Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Bern, 29. November 2023

Die Förderung des ethischen Hackings in der Schweiz

Bericht des Bundesrates in Erfüllung des Postulats 20.4594, Bellaiche, vom 17. Dezember 2020

Inhaltsverzeichnis

1 Einleitung

Cybersicherheit ist eine zentrale Herausforderung für die Sicherheit unserer Gesellschaft. Die Digitalisierung hat zu einer umfassenden Abhängigkeit der Wirtschaft, des Staats und der Bevölkerung von funktionierenden und sicheren Informations- und Kommunikationstechnologien (IKT) geführt. Viele Prozesse des täglichen Lebens wären ohne IKT nicht mehr umsetzbar, da diese verschiedene Anwendungen zu – für die Nutzer wichtigen – multifunktionalen Gesamtsystemen verbinden. Diese umfassenden IKT-Netzwerke bilden deshalb die Kerninfrastruktur für die Digitalisierung.
Charakteristisch für solche Systeme ist ihre Komplexität. Der Zusammenschluss von verschiedenen IKT-Anwendungen führt zu zahlreichen Schnittstellen und Interdependenzen, welche es schwierig machen, das Gesamtsystem umfassend zu überblicken. Die Programmiercodes von solchen Systemen umfassen oft mehrere Millionen von Zeilen. Es ist deshalb nicht erstaunlich, dass darin immer wieder Schwachstellen auftreten. Schwachstellen sind Eigenschaften des IKT-Systems, welche seine Sicherheit gefährden können. Typischerweise handelt es sich um Programmierfehler oder Fehlkonfigurationen, welche unbefugte Zugriffe auf die Systeme oder auf deren Daten ermöglichen. Viele Cyberangreifer nutzen solche Schwachstellen aus, um in die IKT-Systeme einzudringen und gefährden damit ihre Sicherheit.
Für die Cybersicherheit ist es entscheidend, dass alles unternommen wird, um die Risiken von Schwachstellen in IKT-Systemen zu minimieren. Sicherheit muss bei der Entwicklung und beim Betrieb von Hard- und Software höchste Priorität erhalten. Sehr wichtig ist, dass die Systeme laufend auf allfällige Schwachstellen geprüft werden. Nur so können diese bei komplexen IKT-Systemen frühzeitig erkannt und behoben werden, bevor Angreifer sie ausnutzen.
Es gehört zu den Kernaufgaben der Cybersicherheit, aktiv nach Schwachstellen zu suchen und diese so zu beschreiben sowie zu bewerten, dass einerseits eine Risikoabschätzung möglich ist und anderseits Gegenmassnahmen ergriffen werden können, um diese Sicherheitslücken zu schliessen oder deren Gefahren zu minimieren. Angesichts des Umfangs und der Komplexität der IKT-Systeme sind das aber Aufgaben, welche von den zuständigen Sicherheitsteams der Hersteller und der Anwender nicht mehr in jedem Fall in ausreichender Qualität wahrgenommen werden können. Deshalb bleiben viele Schwachstellen von den Sicherheitsteams unentdeckt und können dann von Cyberangreifern ausgenutzt werden.
Aus diesem Grund birgt ethisches Hacking ein enormes Potenzial, die Cybersicherheit zu verbessern. Die Grundidee des ethischen Hackings ist, dass Hacker aktiv nach Schwachstellen in Computersysteme und Netzwerken suchen, diese dann aber nicht für Cyberangriffe nutzen, sondern sie den betroffenen Organisationen und Herstellern melden. Die Förderung des ethischen Hackings hat zum Ziel, Hackern möglichst gute Anreize zu bieten, dass sie ihre Fähigkeiten im Sinne des ethischen Hackings nutzen und so zur Cybersicherheit beitragen.

1.1 Ausgangslage

Die Bedrohung durch Cyberangriffe gehört seit Jahren zu den relevantesten Risiken für Behörden, Unternehmen sowie Bürgerinnen und Bürger. Dem Nationalen Zentrum für Cybersicherheit (NCSC) wurden allein im Jahr 2022 34'000 Vorfälle gemeldet.[1] Die grosse Mehrheit der Cyberangriffe sind kriminell motiviert. Das Spektrum reicht von klassischen Delikten, welche mit Hilfe von digitalen Mitteln verübt werden («digitalisierte Kriminalität»), bis zu Straftaten, die sich gegen das Internet, IKT-Systeme oder deren Daten richten («Cyberkriminalität»). Stark zugenommen haben insbesondere Ransomware-Angriffe, bei denen Hacker ins System eindringen, Daten verschlüsseln und häufig auch entwenden. Anschliessend erpressen sie die Opfer, indem sie anbieten, die Verschlüsselung gegen

