Benutzerkonten von ca. 130 prominenten Personen und Unternehmen gehackt – u.A. die der Unternehmer Elon Musk und Bill Gates sowie von Politikern wie Barack Obama und Joe Biden. Über diese Konten wurden Tweets veröffentlicht, die darauf abzielten, Internetnutzer*innen um Bitcoin-Guthaben zu betrügen. In der medialen Berichterstattung wurde der Vorfall einerseits als gravierend, anderseits jedoch auch als glimpflich eingeordnet, da keines der Benutzerkonten als Sprachrohr zur Verbreitung politischer Inhalte oder Falschmeldungen verwendet wurde, was ohne Weiteres in orchestrierter Form möglich gewesen wäre.

Angreifer*innen und den Sicherheitsabteilungen ihrer Organisation. Der Schutz von Firmen vor Cyberangriffen, externer Einmischung und Spionage ist alles andere als neu, jedoch hat die massive Verbreitung von Informations- und Kommunikationstechnologien (IKT) im beruflichen wie privaten Umfeld, die Sicherheitsproblematik in den letzten Jahrzehnten zusätzlich verstärkt (Morozov 2013). Aus Unternehmenssicht können daher praktisch alle Beschäftigten unfreiwillig zu einem Sicherheitsrisiko werden, weshalb die Investitionen in IT-Sicherheitsschulungen und -trainings für Mitarbeitende seit Jahren massiv steigen (Grand View Research 2020).

In diesem Bereich hat sich in den letzten Jahren eine eigene Branche etabliert, die Beratung, Trainings und Bewertungsinstrumente anbietet, um mit derartigen Risiken umzugehen. Besonders wird hier die Konvergenz von technischer und sozialpsychologisch inspirierter Expertise betont, die zum Schutz vor SH-Angriffen zentral sei und eine spezifische Expertengemeinschaft hervorgebracht hat. Allerdings: Die meisten der angebotenen Trainings und Sicherheitslösungen zeigen nicht die erwünschte Wirkung, wie unsere Interviewpartner*innen immer wieder festgestellt haben. Denn mehr noch als herkömmliche Hacking Methoden, die auf Schwachstellen in fehlerhafter Software abzielen, ermöglicht es SH den Angreifern, auch in vorbildlich gewartete und abgesicherte IT-Systeme einzudringen. Diese kontinuierliche Bedrohung und die scheinbare Unmöglichkeit eines flächendeckenden Schutzes vor SH-Angriffen hat das Wachstum dieser Branche der Sicherheitsindustrie eher zusätzlich gefördert als gehemmt.

Dieser Beitrag untersucht, wie Hacker*innen und Sicherheitsexpert*innen diskursiv die Figur der, wie wir sie bezeichnen, *defizitären Benutzer*in* konstruieren und den Menschen als das schwächste Glied in der Sicherheitsarchitektur darstellen. Unsere Analyse baut auf den Science and Technology Studies (STS) auf, welche die wechselseitigen Einflüsse von technischer Rationalität und gesellschaftlichen Wertvorstellungen in den Blick nehmen (Jasanoff 2004; Sismondo 2010; Wynne 2006).

Anhand von qualitativen Expert*innen-Interviews untersuchen wir das Zusammenspiel zwischen Nutzer*innen, IT-Sicherheitsabteilungen und dem weiter gefassten SH-Expertendiskurs in Bezug auf die IT-Sicherheit in Unternehmen. Hier zeigt sich eine Verschiebung in der Art und Weise, wie individuelle Defizite vis-à-vis einer kollektiven Sicherheit konstruiert werden: Während viele Unternehmen weitgehend von der sogenannten digitalen Revolution profitiert haben, wurden damit einhergehende sicherheitsbezogene Risiken zunehmend auf die einzelnen Mitarbeitenden ausgelagert.

Unsere Analyse basiert auf insgesamt 13 Expert*innen-Interviews sowie teilnehmender Beobachtung und Hintergrundgesprächen während der beiden wichtigsten Computersicherheits- und Hacking-Konferenzen *Black Hat* und *Defcon* im Juli 2017 in Las Vegas. Zum Abgleich unserer induktiv generierten Interpretatio-

nen mit europäischen Debatten haben wir an der *Vienna Cyber Security Week* im Januar 2018 teilgenommen und weitere Personen aus Unternehmen mit umfassender IT-Sicherheitsinfrastruktur in Finanz- und Gesundheitswesen interviewt. Zudem haben wir eine Dokumentenanalyse durchgeführt, für die wir systematisch Medienberichte und Blogs zum Thema IT-Sicherheit sowie Websites von SH-Expert*innen-Netzwerken ausgewertet haben.

Zunächst zeigen wir in unserer Analyse, wie Nutzer*innen einerseits als grundsätzlich unberechenbare Gefahrenquelle, zugleich jedoch auch als einzig wirksamer Ansatzpunkt für eine Gegenstrategie konstruiert werden. Diese Herstellung eines Defizitverständnisses, betrifft nicht nur einzelne Sicherheitspraktiken, sondern erstreckt sich über weite Bereiche von Organisationen und Institutionen in Politik und Wirtschaft, Wissenschaft und Medien. Abschließend diskutieren wir, wie eine Alternative zum Defizitdenken im Bereich der digitalen Sicherheit aussehen könnte, und zwar in der Form einer »Kultur der Vulnerabilität« und der aktiven Auseinandersetzung mit einem im Entstehen begriffenen sozio-technischen Regime digitaler Organisationssicherheit, das auf geteilter statt auf individueller Verantwortung basiert.

Konzeptioneller Zugang

Von einer Politik der Defizitkonstruktion …

In Bezug auf SH-Angriffe werden die Mitarbeiter*innen oft als das »schwächste Glied« in der Sicherheitsinfrastruktur bezeichnet. In unserer empirischen Auswertung wurde deutlich, dass viele IT-Spezialist*innen von unwissenden und leichtgläubigen Benutzer*innen ausgehen, die in ihrer Arbeitsroutine zwar leicht zu manipulieren seien, deren Verhalten in Bezug auf die Sicherheitspraxis des Unternehmens zugleich jedoch schwer vorhersehbar sei.

Diese Muster der Problematisierung ähneln dem Defizitmodell in Teilen der konventionellen Wissenschaftskommunikation (*public understanding of science*), welches in den STS umfassend kritisiert worden ist (Irwin 2014; Jasanoff 2016; Wynne 2006). Die Kritik richtet sich vor allem auf ein reduktionistisches Verständnis von gesellschaftlichen Kontroversen, die regelmäßig um neue wissenschaftliche Einsichten und Technologien entbrennen, wie beispielsweise Gentechnik oder Atomenergie. Obwohl gesellschaftliche Konflikte um Wissenschaft und Technik niemals rein epistemisch motiviert sind, sondern vielmehr grundlegende politische und soziale Wertfragen adressieren, sehen Vertreter*innen des Defizitmodells das Heilmittel gegen Dissens darin, die wissenschaftliche Kompetenz (*literacy*) der Bevölkerung zu fördern. Diese, so die Annahme, führe dann automatisch zur Akzeptanz umstrittener wissenschaftlich-technischer Entwicklungen (Bodmer und Wil-

kins 1992; Bybee 1997). Während diese Perspektive eine breite institutionelle Unterstützung fand, wurde die implizite Charakterisierung von Bürger*innen als irrational und aufklärungsbedürftig jedoch auch normativ hinterfragt und empirisch widerlegt. So zeigte Brian Wynne (1992) in einer vielzitierten Studie zum Umgang mit radioaktiv kontaminierten Ländereien in England nach dem Tschernobyl-Reaktorunglück, wie vorkonfigurierte Machtasymmetrien eine Dominanz von wissenschaftlichem Expertenwissen sicherstellen. Widersprechende Positionen wurde in dem untersuchten Fall frühzeitig als Wissenschaftsfeindlichkeit gedeutet, obwohl die Farmer*innen über relevantes Erfahrungswissen verfügten und als unmittelbar Betroffene ein besonderes Interesse an der Mitdeutung der Problemlage hatten – anders als die Forschenden.

