Inhalt

Einleitung

Es ist viel zu einfach

Im Herbst 2019 habe ich den IT-Sicherheitsberater des früheren US-Präsidenten Barack Obama gehackt. Damals wurde mir klar, dass die Welt dieses Buch braucht. Denn es war viel zu einfach.

Es war ein Auftragshack – und der Auftrag kam vom Opfer selbst: Eric Rosenbach, dem sogenannten Cyberzar. Unter der offiziellen Rollenbezeichnung Deputy Assistant Secretary of Defense for Cyber verantwortete er von 2011 bis 2014 die Cyberstrategie des US-Verteidigungsministeriums, von 2014 bis 2017 war er Stabschef des Pentagon. Rosenbach begleitete in dieser Zeit alle wesentlichen Entwicklungen, die den Cyberraum betreffen, und mit seinem Team gelang es ihm, allerlei Attacken teils oder vollständig abzuwenden oder zumindest im Nachhinein zu analysieren. Das waren in diesen Jahren gleich eine ganze Reihe – von Chinas Diebstahl geistigen Eigentums großer US-Unternehmen durch Spähangriffe über iranische und nordkoreanische Cyberangriffe auf kritische Infrastrukturen bis zu den immer massiveren Versuchen des russischen Geheimdiensts, sich mithilfe von Hacking-Angriffen und der Verbreitung von Falschnachrichten in die US-Politik einzumischen.

2019 erhalte ich also die Aufgabe Rosenbachs, ihm eine Spear-Phishing-E-Mail zu schreiben. Das sind sehr gezielte, auf eine Person zugeschnittene E-Mails mit dem Ziel, die Angeschriebenen dazu zu bewegen, einen schädlichen Anhang anzuklicken. Tun sie das, breitet sich ein Virus auf ihrem Computer aus, der sie wahlweise ausspioniert und Daten klaut oder alles verschlüsselt – oder gleich beides.

Eric Rosenbach unterrichtet heute Cybersecurity als Direktor des Belfer Centers an der Harvard Kennedy School. Die Phishing-E-Mail ist eine Hausaufgabe in einem Intensivseminar in Harvard, das ich zu dieser Zeit zweimal in der Woche besuche: »Cyber and Info Ops: War, Peace and the Space Between«, so lautet der Name des Seminars, der mich besonders anspricht, weil ich mich genau dafür interessiere: für Krieg, Frieden – und alles, was dazwischen in der Cyberwelt existiert. Ich bin keine reguläre Studierende, sondern habe ein Fellowship für Wissenschaftsjournalismus am MIT. Deshalb muss ich Rosenbach erst überzeugen, dass ich als Stipendiatin an seinem Seminar teilnehmen darf. »Sie müssen aber die gesamte Arbeit machen«, schreibt er mir drohend. Die Arbeit – das ist alles, was er von den ehrgeizigen Midcareer-Fellows, die mit mir an dem Seminar in Harvard teilnehmen, auch erwartet. Für mich klingt das spannend, und ich sage zu – was tatsächlich einen Berg Arbeit nach sich zieht: schier endlos lange Leselisten zur Vorbereitung jedes Termins etwa, deren Inhalt er ohne Vorwarnung vor der ganzen Klasse abfragt. Ein mehrtägiges Bootcamp mit technischen Inhalten. Gleich mehrere Quize und zu verfassende Politik-Strategiepapiere. Spontane »On the spot briefings«, bei denen wir die Rolle der Beteiligten eines Cybervorfalls einnehmen und ein Statement abgeben müssen, und vor allem Simulationen: realistisch nachempfundene Rollenspiele aus dem Verteidigungsministerium, in denen Rosenbach meist den US-Präsidenten spielt, den wir beraten müssen.

Es gibt sonst im Leben wohl kaum eine Gelegenheit, sich so intensiv, dicht gepackt und umfassend damit zu beschäftigen, was im digitalen Raum geschieht, welcher massive Schaden durch Cyberangriffe entsteht, wie gefährlich das Zeitalter der Cyberwars ist – und vor allem: wie angreifbar wir sind. Wir alle. Nicht die USA, sondern die Gesellschaft, die Welt.

Seither habe ich nicht aufhören können, in diesem Themenbereich zu recherchieren, und das Bild wird immer umfassender.

Neue Perspektiven kommen hinzu, bei manchen Themen gibt es unterschiedliche Einschätzungen, aber eines bleibt – meine Gewissheit: Wer sich die großen Cyberangriffe der vergangenen Jahre und die aktuelle Entwicklung anschaut, sieht, dass wir handeln müssen. Und damit meine ich nicht nur die Regierungschefs und Sicherheitsberater.