[1] Bericht des Nationales Zentrum für Cybersicherheit (NCSC) «Informationssicherung – Lage in der Schweiz und International. Halbjahresbericht 2022/II» vom 11. Mai 2023, S. 10 (abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2022-2.html).

ein Lösegeld wieder rückgängig zu machen und bei einer entsprechenden Zahlung auf die Veröffentlichung der Informationen zu verzichten.
Da sehr viele Angriffe Schwachstellen in IKT-Systemen ausnutzen, ist die Verhinderung und Schliessung von Schwachstellen von zentraler Bedeutung. In der vom Bundesrat und den Kantonen im April 2023 gutgeheissenen Nationalen Cyberstrategie (NCS) wird dies deutlich hervorgehoben. Dort steht: «Für die Cybersicherheit ist es von essenzieller Bedeutung, dass die Entstehung solcher Schwachstellen wo immer möglich verhindert wird und bestehende Schwachstellen rechtzeitig erkannt und rasch behoben werden.»[2] Die Förderung von ethischem Hacking ist dabei für letzteres eine der wichtigsten Massnahmen. Ziel ist es, das grosse Potential von Hackern mit ethischen Absichten zu nutzen, ihnen gute Rahmenbedingungen für die Suche nach Schwachstellen und deren Meldung zu schaffen und dadurch Schwachstellen früher zu erkennen und zu schliessen. Grundvoraussetzung für die Förderung des ethischen Hackings ist, dass dabei die Grenzen des anwendbaren Rechts respektiert werden. Insbesondere müssen die strafrechtlichen Bedingungen für legales Hacking erfüllt sein. Art. 143bis StGB legt fest, dass sich strafbar macht, wer unbefugt in ein fremdes, gegen seinen Zugriff besonders geschütztes Datenverarbeitungssystem eindringt. Davon zu unterscheiden ist das Hacking im Auftrag oder jedenfalls mit der Einwilligung des Systemberechtigten. In diesem Fall liegt aufgrund des Auftrags, der Einladung oder der Ausschreibung kein unbefugtes Eindringen und damit auch kein widerrechtliches Verhalten vor.

1.2 Auftrag

Um die Bedeutung und das Potenzial des ethischen Hackings in der Schweiz besser einschätzen zu können, hat der Nationalrat am 19. März 2021 folgendes Postulat angenommen:

Po. 20.4594 Bellaiche «Ethisches Hacking institutionalisieren und Cybersicherheit erhöhen»
Der Bundesrat ist beauftragt zu prüfen, inwiefern ethisches Hacking als Grundsatz für die Erhöhung der Cybersicherheit zu institutionalisieren und in Bundesverwaltung und bundesnahen Betrieben mit den folgenden Massnahmen zu fördern:

1. Öffentliche Verwaltung und bundesnahe Betriebe sollen Offenlegungsrichtlinien, sogenannte «Vulnerability Disclosure Guidelines» erarbeiten. Diese Richtlinien sollen einen klar geregelten Ablauf beim Auffinden einer Sicherheitslücke in einem Datenverarbeitungssystem vorsehen und eine koordinierte Offenlegung durch Dritte, sogenannte Coordinated Disclosure, sicherstellen. Die Richtlinien legen insbesondere fest, welche Systeme überprüft werden dürfen, welche Tests dazu erlaubt sind und wohin eine Lücke gemeldet werden kann. Sie schaffen Rechtssicherheit für ethische Hacker, indem sie den Verzicht auf Strafverfolgung regeln, sofern die Bedingungen der Richtlinien eingehalten worden sind.
2. Die Betriebe sollen ihre Datenverarbeitungssysteme proaktiv im Rahmen von Bug Bounty Programmen auf Schwachstellen prüfen lassen. Davon ausgenommen sind klassifizierte Systeme. Da diese Programme in der Regel erfolgsbasiert prämiert werden, sollen die Budgets der Staats- und staatsnahen Betriebe entsprechen ausgestaltet werden dürfen.
3. Das National Cyber Security Center (NCSC) unterstützt diesen Prozess aktiv und begleitet die Umsetzung.