Forschung in den STS verweist häufig darauf, dass institutionell getragene Initiativen, die von Kompetenzdefizits ausgehen, nicht die erwünschten Ergebnisse erbracht haben – nämlich Kontroversen um Expertise zu befrieden (Irwin 2014; Jasanoff 2016; Stilgoe et al. 2014). Darüber hinaus haben STS-Studien untersucht, wie Machtasymmetrien durch die Professionalisierung und Institutionalisierung von Expertise zu einer Schließung von Diskursen führen, wodurch nicht-wissenschaftliche, aber potenziell betroffene Akteur*innen nicht auf Augenhöhe mitwirken können (Wynne 2006). Aus Sicht des Defizitmodells gelten Personen und Gruppen, die nicht durch ihre institutionelle Position als Wissensträger*innen legitimiert sind lediglich als Rezipient*innen von Wissen. Diese Gruppen bedürfen einer angemessenen Aufklärung und Bildung oder müssen sich – falls sie diese ablehnen – den Vorwurf mutwilliger Ignoranz gefallen lassen.

Die Verbreitung und Wirkmächtigkeit des Defizitmodells kann auch in anderen gesellschaftlichen Kontexten beobachtet werden. So konstatieren Pfotenhauer et al. (2019) den Trend, die Zukunftsfähigkeit von institutionellen Akteuren aller Art – angefangen bei Unternehmen bis hin zu ganzen Nationalstaaten – in Kategorien eines »Innovationsdefizits« zu betrachten. Akteur*innen, denen ein Innovationsdefizit diagnostiziert wird, werden dadurch unter Rechtfertigungsdruck gesetzt. Von ihnen wird erwartet, das Defizit mittels externer Expertise zu schließen. Die Autoren argumentieren, dass solche Defizitdiagnosen eine bestimmte politische Problemlage performativ erzeugen, statt diese – wie oft behauptet – objektiv zu beschreiben. Pfotenhauer und Jasanoff (2017) beobachten hier eine »Wende in der Innovationspraxis« der letzten Jahre: Indem wirtschaftliche, politische und wissenschaftliche Akteur*innen sich zunehmend an globalen Vorbildern für erfolgreiche Innovation wie dem Silicon Valley oder MIT orientieren, werden lokales Wissen, regionale Erfahrungen und Interessen Betroffener häufig marginalisiert. Dieser Dynamik liegt die Annahme zu Grunde, dass Akteur*innen, die nicht dem dominanten Innovationsregime folgen, unweigerlich ins Hintertreffen geraten würden, so Pfotenhauer und Jasanoff.

Analog zu diesem Defizitmodell der Innovation, gehen auch Führungskräfte von Unternehmen und IT-Abteilungen häufig davon aus, dass ihre Belegschaft durch fehlende Kompetenz im Umgang mit potenziellen SH-Angriffen hinter die Sicherheitsstandards des Unternehmens zurückfällt. Dieses Framing zeigte sich deutlich in den von uns ausgewerteten Sicherheitsstrategien der Firmen, Berichten in Branchennachrichten und in den Diskussionen auf den von uns besuchten Security-Tagungen. Auch in diesem Fall erheben technische Expert*innen den Anspruch auf alleinige Definitionsmacht darüber, was als geeignetes Wissen im Umgang mit (Sicherheits-)Problemen gelten soll. Die von uns recherchierten SH-Schulungen für Mitarbeitende gehen dem entsprechend davon aus, dass die Teilnehmenden selbst ein Sicherheitsrisiko innerhalb des Unternehmens darstellen. Ziel sei es dieses Risiko auf der Individualebene zu identifizieren, zu »diagnostizieren« und somit die Daten- und Kommunikationssysteme der Firmen widerstandsfähiger gegenüber SH-Angriffen zu machen.

Pfotenhauer et al. (2019) haben in diesem Kontext eine Forschungsperspektive entwickelt, welche die Aufmerksamkeit auf die verschiedenen Ebenen der Defizitkonstruktion lenkt: Etwas als defizitär zu konstruieren – sei es die Benutzer*innen eines Computers oder eine ganze Volkswirtschaft – beginnt mit der Diagnose eines Problems, das es zu lösen gilt. Expert*innen versprechen in diesem Sinne nicht nur potentielle Lösungsansätze, sondern beanspruchen zugleich auch die Deutungshoheit über die Problemdefinition selbst und stützen sich dabei auf vermeintlich objektiv feststellbare Methoden und Maßstäbe. Arbeiten aus den STS zu diesem Spannungsfeld haben gezeigt, dass solche Problematisierungen und vorgeschlagenen Lösungsansätze immer auch Annahmen über eine wünschenswerte soziale, politische und wirtschaftliche Ordnung implizieren (Jasanoff 2016; 2015).

… zu einem neuen Verständnis von sozio-technischer Vulnerabilität

Um die Bedeutung von SH für Sicherheitsdiskurse zu verstehen, schlagen wir eine Perspektive vor, die die Belegschaft nicht prinzipiell pathologisiert, sondern von technifizierten Lebenswelten ausgeht, die aus dem Wechselspiel technischer Rationalität und sozialer Normen hervorgehen. Aufbauend auf STS-Arbeiten zu »technological culture« (Bijker 2006) und »socio-technical vulneraility« (Hommels et al. 2014) schlagen wir in diesem Beitrag den Begriff *Kultur der Vulnerabilität* vor, um dem eher technokratischen Risikovokabular eine reflexive Sicht hinzuzufügen. Die Figur der Vulnerabilität wurde in den STS als Antwort auf den Risikobegriff im Sinne von Ulrich Becks (1992) Risikogesellschaft entwickelt. Vulnerabilität ist in der STS-Konzeption weder objektivierbar noch kann sie als inhärentes Merkmal bestimmter als risikohaft beschriebener gesellschaftlicher Bereiche verstanden werden. Auf normativer Ebene kann die Berücksichtigung von Vulnerabilität den Deutungsraum einer Gesellschaft über das vorherrschende Risikoverständnisses

hinaus ausweiten, was besonders dringlich erscheint, wenn sich im Zuge der zunehmenden Digitalisierung vieler Lebensbereiche Fragen von Verantwortung und Vertrauen neu stellen.

Methodischer Ansatz und Feldforschung

Unsere Analyse stützt sich auf ethnographische Feldforschung sowie Experteninterviews, welche im Rahmen von drei internationalen Konferenzen zu IT-Sicherheit und Hacking durchgeführt wurden. Wir haben dafür an der *Vienna Cyber Security Week* im Januar 2018 sowie den internationalen Konferenzen *Black Hat* und *Defcon* teilgenommen, die im Juli 2017 in Las Vegas, USA stattfanden. Insbesondere die beiden letztgenannten Konferenzen sind die führenden Veranstaltungen in diesem Bereich und ziehen jedes Jahr rund 20.000 Interessierte an. *Black Hat* richtet sich v.a. an Unternehmen und Regierungsbehörden in verschiedenen Bereichen, wie Justiz, Wirtschaft und Gesundheit sowie Energie und Verteidigung. Die *Defcon* wiederum gilt als die informellere und kreativere Konferenz mit einem gemischten Publikum, welches aus Hacker*innen und IT-Fachleuten sowie Journalist*innen, Nichtregierungsorganisationen im Bereich des Datenschutzes, Aktivist*innen und Forschenden besteht. Während der letzten Jahre wurden auf beiden Konferenzen vermehrt Vorträge über menschliche Faktoren in der IT-Sicherheit gehalten sowie ein *Social Engineering Village* eingerichtet – vergleichbar mit einer Sektion bei akademischen Konferenzen.

Konferenzen und Großveranstaltungen wie diese können als ›Seismographen‹ der Debatten, Schlüsselthemen und sozialen Interaktionen ihrer jeweiligen Bereiche verstanden werden und sind zentral für anthropologische Untersuchungen (Høyer Leivestad und Nyqvist 2017). Darüber hinaus verstehen wir diese Großveranstaltungen, von Keynote Talks, Lunch Talks, Podiumsdiskussionen und Arbeitsgruppen bis hin zu After-Partys, als aktive gesellschaftspolitische Räume, in denen wir die Prozesse untersuchen können, durch die Wissen und Expertise präsentiert, generiert, erprobt oder stabilisiert werden (Hajer 2009; 2005; Harper 1998; Little und Painter 1995).