Wie sehr das jeden Einzelnen von uns betrifft, wird mir klar bei der Aufgabe, die Spear-Phishing-E-Mail an Rosenbach zu schreiben. Ich recherchiere eine Nacht lang über Rosenbach und bin erstaunt, wie viel Privates ich nach dieser Zeit schon über ihn weiß, wie viele potenzielle Angriffsmöglichkeiten sich auftun.

Für die E-Mail bekomme ich ein A, die Bestnote nach dem US-Notensystem. Das bedeutet, erklärt mir Rosenbach, dass er meine E-Mail für vertrauenswürdig gehalten hat: Wäre es eine echte Phishing-Mail gewesen, hätte er sich mit ihr einen Virus eingefangen.

Wenn es so einfach ist, einem problembewussten Menschen wie Rosenbach eine schädliche E-Mail unterzujubeln: Wie können wir uns dann überhaupt schützen? Mir wurde in dem Seminar damals plötzlich bewusst, wie viele Anhänge ich schon geöffnet hatte, weil die zugehörige E-Mail absolut vertrauenswürdig klang. Ob eine E-Mail das wirklich ist, lässt sich nur schwer überprüfen. Es muss sich nur jemand wie ich einen Tag Zeit nehmen und ein bisschen im Internet recherchieren – genau so, wie ich es mit Rosenbach getan habe. Und schon kann man eine persönliche, vertrauenswürdige E-Mail schreiben, die von den meisten Menschen arglos geöffnet würde. Die Absenderadresse zu fälschen, ist eine leichte Übung. Entsprechende Schadsoftware im Internet zu kaufen, braucht auch nur wenig Rechercheleistung. Und fertig ist der Angriff.

Die meisten Phishing-Attacken werden mit noch viel weniger Aufwand durchgeführt. Die meisten sind nicht persönlich, sondern es genügen vielfach verwendete Textbausteine – und trotz-

dem sind sie erfolgreich. Die Masse macht es. Wer genug solcher E-Mails hinaus in die Welt schickt, erwischt immer mal wieder eine leichtgläubige Person. Sobald es um größere Geldsummen geht, lohnt es sich, etwas Aufwand zu investieren und den Angriff maßzuschneidern. Das ist dann eine ziemlich lukrative Investition, wenn man bedenkt, welche Summen Unternehmen bezahlen, um ihre verschlüsselten Daten zurückzubekommen. Es gibt heute tatsächlich nur wenige effizientere Investitionen als die in Schadsoftware. Und der Schaden für uns alle ist immens.

Es braucht nur einen falschen Klick.

Wie geht es wohl dem Mitarbeiter oder der Mitarbeiterin, der oder die durch einen unbedachten Klick Kriminelle ins Unternehmensnetzwerk lässt und damit einen Millionenschaden auslöst? Das frage ich mich ganz aktuell im Februar 2022, als ich aus der Managementetage des Osnabrücker Logistikunternehmens Hellmann drei Etagen weit hinunterschaue auf den großen Vorplatz, auf dem es wie in einem Ameisenhaufen wimmelt. Dort rangieren riesige Lastwagen des Unternehmens, die Tag für Tag unzählige Güter durch die Republik fahren, auf die an ganz verschiedenen Adressen jemand wartet. Nur wenige Wochen zuvor hat hier tatsächlich alles anders ausgesehen. Die hektische Betriebsamkeit wurde jäh unterbrochen, als Hellmann kurz vor Weihnachten 2021 Opfer eines Cyberangriffs wurde. Das Unternehmen mit weltweit knapp 11 000 Beschäftigten und einem Jahresumsatz von 2,5 Milliarden Euro ging von einer Sekunde zur anderen und ohne jede Vorwarnung offline.

In diesem Fall floss kein Lösegeld, weil der Konzern den Angriff frühzeitig bemerkte – das heißt, er wurde entdeckt, bevor die Kriminellen die Daten verschlüsseln konnten. Dennoch war der Schaden enorm, schließlich war das Unternehmen einige Tage kaum handlungsfähig – und das im Weihnachtsgeschäft. Zudem standen einige Wochen später mehrere Gigabyte interne Daten

im Darknet, die für Kriminelle ebenso interessant sind wie für die internationale Konkurrenz.

Durch die Veröffentlichung der Daten wurde ich auf den Hack aufmerksam und konnte Hellmann schließlich überzeugen, mich für eine Reportage für die Wochenzeitung *Die Zeit* zu empfangen. Einfach war das nicht, die meisten Unternehmen haben große Angst, über Angriffe zu sprechen. Die öffentliche Schmach, aber auch Sorge davor, Kriminelle erst recht herauszufordern, lassen sie vor dem Schritt an die Öffentlichkeit zurückschrecken.