Um diesen Prüfauftrag zu erfüllen, wird im Bericht einleitend dargestellt, was unter dem Begriff «ethisches Hacking» verstanden wird. Anschliessend werden die verschiedenen Instrumente zur Förderung des ethischen Hackings dargelegt. Im dritten Kapitel wird ausgeführt, welche Instrumente im internationalen Kontext zur Förderung des ethischen Hackings angewendet werden und welche internationalen Organisationen sich dafür einsetzen. Im vierten Kapitel geht es dann um den eigentlichen Prüfauftrag. Das ethische Hacking spielt auch in der Schweiz eine immer wichtigere

[2] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» vom April 2023, S.19 (abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf).

Rolle. Viele Behörden und Unternehmen setzen bereits Instrumente zur Förderung des ethischen Hackings ein. Es wird beschrieben, wie diese Förderung konkret ausgestaltet wird und in welchen Bereichen noch zusätzliches Potential besteht. Abschliessend wird dann der Status quo im Sinne eines Fazits beurteilt und aufgezeigt, wo noch Handlungsbedarf besteht.

1.3 Definition: Was ist ethisches Hacking?

Der Begriff «Hacking» wird sehr breit und häufig als Synonym für die Cyberkriminalität verwendet. Im eigentlichen Sinn bezieht sich «hacken» jedoch auf das Eindringen in Computersysteme.[3] Ein Hacker ist also eine Person, die aktiv in Systeme eindringt, auf die sie keinen Zugriff haben sollte, unabhängig von ihren Motiven. Dabei verwenden Hacker verschiedene Methoden, um in IKT-Systeme einzudringen. Sie können beispielsweise über Phishing-Angriffe ihre Opfer dazu verleiten, Programme auf ihren Systemen zu installieren, welche den Angreifern dann einen Zugriff auf diese ermöglichen. Alternativ nutzen sie für den gleichen Zweck Schwachstellen in IKT-Systemen aus, welche es ihnen erlauben, direkt in die Systeme einzudringen. Oft benutzen Angreifer auch eine Kombination von verschiedenen Methoden, um ihre Ziele zu erreichen.
Um zwischen Hackern mit ethischen und solchen mit unethischen Absichten zu differenzieren, wurde in den 1990er Jahren die Unterscheidung zwischen «Black Hat»- und «White Hat»-Hackern geschaffen. Die «Black Hat»-Hacker handeln aus unethischen, meist kriminellen Motiven und setzen ihre Programmierkenntnisse für strafbare Zwecke ein. Sie entsprechen damit den Bösewichten aus den alten Westernfilmen, welche jeweils schwarze Hüte trugen. Demgegenüber wenden «White Hat»-Hacker ihre Hacking-Fähigkeiten zum Nutze der Gesellschaft an. Zwar versuchen sie genauso wie «Black-hat»-Hacker in Computersysteme einzudringen oder zumindest Möglichkeiten zu identifizieren, welche ein solches erlauben würden. Hierbei verfolgen sie aber keine unethischen oder kriminellen Ziele. Dies bedeutet, dass sie ihre Erkenntnisse den Betroffenen zur Verfügung stellen und so dazu beitragen, die Sicherheit der Systembetreibenden und anderer Betroffenen zu erhöhen.
Die Unterscheidung zwischen ethischen und unethischen Hackern stellt die Absicht ihres Handels in den Vordergrund. Es ist dabei jedoch nicht immer einfach zu beurteilen, welche Absichten den Grundsatz des ethischen Handelns erfüllen und oft führen die Aktionen von Hackern zu Diskussionen über die Grenzen von ethischem zu unethischem Hacking. Des Weiteren darf diese Diskussion nicht darüber hinwegtäuschen, dass ein unbefugtes Eindringen in fremde Systeme auch dann widerrechtlich ist, wenn ihm eine ethische Absicht zugrunde liegt.[4]
Es ist deshalb entscheidend, dass möglichst klare Rahmenbedingungen definiert werden, unter welchen ein Eindringen in Systeme legal und zum Nutzen der Betroffenen stattfinden kann. Neben der Einwilligung der Systemberechtigten ist dabei wichtig zu definieren, wen und wie die Hacker zu welchem Zeitpunkt über die gefundenen Schwachstellen informieren.[5] Wenn klare Rahmenbedingungen definiert sind und diese eingehalten werden, kann von ethischem Hacking gesprochen werden.
Ethisches Hacking basiert also grundsätzlich auf den gleichen Methoden wie widerrechtliches Hacking. Es werden technische Schwachstellen gesucht, um in IKT-Systeme einzudringen. Schwachstellen können definiert werden als «ein Verhalten oder eine Reihe von Bedingungen in einem System, Produkt, einer Komponente oder einem Dienst, das oder die gegen eine implizite oder explizite Sicherheitsrichtlinie verstösst. Eine Schwachstelle kann als eine Schwäche oder Bedrohung

[3] Als Hacking versteht der Schweizer Gesetzgeber das unbefugte Eindringen in eine Datenverarbeitungsanlage, vgl. hierzu Botschaft und Gesetzesentwürfe vom 24. April 1991 über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen), BBl **1991** 969 ff., 1011.