Die Teilnahme an den jeweiligen Konferenzen ermöglichte es uns, zu verstehen, in welcher Form »contextualized interactions produce social realities like understandings of particular problems and the power relations brought into being in addressing those problems« (Campbell et al. 2014: 5). Darüber hinaus, und aufgrund des oft sensiblen Charakters von IT-Sicherheitsthemen, haben wir während der Veranstaltungen informelle Interviews und Diskussionen mit den Teilnehmenden durchgeführt, oft in Form von unstrukturierten Gesprächen während der Pausen oder in der Warteschlange für einen Vortrag.

Das empirische Material wurde nach Hajers (2003) Ansatz der argumentativen Diskursanalyse ausgewertet. Dieser sieht Diskurs »als ein Ensemble von Ideen, Konzepten und Kategorien [.], durch das ein Phänomen mit Bedeutung versehen wird, und welches durch ein bestimmtes, identifizierbares Set von Praktiken produziert und reproduziert wird« (Hajer 2003: 278). Dieser Ansatz ermöglicht es zu verstehen, wie und unter welchen Bedingungen ein spezifischer Diskurs dominant wird. Besonders relevant für unseren Beitrag ist dabei der Begriff der *Storylines*, der verdichtende, zentrale Elemente eines breiteren SH-Diskurs bezeichnet.

Empirische Analyse

SH gilt heute als zentrale Komponente nahezu aller Cyberangriffe (Abraham und Chengalur-Smith 2010: 183) und basiert auf einer Kombination aus technischen und sozialen Angriffen, wie die folgende Anekdote exemplarisch illustriert: Kevin Mitnick, einer der Protagonist*innen des sozialpsychologisch interessierten Teils der Hackerszene, legte 2010 die inhärente Vulnerabilität maschinenlesbarer Dienstausweise und Zugangskontrollen in gesicherten Gebäuden offen. Im Auftrag eines Kunden, der die Sicherheitsinfrastruktur seines Unternehmens testen wollte, kam Mitnick in der Raucherecke vor dem Gebäude ins Gespräch mit Mitarbeitenden, die ihn für einen Kollegen hielten. Währenddessen gelang es Mitnick unbemerkt über einen versteckten RFID-Scanner in seiner Tasche, die Zugangskarten der Mitarbeitenden auszulesen, die Kartendaten zu kopieren und sich so Zugang zu verschaffen. Im Gebäude selbst war Mitnick mittels einer in seiner Brille installierten Mini-Webcam in der Lage, die Mitarbeitenden bei der Eingabe ihrer Passwörter zu filmen und sich so auch Zugang zur digitalen Infrastruktur zu verschaffen (Klimburg 2017). Dieses Beispiel verweist auf den kritischen Problemfokus des SH-Expertendiskurses, welchen wir in der folgenden empirischen Analyse systematisch dekonstruieren.

Die Suche nach den Verantwortlichen: Die »dummen Mitarbeitenden« als Sicherheitsrisiko?

In den letzten Jahren sind im Bereich der IT-Sicherheit zahlreiche Fachbücher publiziert worden, die sowohl Methoden und Techniken zur Manipulation menschlichen Verhaltens als auch Präventionsstrategien gegen solche Angriffe thematisieren (Hadnagy 2010; Long et al. 2011; Workman 2007). Professionelle Anbieter*innen werben im Internet für ihre Beratungsleistungen und führen dabei häufig spektakuläre Hackerangriffe wie das oben erwähnte Beispiel als Beleg für die Dringlichkeit des Problems an. Dabei wird häufig eine permanente Bedrohungslage konstruiert, in der katastrophale Angriffe jederzeit eintreten können oder bereits ein-

getreten, jedoch vom Unternehmen unbemerkt geblieben sind. Ein Artikel im Tech-Magazin *Wired* mit dem Titel »Social Engineering Always Wins: An Epic Hack Revisited« bringt dieses Gefühl der permanenten Bedrohung auf den Punkt: »In short, all of this has happened before, and all of it will happen again« (Honan 2014).

Während sich Ingenieur*innen und Programmierer*innen vormals hauptsächlich mit Schwachstellen in Soft- und Hardware beschäftigten, wird in den zunehmend nutzerzentrierten Sicherheitsdiskursen die menschliche Fehleranfälligkeit als das Hauptproblem dargestellt. In unseren Interviews und während der Konferenzen wurde deutlich, dass die meisten befragten Expert*innen den Menschen als das »schwächste Glied« in der Sicherheitsinfrastruktur sehen (IP 1; 3, 4, 5), was in Aussagen wie dieser deutlich wird: »users are the problem, not the system« (IP 2). Bemerkenswert an diesem Zitat ist, dass der bzw. die Benutzer*in nicht als Teil des Systems verstanden wird, sondern als ein externer Faktor, der entweder richtig oder falsch handelt. In Interviews und in Vorträgen wurde häufig die Figur der »stupid people« angeführt, die auf die vermeintliche Unfähigkeit der Benutzer*innen, sich den immer komplexeren sozio-technischen Herausforderungen der IKT anzupassen, rekurriert – unabhängig davon »how much education and training is thrown upon them« (IP 4). Dieses Zitat deutet bereits an, dass die Benutzer*innen als unfähig angesehen werden, selbst die einfachsten Vorsichtsmaßnahmen zu treffen, wie beispielsweise adäquate Passwörter zu erstellen oder die Identität eines*r vermeintlichen Mitarbeitenden zu prüfen, die/der sich Zugang zu sensiblen Information verschaffen möchte.

Unabhängig davon, wie gesichert die IT-Infrastruktur eines Unternehmens auch sein mag, wie der IT-Sicherheitsexperte Hulme (2015) in einem Onlinebeitrag betont, »there's always going to be employees who hand over the keys to the kingdom – or at least raises the drawbridge when asked nicely, or with authority.«

Besonders auffällig war, dass in den meisten Interviews und auf allen von uns besuchten Konferenzen die Angreifer*innen als ein unvermeidliches Übel gesehen wurden. Dies zeigte sich u.a. in der häufigen Darstellung des Hackers und der Hackerin als jemand, der bzw. die in der Lage sei, alles zu tun, was er oder sie will – nicht aufgrund außergewöhnlicher technischer Fähigkeiten, sondern aufgrund der vermeintlichen Unfähigkeit der Nutzer*innen. Während also Hacker*innen oft mit Bewunderung für ihre elaborierten Angriffe beschrieben wurden, sind es die unachtsamen Mitarbeiter*innen, die ihre Daten versehentlich an diese preisgeben würden und somit diskursiv als die eigentliche Gefahrenquelle konstruiert werden. Doch warum rekurrieren so viele Expert*innen in erster Linie auf menschliche »Dummheit« und worauf gründet sich diese ihrer Ansicht nach?

Unseren Interviewpartner*innen zufolge und in Übereinstimmung mit der (eher technischen) Literatur zu SH ist seitens der Expert*innen die wichtigste Erklärung für den Erfolg von SH-Angriffen, dass diese Manipulationen auf Emotionen wie Angst, Neugier, Aufregung oder Gier nach ökonomischen Gewinnen

abzielen. Zudem öffnet oftmals auch Vertrauen den Angreifenden die Tür, wie ein weiteres Zitat aus dem oben genannten Onlinebeitrag zeigt:

> »Humans are fairly dumb; we are easily led; trust readily and we have this natural tendency (for the most part) to think other folk have our best interests in mind. It's this naivety that attackers will take advantage of when attacking your system. SE is taking advantage of a human's natural desire to trust and reciprocate kindness.« (Hulme 2015)

Dabei wird in der Regel wenig berücksichtigt, dass Vertrauen eine Grundvoraussetzung der Zusammenarbeit in einem Unternehmen, aber auch für unternehmensübergreifende Kooperationen ist. Wenn selbstverständliche Vertrauensbeziehungen in Frage gestellt werden, kann dies für die individuellen Mitarbeiter*innen im Arbeitskontext zu Spannungen zwischen widersprüchlichen Erwartungen führen. Zwei unserer Interviewpartner*innen aus dem mittleren Management im Bank- bzw. Gesundheitswesen berichteten von dieser Gratwanderung zwischen pragmatischem Vertrauen und kodifiziertm Misstrauen, insbesondere in Interaktionen mit den jeweiligen Kund*innen.