Aber wenn Cyberangriffe ein Tabu sind, bleiben wir für immer angreifbar. Auch im Kleinen begegnet mir oft diese Haltung: »Ich will das lieber nicht so genau wissen, ich verstehe das sowieso nicht –, und mich wird es schon nicht treffen.« Leider trifft es immer unvorbereitet, wenn man sich nicht vorbereitet. Genau diese Menschen rufen mich dann an: »Eva, ich habe da so eine E-Mail angeklickt, die klang schon ein bisschen komisch. Was soll ich denn jetzt tun?«

Allein in meinem persönlichen Umfeld hat es innerhalb eines Jahres mehrere Privatpersonen getroffen, die sich über E-Mails schädliche Viren einfingen oder auf Fake-Nachrichten hereinfielen, sowie zwei mittelständische Unternehmen, die fünf- bis sechsstellige Summen an Geld verloren haben.

Bei Hellmann sind die Kosten vermutlich deutlich höher, aber auch dieses Opfer eines Hackerangriffs ist nur eines von vielen: Der deutschen Wirtschaft entsteht laut einer Studie des Digitalverbands Bitkom ein jährlicher Schaden von rund 203 Milliarden Euro durch Cyberattacken. Es trifft die Mehrheit aller Unternehmen, rund 84 Prozent berichteten entsprechende Angriffe.

Ich habe für dieses Buch viele Recherchereisen gemacht – reale Reisen nach Russland, in die Ukraine, nach Großbritannien, in die Niederlande und in die USA ebenso wie virtuelle Zeitreisen: Ich habe mich mit Sicherheitsforscher:innen in die Geschichte des Cyberwars und der Cyberkriminalität vertieft und diese in tage-

langen Gesprächen minutiös rekonstruiert. Es ist eine noch junge Geschichte, aber nicht minder ereignisreich. Ich habe für dieses Buch einige der größten und interessantesten Cybervorfälle der vergangenen Jahre ausgewählt und deren Spuren bis in die Gegenwart intensiv verfolgt. Ich habe Hacker:innen jeder Couleur getroffen, ich habe Opfer besucht und Sicherheitsforscher:innen bei ihrer unermüdlichen Detektivarbeit begleitet.

Das Ergebnis gliedert sich in vier Teile: Im ersten Teil begleite ich kriminelle Hacker, im zweiten Teil geht es um staatliches Hacking und den Beginn des Cyberwars, im dritten Teil zeige ich, wie der Cyberwar mit teils lebensgefährlichen Folgen für Unbeteiligte außer Kontrolle gerät, und im vierten Teil untersuche ich die Fragen, wieso wir so angreifbar sind und was wirklich hilft.

Wie ich werden auch Sie erstaunt und frustriert feststellen, dass die Unterscheidung zwischen kriminellen und staatlichen Angriffen nicht immer eindeutig ist, dass es Mischformen gibt, weil die einen von den anderen profitieren und umgekehrt. Das macht die Sache umso gefährlicher, denn eine Erkenntnis zieht sich durch die gesamte Geschichte der IT-Sicherheit: Auch vermeintlich »gutes«, staatliches Hacking im Kampf gegen Kriminelle schwächt in der Konsequenz die Sicherheit aller.

Was aber können wir tun? Wir müssen Sicherheitslücken schließen – im Großunternehmen wie am heimischen Schreibtisch –, und dazu müssen wir uns damit beschäftigen, wie und welche Lücken unsere Systeme für Angreifer:innen öffnen. Das tun wir in diesem Buch. Wir werden dabei auch organisatorische, ja sogar psychische »Lücken« aufdecken, denn das ist einer der Trends: Kriminelle und staatliche Hacker:innen nutzen unser Vertrauen aus. Sie werden staunen, was eine sogenannte Social-Engineering-Expertin – gewissermaßen eine Fachfrau im Überlisten und Hereinlegen – alles erreicht, ganz ohne Gewalt, ganz ohne Viren.

Mitten in die Schlussredaktion dieses Buches platzt ein Anrufer mit einer schrecklichen Nachricht: Er rufe von Europol an, auch

das FBI höre mit, sagt der Mann an meinem Handy, denn ich werde gesucht als Teil einer internationalen schwerkriminellen Bande. Er werde nun mein Bankkonto sperren, und auch mein Ausweis sei ab sofort nicht mehr gültig. In einem von mir angemieteten Fahrzeug sei vermutlich eine Gewalttat geschehen, es sei völlig verbeult und voller Blut am Stadtrand von Berlin gefunden worden, und über meine Konten werde Geldwäsche betrieben. Glücklicherweise scheint er mir aber zu glauben, dass ich mit alldem nichts zu tun habe, sondern dass offenbar jemand meine Daten erbeutet hat – nur wer? Er wolle mir helfen, sagt er. Zuallererst müsse ich den Behörden beweisen, dass mein Geld legalen Ursprungs sei. »Öffnen Sie Ihren Laptop und googeln Sie TeamViewer«, sagt er.