[4] Anderer Meinung sind Dr. Michael Isler/Oliver M. Kunz/Gina Moll, welche in einem Rechtsgutachten zu Händen des Nationalen Testinstituts für Cybersicherheit (NTC) argumentieren, dass es bereits in der heutigen Rechtslage für ethisch handelnde Hacker möglich ist, sich unter gewissen Voraussetzungen auf den strafrechtlichen Rechtfertigungsgrund des Notstand nach Art. 17 StGB berufen können (vgl. Michael Isler/Oliver M. Kunz/Gina Moll, Rechtsgutachten: «Strafbarkeit von Ethical Hacking», walderwyss rechtsanwälte, 26. Juni 2023, N 209, S. 60, abrufbar unter: https://www.walderwyss.com/user_assets/news/230625-MASTERFILE-NTC-Gutachten.pdf).

[5] Vgl. Alana Maurushat, Ehtical Hacking, Ottawa 2019, Zweites Kapital [besser wäre es die Seitenzahl mit ff. anzugeben, z.B. S. 15 ff.); Sandro Germann/David Wicki-Birchler, Hacking und Hacker im Schweizer Recht, in: Aktuelle Juristische Praxis (AJP), 1/2020, S. 86 (abrufbar unter: https://fh-hwz.ch/api/assets/31755dd2-fc53-47c2-914c-099ac3b1ede5).

verstanden werden, die sich auf die Sicherheit auswirken oder sicherheitsrelevante Folgen haben kann.»[6] Schwachstellen können in einzelnen Hard- oder Softwareprodukten vorhanden sein oder auch erst durch die Vernetzung und Konfiguration solcher Produkte entstehen.
Weil Schwachstellen oft nicht einfach zu finden sind, ist es sehr wertvoll, wenn spezialisierte Hacker aktiv nach solchen suchen. Eine solche externe Prüfung erhöht die Chancen, dass Schwachstellen entdeckt werden, bevor sie von kriminellen Hackern ausgenutzt werden können.

2 Instrumente zur Förderung des ethischen Hackings

Ethisches Hacking leistet einen wertvollen Beitrag zur Cybersicherheit der Wirtschaft und Gesellschaft. Ihre Arbeit ist für die Sicherheit der Unternehmen und Behörden wichtig. Zudem ist das ethische Hacking auch aus ökonomischer Perspektive sinnvoll. Wenn Hacker im Auftrag oder aus eigener Initiative Schwachstellen finden und diese den Betroffenen melden, kann ein potentiell hoher Schaden verhindert werden. Aus ökonomischer Sicht besonders attraktiv sind dabei Programme, bei denen Hacker ermuntert werden, Schwachstellen zu suchen und zu melden, ohne dass sie dafür direkt beauftragt werden. In diesen Programmen werden sie nur dann bezahlt, wenn sie wirklich eine Schwachstelle gefunden haben.
Auf der anderen Seite darf ethisches Hacking nicht mit Altruismus gleichgesetzt werden. Es ist legitim, dass Hacker versuchen, über legale Wege aus ihrem Können den höchstmöglichen Gewinn zu erzielen. Aus diesem Grund ist es für sie wichtig zu wissen, was sie bei einer Meldung von Schwachstellen erwarten können. Dabei helfen klare Bedingungen für die Suche und die Meldung von Schwachstellen sowie Transparenz darüber, welche Belohnungen für welche Funde ausgerichtet werden.[7]
Das ethische Hacking kann damit als Geschäftsmodell bezeichnet werden. Sehr viele Dienstleister in der IT-Sicherheit bieten ethisches Hacking als Teil ihres Auftrags-Portfolios an. Zudem gibt es heute bereits verschiedene Hacker, die sich auf die bezahlte Suche nach Schwachstellen spezialisiert und sich als selbständige Unternehmen in diesem Bereich etabliert haben.[8]
Entscheidend für den Erfolg des ethischen Hackings sind möglichst klare Rahmenbedingungen. Es liegt schlussendlich in der Verantwortung der Unternehmen und Behörden festzulegen, unter welchen Umständen und für welche Systeme oder Bereiche hiervon sie die Einwilligung für die Suche nach Schwachstellen durch Hacker erteilen. Wenn sie dies tun, ermöglichen sie es den Hackern, aktiv nach Schwachstellen zu suchen, ohne dabei zu riskieren, dass sie eine Grenze zum widerrechtlichen Hacken überschreiten, das heisst, den Straftatbestand des unbefugten Eindringens in fremde Datenverarbeitungssysteme nach Art. 143bis StGB zu erfüllen.
Die Rahmenbedingungen werden über Programme zur Förderung des ethischen Hackings definiert. Weil die verschiedenen Programme zur Förderung des ethischen Hackings sich bezüglich der Rolle der Unternehmen und Organisationen ebenso wie hinsichtlich der Anreize für ethisches Hacking stark unterschieden, sollen sie nachstehend kurz beschrieben werden. Hierbei wird auch dargelegt, wie wichtig die Koordination zwischen den Hackern und den Betroffenen sein kann und welche Rolle staatliche Akteure dabei übernehmen können.