Zum Beispiel gelte im Außeneinsatz in den Büros der Kund*innen für alle Anwesenden die strikte Sicherheitsregel, den eigenen Laptop mit Schloss und Kabel zu sichern. Halte man sich nicht an diese Regel, werden unabgeschlossene Laptops konfisziert und erst nach dem Ende eines Meetings wieder ausgegeben. »Trotzdem schließt oft niemand seinen Laptop an«, erklärt uns einer der Interviewpartner. »Wenn die Kunden das selbst nicht machen, dann machst du das auch nicht als Externer, du möchtest nicht den Eindruck vermitteln, dass du misstrauisch bist. […] Man will ja keinen Zweifel an der anderen Person kommunizieren« (IV 12).

Diese symbolische Geste des Vertrauens, seinen Laptop nicht anzuschließen, wird von den Akteur*innen für wichtiger erachtet als die Einhaltung der IT-Sicherheitsvorgaben, was jedoch auch bedeutet, dass im Falle eines Datendiebstahls der oder die individuellen Mitarbeiter*in die Verantwortung und damit das Risiko trägt, wenn er oder sie im Sinne des eigenen Unternehmens einen vertrauensvollen Umgang mit den Kund*innen kultiviert. Dieses Risiko war unseren Interviewpartner*innen, die sich in ihrem Arbeitsalltag über eine Reihe von Regeln wissentlich hinwegsetzten, bewusst. Sie empfanden die Praxis aller Beteiligten, ihre Laptops nicht anzuschließen, als fahrlässig, weil die Büros »meistens so groß sind, dass einfach jemand einen Laptop mitnehmen könnte, ohne dass das auffällt«. Aber, so die Person, »dadurch, dass das oft keiner macht, würde man dann komisch auffallen« (IV 13).

Auch aufseiten der IT-Sicherheitsabteilungen sind sich viele Verantwortliche der Tatsache bewusst, dass die Mitarbeiter*innen mit einer Situation konfrontiert sind, die sie selbst nicht aktiv herbeigeführt haben und die vor einigen Jahrzehnten noch unvorstellbar war. Einer unserer Gesprächspartner gab an, dass sich die

Last, für die Sicherheit des eigenen Unternehmens zu sorgen, mit der Anzahl der Mitarbeiter*innen und den technischen Entwicklungen vervielfacht hat: »A while ago, you had a fence, a guard with a flashlight and a German shepherd at the gate, and your premises were basically secured«. Heute wiederum müssten fast alle Mitarbeiter*innen so vorsichtig und gut geschult sein wie der besagte Wachmann am Tor und verdächtige Aktivitäten von sich aus erkennen. »But of course, this is not the people's primary job. They are office workers, accountants, technicians – how are they supposed to handle targeted phishing attacks deliberately designed for them, while going about their regular business?« (IP 7).

Diese durchaus differenzierte Sichtweise steht jedoch in starkem Kontrast zu dem, was in vielen Vorträgen auf den besuchten Konferenzen diskutiert wurde. In Bezug auf Informationssicherheit wurden die Mitarbeiter*innen insbesondere auf SH-Events als ungebildet und unfähig dargestellt, sich selbst oder ihr Unternehmen zu schützen. Die beschriebene Verantwortungsverlagerung und -diffusion in Bezug auf die Unternehmenssicherheit wurde von den meisten SH-Expert*innen dabei jedoch nicht hinterfragt. Auch die Paradoxie, die sich aus dem Abzielen von SH-Angriffen auf menschliche Emotionen wie Vertrauen, die auch im Arbeitsumfeld eine entscheidende Rolle spielen, ergibt, wurde in diesem Kontext kaum kritisch reflektiert. Auffallend war vor allem, wie viele Redner*innen auf eine Arzt-Patienten Metaphorik zurückgriffen, in der sie Beschäftigte als Patient*innen beschrieben, während sie sich selbst oder die Mitglieder der SH-Expertengemeinschaft wiederum mit Ärzt*innen gleichsetzten, also mit denjenigen, »who take care of the stupid people because they need us« (IP 2). Wie im nächsten Abschnitt ausführlicher dargelegt wird, stützen sich die Expert*innen häufig auf Metaphern aus Medizin und Psychologie um die Pathologie des »dummen« Benutzers bzw. der »dummen« Benutzerin und die begrenzte Wirksamkeit von IT-Sicherheitsschulungen zu diagnostizieren.

Die Rolle von Expertise und die fortlaufende Defizitkonstruktion

In der folgenden Vignette erörtern wir eine Beobachtung, die wir während unserer Feldforschung auf der *Defcon* Tagung gemacht haben, die eindringlich zeigt, wie IT-Sicherheitsexpert*innen ihre SH-Expertise konstituieren und performativ umsetzen:

> Am zweiten Tag der *Defcon* stehe ich an der Circle Bar im berühmten Caesar's Palace Hotel in Las Vegas. Der Andrang an der Bar ist nach den Vorträgen groß. Die meist männlichen Konferenzteilnehmer, die sich hier versammeln tragen alle möglichen – z.T. ironisch gemeinten – Hacker-Insignien, angefangen von Abzeichen aus früheren Konferenzen bis zu Hüten aus Alufolie »zum Schutz subversiver

> Gedanken«. Plötzlich kommen zwei Männer auf eine Gruppe von etwa zehn Personen zu, einer von ihnen hält eine kleine silberne Dose in der Hand, die schnell die Aufmerksamkeit der Gruppe erregt. Auf die Frage, was da drin sei, antwortet er: »*Pfeffer. Sehr scharfer Pfeffer, der euch zum Weinen bringen wird wie ein Baby. Wollt ihr ihn probieren?*« Jemand aus der Gruppe nimmt die Dose, streut etwas von dem roten Pulver auf seinen Handrücken und leckt ihn ab. Die Menge jubelt, während er zu husten beginnt, flucht und würgt. Der Mann, der die Dose anbot – nennen wir ihn Lukas – lächelt und übergibt sie dem Freiwilligen feierlich zusammen mit einem T-Shirt – jetzt ist es an ihm, jemanden außerhalb seiner Gruppe für diese Herausforderung zu gewinnen. Was wie ein Initiationsritus wirkt, wird mehrmals fortgesetzt, und fast alle, die den Pfeffer nehmen, bleiben im Anschluss bei der Gruppe.
>
> Es stellt sich heraus, dass Lukas nicht nur zum Spaß Fremden Pfeffer anbot. Er ist der Inhaber einer sehr erfolgreichen »Penetrationstest«-Firma, die diese Methode nutzt, um Menschen in unbequeme Situationen zu locken, die diese als aufregend und verbindend erleben, um dadurch neue Geschäftskontakte zu knüpfen. Lukas Kunden – meist Wirtschaftsunternehmen, aber auch Regierungsbehörden – beauftragen ihn, das Risikobewusstsein ihrer Mitarbeiter zu testen und sie im Zuge dessen wissentlich oder unwissentlich unter enormen Stress zu setzen. Anschließend meldet seine Firma diese »menschlichen Sicherheitsverletzungen« an die Führungskräfte und bietet Schulungen an, die zeigen sollen, wie diese »Fehler« in Zukunft verhindert werden können. Laut Lukas könnte jeder auf diese Angriffe hereinfallen, und je schwieriger es ist, Social Hacking erfolgreich durchzuführen, desto mehr spornt das ihn und seine Kollegen an. (FN. 2:2017_7.27)