Sie ahnen schon, worauf es hinausläuft: Der Anrufer war ein krimineller Hacker. Er versuchte, mich zu überreden, ihn mit einem Programm auf meinen Computer einzuladen, damit er dort unter dem Vorwand, mir zu helfen, mein Konto leerräumen kann.

Natürlich tat ich das nicht, denn ich war nicht unvorbereitet. Stattdessen überlegte ich mir viele technische Ausreden, um den Anrufer auszutesten und zu sehen, was er auf Lager hat.

Ich muss gestehen: Ich war am Ende ziemlich beeindruckt, denn er hatte eine enorme Überzeugungskraft und auf alles eine Antwort. Ich wurde mehrmals weiterverbunden zu »Beamten« anderer Hierarchieebenen, die sich stets mit vollem Namen und Dienstnummer vorstellten und das »Good-Cop-Bad-Cop«-Spiel zur Vollendung spielten.

Ich bin nach der Recherche für dieses Buch natürlich kein geeignetes Opfer mehr für die Bande, doch mir wurde klar, dass sie viel investiert hatten und dass sich das vermutlich auszahlt. Und ich weiß aus erster Hand von einem Opfer, wie die Geschichte weitergeht, wenn man nicht vorbereitet ist: Im Zuge der Recherche habe ich eine junge Frau kennengelernt, die eine fünfstellige Summe an die Kriminellen verloren hat.

Wenn Sie sich jetzt fragen, wie das sein kann, lesen Sie bitte das Kapitel über Social Engineering: Es ist so aktuell wie der Anruf mitten in der Schlussphase meines Schreibprozesses. Daher gibt es in allen Bereichen dieses Buchs Hinweise auf aktuelle Entwicklungen: Eine Hackinggruppe des russischen Geheimdiensts, die sich eine ganze Zeit lang bedeckt gehalten oder im Verborgenen agiert hat und die für einige der gefährlichsten Cyberangriffe der Geschichte verantwortlich ist, ist im Zuge des russischen Angriffskriegs auf die Ukraine wieder aktiv und hat mit einer – glücklicherweise missglückten – Attacke auf ein Elektrizitätswerk gezeigt, dass sie nach wie vor eine große Gefahr darstellt – auch und gerade für westliche Infrastrukturen. Auch im Bereich der Entwicklung staatlicher Spionagesoftware und deren Missbrauchspotenzial überschlagen sich die Ereignisse: Unter anderem zeigen aktuelle Recherchen rund um die Spionagesoftware Pegasus, wie Nichtregierungsorganisationen, Journalist:innen und Oppositionelle in Diktaturen in den Fokus staatlicher Repression geraten. Cyberwaffen aus Europa helfen repressiven Regimes bei der Unterdrückung kritischer Stimmen – im Jahr 2021 war Deutschland Exportweltmeister von Spionagesoftware. Diese ging beinahe ausschließlich an nicht demokratische Regimes.

Auch die Kriminellen, die ich im ersten Teil begleitet habe, werden immer kreativer. Eine wachsende Zahl von Menschen verliert Geld, weil Kriminelle sich auf verschiedenen Wegen Zugang zu ihrem Bankkonto verschaffen. Beinahe täglich liest man von neuen Ransomware-Angriffen auf Unternehmen, die dabei Millionen verlieren. Auch hier gilt: ein falscher Klick genügt.

Als ich kurz vor Erscheinen dieses Buches auf Twitter fragte, was denn Wichtiges ins Vorwort solle, wurde mir geraten, Sie – liebe Leser:innen – im Stil von Walter Moers' *Stadt der Träumenden Bücher* zu warnen. Moers schreibt einleitend, es sei keine Geschichte »für Leute mit dünner Haut und schwachen Nerven – welchen ich auch gleich empfehlen möchte, dieses Buch wieder

zurückzulegen«[1]. In der Tat werden Sie sich möglicherweise auch bei der Lektüre meines Buchs gruseln, aber ich möchte Sie warnen: Es nicht zu lesen, könnte ebenfalls gefährlich sein. Denn Sie würden wertvolles Wissen verpassen, das Sie vor Cyberangriffen schützt. Im Gegensatz zu Walter Moers' Arbeit handelt es sich hier nämlich ausnahmslos um wahre Gegebenheiten. Vor diesen sollten Sie besser nicht die Augen verschließen.

1 Walter Moers, *Die Stadt der Träumenden Bücher: Ein Roman aus Zamonien von Hildegunst von Mythenmetz,* Piper Verlag, München 2007, S. 11.