Diese Feldnotiz enthält bereits einige der Schlüsselelemente für die Konstituierung eines SH-Expertisebereiches, einer entsprechenden Community und der für sie zentralen Prämissen, durch die der bzw. die »defizitäre Nutzer*in« konstruiert wird. Erstens verdeutlicht sie, dass SH-Expert*innen in den meisten Fällen nicht nur technische Expert*innen sind, sondern die für SH-Angriffe erforderlichen sozialen Kompetenzen mit ihrer technischen Expertise kombinieren. Sofern sie nicht in anderen Bereichen der IT-Sicherheit tätig sind, leitet sich ihre epistemische Autorität daher nicht primär aus ihren technischen Fähigkeiten ab. Auch der zuvor erwähnte Hacker Kevin Mitnick hat seinen Ruf nicht seinen besonderen Programmierfähigkeiten zu verdanken. Vielmehr ergibt sich die Rolle derartiger SH-Expert*innen aus der Tatsache, dass sie beide »Sprachen« sprechen können – (technischen) »Code« und »Social« –eine Verbindung, welche häufig von Konferenzteilnehmer*innen verwendet wurde. Wie in vielen professionalisierten Bereichen wird auch in der IT-Sicherheit vor allem technisches Knowhow als Expertenwissen dargestellt, welches qua Definition der breiten Öffentlichkeit unzugänglich bleibt, sodass es ausgewiesener Expert*innen bedarf, um Probleme und Fragestel-

lungen adäquat zu adressieren. Im Falle von SH wird diese Wissensasymmetrie noch in eine weitere Richtung ausgedehnt: Das unterstellte Kompetenzdefizit bezieht sich hier nicht nur auf das technische Fachwissen, sondern auch auf die soziale Kompetenz.

Gerade diese Verknüpfung gilt als Alleinstellungsmerkmal, das SH-Expert*innen sowohl von z.B. Personalmanager*innen als auch von den vermeintlich rein Technik-fokussierten Hacker*innen unterscheidet.

Zweitens wurde nicht nur in der oben beschriebenen Situation, sondern in zahlreichen Gesprächen und Interviews deutlich, dass SH-Expert*innen nicht nur Antworten auf Sicherheitsproblematiken präsentieren, sondern zugleich auch selbst bestimmte Betriebsabläufe als Sicherheitsprobleme konstruieren. Um ihr Geschäftsmodell aufrechtzuerhalten, perpetuieren sie ein Narrativ von ständiger Bedrohung und sprechen sowohl diffuse Ängste bei Mitarbeiter*innen an, die nicht für die Gefährdung des gesamten Unternehmens verantwortlich sein wollen, als auch die schwer nachvollziehbare Fehleranfälligkeit der Technik selbst. Hierbei ist die Art, wie suggeriert wird »nobody is safe, everybody could become a victim, even experts« (IP6) von grundlegender Bedeutung, um erfolgreich Beratungsleistungen und Weiterbildungen anzubieten bzw. für diese Leistungen zahlende Kund*innen zu finden. Daraus ergibt sich, drittens, eine wechselseitige Abhängigkeit zwischen Expert*innen und Laien bei der Konstruktion von SH-Expertise: Da sich das Fachgebiet der Expert*innen letztlich aus den Folgen menschlicher Verhaltensmuster ergibt, erwartet kaum jemand aus diesem Bereich, dass die adressierten Probleme jemals endgültig gelöst werden. In diesem Sinn leben SH-Expert*innen von der fortwährenden Defizitkonstruktion. Diese Dynamik spiegelt sich, wie im Folgenden gezeigt wird, auch in der Konstruktion möglicher Maßnahmen und Erfolgsbeurteilungen wider.

Vertrauenswürdigkeit testen: Präventionsmaßnahmen und ihre Erfolgsmessung

In Anbetracht von SH als häufigstem Angriffsmodus im Bereich der Cyberkriminalität sowie der diskursiv verstärkten Risikowahrnehmung, diskutieren wir im letzten Teil dieses Beitrags, wie sich SH-Expert*innen Sicherheitsmaßnahmen vorstellen, wer diese durchführen soll und woran sich ihr Erfolg messen lässt. In den meisten Gesprächen, Interviews und Dokumenten wurde die wiederholte Schulung und Ausbildung der Mitarbeiter*innen als die vielversprechendste Lösung des SH-Problems genannt. In seinem Vortrag zu »Why most cyber security trainings fail« auf der *Black Hat* Conference argumentierte Arun Vishwanath jedoch, dass die meisten benutzerorientierten IT-Sicherheitsbewusstseinsschulungen bei weitem nicht den gewünschten Effekt hätten. Der Grund dafür sei, so Vishwa-

nath, dass die finanziellen Ausgaben für die Schulungen (z.B. durch hohe Honorare für die eingeladenen SH-Experten und den Dienstausfall der Mitarbeiter*innen) die finanziellen Verluste durch Angriffe oft überwiegen. Gleichzeitig würden auch selbst nach wiederholten Schulungen Mitarbeiter*innen fehlerhafte Links öffnen oder sensible Informationen unbedacht preisgeben. Obwohl diese Beobachtung in SH-Kreisen weit verbreitet ist, würden Unternehmen und Regierungen weiterhin große Summen für Sicherheitsfirmen ausgeben, die ihren Mitarbeiter*innen zumindest theoretisch beibringen, wie sie sich vor SH-Angriffen schützen können.

Laut Vishwanath sei erfolgreiches SH demnach nicht das Ergebnis des sprichwörtlichen »people problem«, sondern ein Problem von »our understanding of people«. Für ihn liegt die Hauptherausforderung in den Unternehmen darin, ihre Mitarbeiter*innen richtig zu diagnostizieren und Antworten auf die Fragen zu finden »Who is at risk from spear phishing? Why are they at risk? And how much of a risk are they?« Um diejenigen Mitarbeiter*innen zu selektieren, die am ehesten Opfer eines SH-Angriff werden könnten und dadurch das gesamte Unternehmen gefährden, entwickelten Vishwanath und seine Kolleg*innen den Cyber Risk Index (CRI). Der CRI ist eine Metrik zur Identifizierung von Risiko-Mitarbeiter*innen, in welcher individuelles Verhalten am Arbeitsplatz und darüber hinaus systematisch erfasst und nach festgelegten Kriterien bewertet wird. Als Selbsttest konzipiert umfasst der CRI 40 Fragen zu individuellen Gewohnheiten und Arbeitsroutinen (z.B. SMS schreiben während des Autofahren und damit zusammenhängende Unaufmerksamkeit gegenüber möglichen betrügerischen Nachrichten), heuristischem Denken (z.B. ob ein fehlenden Buchstaben wie das »s« auf einer gefälschten Starbucks-website bemerkt wird), persönlichen Einstellungen zu Cyber-Risiken (z.B. die Annahme, Microsoft Word sei sicherer als PDF) sowie die nicht näher spezifizierte Kategorie »Persönlichkeit«. Obwohl man erwarten könnte, dass Geschlecht, Alter, kultureller Hintergrund oder der Status in der internen Hierarchie der Institution bei dieser Risikobewertung eine Rolle spielen, sind diese sozialen Kategorien laut Vishwanath sowie den meisten unserer Interviewpartner*innen irrelevant. Im Gegenteil, viele bewerten diese sozialen Kategorien als unerheblich für die Wahrscheinlichkeit, ein Opfer von SH zu werden.

Nach dem Ausfüllen des Formulars werden die Mitarbeitenden anhand ihrer individuellen Antworten bewertet, wobei ihre Punktzahl die Entscheidungsgrundlage dafür bildet, ob sie weiterhin Zugang zu den sicherheitsrelevanten Netzwerken des Unternehmens erhalten. Die Grundidee des CRI besteht darin, Unternehmen die Möglichkeit zu geben, vermeintlich risikoreiche Mitarbeiter*innen zu identifizieren und ggf. nicht mit sicherheitsrelevanten Aufgaben zu betrauen und ihren Zugang zu sensiblen Daten einzuschränken und so Präventionsmaßnahmen treffen zu können. Um die Auseinandersetzung von Mitarbeiter*innen mit dem Thema SH und seinen Risiken zu erhöhen, empfehlen Vishwanath schlechte CRI Ergebnisse firmenintern zu veröffentlichen und ein-

zelne Mitarbeiter*innen als »Sicherheitsrisiko« bloßzustellen. Diese – durchaus zweifelhafte – Praxis deckt sich größtenteils mit den vorherrschenden Ansichten, die uns während der *Black Hat* Konferenz mitgeteilt wurden, nämlich »the need to identify the weak-links in the organization«, »to track and improve individual readiness and cyber-attack resilience«, oder sogar der Aufruf, »stupid people should be embarrassed and eventually fired« (IV 3, 6).

Auch in diesem Kontext zeigt sich wieder die medizinische Rhetorik des Diskurses: Vishwanath vergleicht SH mit einer sich ausbreitenden Epidemie. Dabei konstruiert er die Nutzer*innen als Patient*innen, welche schlichtweg einer genaueren Diagnose bedürfen, um sie selbst und ihre Umgebung vor möglichen Bedrohungen schützen zu können und deren Symptomatik die Unfähigkeit sei, verantwortungs- und risikobewusst zu agieren. Der hier verwendete Vergleich mit Patient*innen steht stellvertretend für einen prominenten Teil des SH-Diskurses (und einer damit verbundenen Schulungs- und Softwareindustrie), der verstärkt das Prinzip der »Cyberhygiene« propagiert. »Cyberhygiene« soll, analog der Krankheitsprävention in medizinischen Bereichen, dazu beitragen, Hacker*innen und deren Computerviren aus den IT-Systemen fernhalten. In dieser Rhetorik werden Unternehmen dazu angehalten, solch prophylaktische Maßnahmen zu ergreifen und zu forcieren. Diese medizinische Metaphorik untermauert das fortlaufende Narrativ von Individuen als primäres Sicherheitsrisiko in »gefährlichen« digitalen Räumen, in denen »cyber insecurities« generiert werden »by individuals who behave irresponsibly thus compromising the health of the whole« (Hansen und Nissenbaum 2009: 1166).

Maßnahmen der Cyber-Hygiene wurden auch in den Interviews mit Mitarbeiter*innen im Banken- und Gesundheitswesen angesprochen, die beide regelmäßig ähnliche Tests wie den CRI machen müssen. Dabei zeigte sich ein auf verschiedenen Ebenen problematisches Bild der standardisierten und vermeintlich objektiven Werkzeuge der SH-Prävention. Zum einen fühlten sich die Mitarbeiter*innen trotz ausgeprägter IT-Kompetenz von ihren Unternehmen auf die jährlich stattfindenden Tests schlecht vorbereitet: Ein Mitarbeiter schilderte, dass die Tests »eher so in Eigenregie« konzipiert wurden, es wurde demnach »vorher nicht erwähnt oder erprobt, was richtig wäre. Wir wussten nichts über den Aufwand, hatten keine Vorbereitung. Aber es musste halt irgendwie bestanden werden, das auf jeden Fall.« Der Aufwand der Maßnahmen wurde zudem als sehr hoch eingestuft: »Das hat schon lange gedauert, die ganzen Fragen […] da hat man dann einfach oft geraten« (IV 12). »Manche Szenarien waren so kompliziert […] das war eine Kette, da konnte ich nicht drüber nachdenken, da hatte ich gar keine Zeit für und dann war meine Antwort falsch« (IV 13).

Auch wenn solche SH-Tests in Unternehmen sehr unterschiedlich gehandhabt werden, bergen die Ergebnisse in den meisten Fällen Konfliktpotential für Unternehmensführung und Mitarbeiter*innen während gleichzeitig eine genaue Umset-

zung aller verordneten Sicherheitspraktiken durch die Mitarbeitenden unmöglich scheint. Bei einem der befragten Mitarbeiter wurde das Testergebnis an die Führungskraft gemeldet: Das »war schon ein bisschen peinlich […] wenn man das nicht geschafft hat. Aber das war so viel, man hatte keine Zeit dafür oder irgendeine Diskussion davor« (IV 12). Selbst, wenn sämtliche erforderlichen Verhaltensweisen bekannt sind, können Mitarbeitende diese in ihrem Unternehmen unter Umständen nicht umsetzen. Dies wurde ebenfalls in einem unserer Mitarbeiter-Interviews am Beispiel der Verarbeitung sensibler Daten deutlich. Mit Blick auf die Frage, wie solche Daten ohne den potentiellen Einblick Dritter verarbeitet werden können, zeigten sich unter anderem Schwierigkeiten in Bezug auf die Arbeitsplatz-Situation: »Bei uns geht das ganz einfach [, dass jemand Zugang bekommt], der Raum ist klein, wir sitzen zu eng zusammen. Eine Führungskraft schaut sicher dreimal die Stunde auf deinen Screen, trotz Schonern [Blickwinkelschutz], die werden einfach hintergangen« (IV 13).

Unsere empirischen Erkenntnisse verdeutlichen wie im Rahmen von SH-Expertendiskursen das Bild des bzw. der »defizitären Nutzer*in« als primäres Risiko für die IT-Sicherheit gezeichnet wird, welchem durch einen etablierten Wissensbestand zu Diagnose- und Abhilfemaßnahmen begegnet werden soll. Im folgenden Abschnitt diskutieren wir, wie eine alternative Konzeptualisierung aussehen könnte.

Der Weg zu einer Kultur der Vulnerabilität

In unserem Beitrag haben wir gezeigt, wie Expert*innen systematisches SH-Wissen samt entsprechender Gegenmaßnahmen entwickeln und Unternehmen als Dienstleistung anbieten. Als Kern dieses SH-Diskurses beobachten wir die Konstruktion eines bzw. einer »defizitären Nutzer*in«, welche*r aufgrund von Emotionen und erlernten Verhaltensmuster nicht in der Lage ist, den zunehmenden Anforderungen an die eigene IT-Sicherheitskompetenz gerecht zu werden. Schwachstellen, die jedem technologischen System inhärent sind, werden dabei zunehmend dem oder der Benutzer*in zugeschrieben, welche*r wiederum als das »schwächste Glied« in der Kette und potenziell größte Sicherheitsbedrohung dargestellt wird. Diese spezielle Form der Defizitkonstruktion ähnelt sehr stark dem, was die Sicherheitsforschung als Versicherheitlichung (*securitization*) bezeichnet (Balzacq 2005; McDonald 2008), d.h. dem Prozess, in dem etwas oder jemand kollektiv als Bedrohung konstruiert wird. Im Kontext des SH-Diskurses in der IT-Sicherheit wird das Individuum als unfreiwilliger Hauptrisikofaktor und gleichzeitig als Verantwortlicher für die kollektive Sicherheit dargestellt. Desweiteren führt die Identifizierung bestimmter Defizite, ähnlich wie in der klassischen Wissenschaftskommunikation, zu simplifizierenden Forderungen

nach mehr Aufklärung für die Bürger*innen oder, wie in unserem Fall, nach mehr »Cyberhygiene« und Schulungen zu »Cyberselbstverteidigung« für Mitarbeitende.

Wir haben gezeigt, dass die in SH-Diskursen konstruierte Sicherheitsbedrohung die Benutzer*innen (und nicht die Angreifer*innen) als Gefahrenquelle identifiziert und zur Entstehung einer Branche von Beratungsfirmen geführt hat, welche ein starkes Eigeninteresse daran hat, dieses Narrativ aufrecht zu erhalten. Dabei wird primär auf das Individuum fokussiert und dessen als »falsches« oder »dummes« definiertes Verhalten. Wir verstehen dies als eine Form der doppelten Absicherung epistemischer Autorität: Erstens wird ein Defizit konstruiert (auf Seiten der Benutzer*innen), dem mittels Expert*innen und Schulungen abgeholfen werden soll – anstelle denkbarer Alternativen wie etwa der Neugestaltung von Arbeitsroutinen, die Mitarbeitenden beispielsweise mehr Zeit zur Prüfung der Vertrauenswürdigkeit eines Links oder Anrufs einräumen. Zweitens liegt dem SH-Diskurs das fortlaufend forcierte Narrativ einer immanenten und unvermeidbaren Bedrohung zugrunde. Dieses Narrativ suggeriert zwar, dass nicht alle Mitarbeiter*innen effektiv geschult werden können und zudem Angreifende in der Lage seien immer neue Wege zu entwickeln, um selbst die am besten geschulten Benutzer*innen zu täuschen. Da Risiken in diesem Defizitframing jedoch nur individuell konzipiert und daher auch nur individuell adressiert werden, bleibt das Mittel der Wahl dennoch als risikoreich verstandene Benutzer*innen zu identifizieren, analysieren und quantifizieren. SH-Schulungen suggerieren allen Beteiligten, dass Mitarbeitende mit dem richtigen Training zu verantwortlichen Hüter*innen der Unternehmenssicherheit ausgebildet werden können – obwohl diese paradoxerweise zeitgleich als unkontrollierbares Risiko dargestellt werden.

Als Alternative zu dieser Art von dramatisiertem Sicherheitsdenken (Hansen und Nissenbaum 2009) und hartnäckiger Defizitkonstruktion bei der Risikoanalyse von IT-Systemen schlagen wir vor, den Zusammenhang zwischen technischen und menschlichen »Schwachstellen« von der Vorstellung »socio-technical vulnerability« (Bijker 2006; Hommels et al. 2014) ausgehend zu denken. Dieser Begriff wurde von STS-Forschenden als Antwort auf die anhaltende Debatte über die »Risikogesellschaft« (Beck 1992) eingeführt. Bijker et al. begreifen Vulnerabilität »as an emergent system's property« [that] »should not be considered as given, intrinsic, and essential, nor as purely negative« (Bijker u.a. 2014: 6). Stattdessen sei Vulnerabilität »natural, sociocultural, and technical,« [as it] »relates to the unit of analysis, as well as to its environment« (ibid. 7). Eine konventionelle Risikobewertung betrachtet Daten und objektivierbare Zusammenhänge, statistische Korrelationen und daraus modellierbare Szenarien in einem vordefinierten System, beispielsweise der Gesamtheit aller IT-Sicherheitsvorkehrungen eines Unternehmens.

> »Vulnerability, however, cannot be analyzed by looking *only* at the inside of a system. It also relates to that system's environment. The same person, clad in many

> layers of wool, can be invulnerable up in the Himalayas but vulnerable in Hyderabad, India. A characterization of a system's vulnerability thus requires attention to its environment, including the risks that it runs as well as the resources that it may draw upon.« (Bijker u.a. 2014: 6, Hervorhebung Original)

Drei Aspekte des Konzepts der socio-technical vulnerability sind für den Kontext der IT-Sicherheit im Allgemeinen und SH im Besonderen von Bedeutung: Erstens ist die sozio-technische Vulnerabilität zu einem allgegenwärtigen Merkmal der heutigen Welt geworden. Mit ihrer Durchdringung des Alltagslebens haben digitale Systeme Schnittstellen zwischen praktisch allen Bereichen sozialer Beziehungen und den jeweiligen kritischen Infrastrukturen geschaffen (Graham und Thrift 2007). Während Menschen auch zuvor auf das Funktionieren technischer Infrastrukturen wie Elektrizität angewiesen waren und diese ebenfalls verwundbar waren, konnten Störungen nur durch physische Eingriffe verursacht werden (Neuman 2006). Der Erfolg des Internets und zunehmend des »Internets der Dinge« hat über die rein physische Anfälligkeit hinaus jeden Teil dieses Netzwerks – Geräte, Menschen und Organisationen gleichermaßen – für potenzielle Störungen angreifbar gemacht (Slayton und Clark-Ginsberg 2018). Zweitens sind diese Schwachstellen ambivalent: Eine Bank kann beispielsweise als besonders verwundbar angesehen werden, da sie ein hohes Volumen an finanziellen Vermögenswerten und Transaktionen verwaltet. Alternativ kann sie jedoch auch als besonders sicher verstanden werden, da Banken oftmals große IT-Sicherheitsabteilungen beschäftigen und so schneller als andere Unternehmen auf potenzielle Bedrohungen reagieren können. In jedem Fall ist das, was Vulnerabilität ausmacht, flexibel, kontextabhängig und interpretationsbedürftig. Drittens ist Vulnerabilität nicht generell negativ. Wie Bijker et al. (2014: 1) argumentieren:

> »A certain degree of vulnerability is necessary to create space for learning and adaptation in a society. Vulnerability, in this sense, is equivalent to openness and flexibility. Once properly addressed, such vulnerability with accompanying coping mechanisms may yield a more flexible and resilient society than one that tries to avoid all vulnerabilities«. (Bijker et al. 2014: 1)

Somit hilft Vulnerabilität als sensibilisierende Perspektive in ihrer praktischen Anwendung den artikulierten Defizitdiagnosen der Security-Expert*innen auf einer anderen Ebene zu begegnen. Es geht nicht mehr um die Optimierung von Systemen – zu denen eben auch Menschen gehören – durch die Mehrung und bessere Anwendung von instrumentellem Wissen. Stattdessen wird kollektive Sicherheit als lebensweltlich eingebettete Wertdimension verstanden – eine unter vielen. Mehr noch lässt sich hinterfragen, ob Sicherheit als Streben nach maximaler Kontrolle von Menschen und ihrer soziomateriellen Umwelt überhaupt als erstre-

benswertem Zustand gelten kann, in welchen Fällen Sicherheit auf Kosten anderer Werte priorisiert werden darf und wer über diese Werteordnung entscheidet.

Schluss

In diesem Beitrag haben wir aufgezeigt, wie IT-Sicherheitsexpert*innen SH als ein schnell wachsendes und potenziell katastrophales Risiko für Unternehmen und andere Organisationen darstellen. Hierbei wurden die Mitarbeitenden diskursiv als »schwächstes Glied« in der Sicherheitsarchitektur von Unternehmen markiert. Derartige Defizitdiagnosen bilden den Grundstein für einen Expertendiskurs sowie eine daran anschließende Beratungsindustrie, die Abhilfe für das verspricht, was unsere Interviewpartner*innen bzw. SH-Expert*innen als die »unachtsamen« oder »dummen« Mitarbeitenden dargestellt haben. Als erfolgreiche Schutzmaßnahmen werden dabei eine verstärkte »Cyberhygiene« sowie Schulungen zur »Cyberselbstverteidigung« empfohlen. Wir wollen mit diesem Beitrag nicht in Abrede stellen, dass derartige Maßnahmen für die IT-Sicherheit eines Unternehmens gewinnbringend sein können. Wir möchten jedoch verdeutlichen, welche performativen Auswirkungen die damit einhergehenden Diskurse haben können, in welchen die Mitarbeitenden und nicht die Angreifer*innen als das primäre Problem konstruiert werden – nicht zuletzt auch als Anstoß für eine gesamtgesellschaftliche Betrachtung der Problematik jenseits von IT-Sicherheitsabteilungen und Managementkreisen.

In unserer Analyse haben wir die Verlagerung der Verantwortung für ein kollektives Problem auf die einzelnen Mitarbeiter*innen beobachtet. Diese Verschiebung spiegelt einen allgemeinen Trend zur Flexibilisierung von Arbeitsumgebungen wider, welche den Arbeitnehmer*innen mehr Autonomie, aber auch Verantwortung bei der Selbstverwaltung ihrer eigenen Produktivität einräumt (Sennett 2007; Boltanski und Chiapello 2005). Aus dieser Perspektive haben Innovationen am Arbeitsplatz, wie z.B. das Home-Office oder *Bring your own device*-Reglungen, die Barriere zwischen dem sozio-technischen Rahmen des zu schützenden Unternehmens und dem oft anfälligeren privaten Umfeld seiner Mitarbeiter*innen zunehmend durchlässiger gemacht. SH-Schulungen problematisieren das Individuum als Risiko, thematisieren aber selten die Tatsache, dass einige Unternehmen bewusst die Grenzen zwischen Arbeit und Privatleben verwischen und damit einen wesentlichen Teil des Problemkontextes überhaupt erst schaffen.

Mit Verweis auf die Literatur in den STS zu Vulnerabilität in technologischen Kulturen haben wir argumentiert, dass die Lösungen für mehr IT-Sicherheit nicht in immer neuen Formen der ausgelagerten Risikobeherrschung liegen können, die das Individuum pathologisieren. Als Alternative zu dieser Sichtweise sollten Führungskräfte von Unternehmen, Regierungen und IT-Sicherheitsabteilungen stär-

ker auf institutionelle Aspekte der IT-Sicherheit fokussieren und dabei auf die zunehmenden Unsicherheiten und unbeabsichtigten Konsequenzen achten, welche durch die Digitalisierung der Arbeitswelt entstehen. Auch wenn aus der Sicht von SH-Expert*innen der Mensch das »schwächste Glied« darstellt, wäre es nachhaltiger, eine Balance zu finden zwischen diskursiver Versicherheitlichung, und einer symmetrischen Betrachtung der sozio-technischen Vulnerabilität, die gesellschaftliche Werte und die potenzielle Produktivität von Risiken hervorhebt. Andernfalls laufen IT-Verantwortliche – und letztlich die Gesellschaft – Gefahr, die Verantwortung bei den Opfern statt bei den Täter*innen zu suchen. Wir hoffen daher, dass unsere Analyse nicht nur einen empirischen Beitrag in den Sozialwissenschaften leistet, sondern auch politische Diskurse stimuliert, indem er aufzeigt, wie Konfigurationen von Sicherheit und Arbeitswelt neuartige sozio-technische Defizite konstituieren und Fragen von Risiko und Sicherheit aus der Perspektive der sozio-technischen Vulnerabilität angegangen werden können.

Literatur

Abraham, S. and Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society* 32(3): 183-196.

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations* 11(2): 171-201.

Beck, U. (1992). *Risk society: Towards a new modernity*, vol. 17. London: Sage.

Bijker, W. E., Hommels, A. M. and Mesman, J. (2014. *Vulnerability in Technological Cultures. New Directions in Research and Governance*. Cambridge: MIT Press.

Bijker, W. E. (2006). The vulnerability of technological culture. In *Cultures of Technology and the Quest for Innovation*, ed. H. Nowotny, 52-70. New York: Berghahn Books.

Bodmer, W. and Wilkins, J. (1992). Research to improve public understanding programmes. *Public Understanding of Science* 1(1): 7-10.

Bybee, R. W. (1997). *Achieving scientific literacy: from purposes to practices*. Portsmouth: Heinemann.

Campbell, L. M., Corson, C., Gray, N. J., MacDonald, K. I. and Brosius, J. P. (2014). Studying Global Environmental Meetings to Understand Global Environmental Governance: Collaborative Event Ethnography at the Tenth Conference of the Parties to the Convention on Biological Diversity. *Global Environmental Politics* 14(3): 1-20.

Coleman, E. G. (2012). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Graham, S. and Thrift, N. (2007). Out of Order: Understanding Repair and Maintenance. *Theory, Culture & Society* 24(3): 1-25.

Grand View Research (2020). *Cyber Security Market Size*. https://www.grandviewresearch.com/industry-analysis/cyber-security-market. Zugegriffen: 05.07.2021.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Indianapolis: Wiley.

Hajer, M. A. (2003). Argumentative Diskursanalyse. Auf der Suche nach Koalitionen, Praktiken und Bedeutung. In *Handbuch Sozialwissenschaftliche Diskursanalyse*, hg. R. Keller, A. Hirseland, W. Schneider und W. Viehöver, 271-298. Wiesbaden: VS Verlag für Sozialwissenschaften.

Hajer, M. A. (2009). *Authoritative governance: policy-making in the age of mediatization*. Oxford: Oxford University Press.

Hajer, M. A. (2005). Setting the Stage: A Dramaturgy of Policy Deliberation. *Administration & Society* 36(6): 624-647.

Hansen, L. and Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53(4): 1155-1175.

Harper, D. (1998). An argument for visual sociology. In *Image-based research: A sourcebook for qualitative researchers*, ed. J. Prosser, 24-41. London: Falmer Press.

Hommels, A., Mesman, J. and Bijker, W. E., eds. (2014). *Vulnerability in technological cultures: new directions in research and governance*. Cambridge, Massachusetts: MIT Press.

Honan, Mat (2014). *Social Engineering Always Wins: An Epic Hack, Revisited*. Wired. https://www.wired.com/2014/01/my-epic-hack-revisited/. Zugegriffen: 21. Dezember 2020.

Høyer Leivestad, H. and Nyqvist, A., eds. (2017). *Ethnographies of Conferences and Trade Fairs: Shaping Industries, Creating Professionals*, 1st ed. Cham: Palgrave Macmillan.

Hulme, G. (2015). *The 2015 Social Engineering Survival Guide What you need to know to keep your enterprise secure from social engineering exploits*. CSO online. https://www.csoonline.com/article/2864598/the-2015-social-engineering-survival-guide.html. Zugegriffen: 05.07.2021.

Irwin, A. (2014). From deficit to democracy (re-visited). *Public Understanding of Science* 23(1): 71-76.

Jasanoff, S. (2016). A Century of Reason: Experts and Citizens in the Administrative State. In *The Progressives‹ Century: Political Reform, Constitutional Government, and the Modern American State*, eds. S. Skowronek, S. M. Engel, and B. Ackerman, 382-404. New Haven: Yale University Press.

Jasanoff, S. (2015). Future Imperfect: Science, Technology, and the Imaginations of Modernity. In *Dreamscapes of Modernity*, eds. S. Jasanoff and S.-H. Kim, 1-33. Chicago; London: The University of Chicago Press.

Jasanoff, S. (2004). The idiom of co-production. In *States of knowledge. The co-production of science and the social order*, ed. S. Jasanoff, 1-12. London: Routledge.

Kaspersky (2019). *Nine-in-Ten Data Breaches in the Cloud Caused by Social Engineering, Finds Kaspersky Lab*. Kaspersky. https://usa.kaspersky.com/about/press-release

s/2019_nine-in-ten-data-breaches-in-the-cloud-caused-by-social-engineering-finds-kaspersky-lab. Zugegriffen: 18. Dezember 2020.

Klimburg, A. (2017). *The Darkening Web: the war for cyberspace*. New York: Penguin Press.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications* 22: 113-122.

Little, P. D. and Painter, M. (1995). Discourse, Politics, and the Development Process: Reflections on Escobar's« Anthropology and the Development Encounter«. *American Ethnologist* 22(3): 602-609.

Long, J., TotalBoox and TBX (2011). *No Tech Hacking*. Elsevier Science. www.totalboox.com/book/id-8741216558554326771. Zugegriffen: 26. Dezember 2020.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations* 14(4): 563-587.

Morozov, E. 2013. *To save everything, click here.*, 1st ed. New York: Public Affairs.

Neuman, M. (2006). Infiltrating infrastructures: On the nature of networked infrastructure. *Journal of Urban Technology* 13(1): 3-31.

Pfotenhauer, S. and Jasanoff, S. (2017). Panacea or diagnosis? Imaginaries of innovation and the ›MIT model‹ in three political cultures. *Social Studies of Science* 47(6): 783-810.

Pfotenhauer, S. M., Juhl, J. and Aarden, E. (2019). Challenging the »deficit model« of innovation: Framing policy issues under the innovation imperative. *Research Policy* 48(4): 895-904.

PurpleSec (2020). *2019 Cyber Security Statistics Trends & Data*. PurpleSec. https://purplesec.us/resources/cyber-security-statistics/. Zugegriffen: 18. Dezember 2020.

Sismondo, S. (2010). *An introduction to science and technology studies*, 2nd ed. Chichester, West Sussex, U.K.; Malden, MA: Wiley-Blackwell.

Slayton, R. and Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection: Beyond regulatory capture. *Regulation & Governance* 12(1): 115-130.

Stilgoe, J., Lock, S. J. and Wilsdon, J. (2014). Why should we promote public engagement with science? *Public Understanding of Science* 23(1): 4-15.

Thomas, D. (2002). *Hacker culture*. Minneapolis: University of Minnesota Press.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security* 16(6): 315-331.

Wynne, B. (1992). Misunderstood misunderstanding: social identities and public uptake of science. *Public Understanding of Science* 1(3): 281-304.

Wynne, B. (2006). Public Engagement as a Means of Restoring Public Trust in Science – Hitting the Notes, but Missing the Music? *Public Health Genomics* 9(3): 211-220.