---

6 Vgl. ISO/IEC 29147:2018-10 (Ausgabedatum 2018-10), «Offenlegung von Schwachstellen».
7 Omer Akgül et al., Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem, S. 1 ff. (abrufbar unter: https://www.usenix.org/system/files/sec23fall-prepub-81-akgul.pdf).
8 Vgl. dazu NZZ vom 10.08.2022: «Xel» ist ein Schweizer Top-Hacker: Ein Besuch im Homeoffice (nzz.ch).

2.1 Programme zur Förderung des ethischen Hackings

Im Folgenden werden drei verschiedene Programme zur Nutzung des Potentials des ethischen Hackings beschrieben: die Durchführung von Sicherheitstests, der Erlass von Richtlinien für die Meldung und Veröffentlichung von Schwachstellen und die Umsetzung von Bug Bounty Programmen.

2.1.1 Sicherheitstests

Sicherheitstests werden seit vielen Jahren durchgeführt, um Schwachstellen in IKT-Systeme frühzeitig zu erkennen. Die verbreitetste Form von Sicherheitstests sind die so genannten Penetrationstests. Dabei beauftragen Unternehmen oder Organisationen Hacker damit, ihre Systeme und Anwendungen anzugreifen und durch das Hacking allfällige Schwachstellen zu identifizieren. Bei solchen Tests wird vom Auftraggeber vorgegeben, welche Systeme auf welche Art getestet werden sollen. Die Hacker suchen innerhalb dieses vorgegebenen Rahmens nach Schwachstellen. Im Unterschied zu anderen Programmen zur Förderung des ethischen Hackings besteht üblicherweise eine vertragliche Vereinbarung zwischen den Hackern und den Auftraggebern und die Hacker werden für ihre Tätigkeiten und eingesetzte Zeit bezahlt, unabhängig davon, ob sie eine Schwachstelle finden oder nicht. Eine Spezialform hiervon sind so genannte öffentliche Sicherheitstests («Public Security Tests»). Dabei veröffentlichen die Entwickler oder die Betreiber eines Systems oder einer Anwendung den entwickelten Code und rufen öffentlich dazu auf, diesen auf Schwachstellen zu prüfen. Die öffentlichen Sicherheitstests haben damit viele Ähnlichkeiten mit einem offenen Bug Bounty Programm (vgl. Kap. 2.1.3), sind aber typischerweise zeitlich begrenzt und auch im Umfang der zu testenden Systeme normalerweise auf ein konkretes System oder eine konkrete Anwendung beschränkt.

2.1.2 Richtlinien für die Meldung und Veröffentlichung von Schwachstellen

Eine sehr einfache Form, ethisches Hacking zu fördern, ist die Definition und Publikation von Richtlinien für die Meldung und Veröffentlichung von gefundenen Schwachstellen. Für Hacker, welche Schwachstellen suchen und melden wollen, ist es wichtig, möglichst viel Sicherheit darüber zu haben, dass sie durch die Suche nach Schwachstellen und die anschliessende Meldung an die betroffenen Organisationen nicht von diesen rechtlich belangt werden. Deshalb ist es für sie sehr hilfreich, wenn die Organisationen bekannt machen, unter welchen Bedingungen sie in welche Art von ethischem Hacking einwilligen und wie die Schwachstellen korrekt gemeldet werden. Genau dies ist der Zweck der Richtlinien für die Meldung und Veröffentlichung von Schwachstellen.
Die betroffenen Organisationen müssen Angaben darüber machen, wie gefundene Schwachstellen korrekt gemeldet werden können. Wie solche Richtlinien ausgestaltet werden sollten, ist beispielweise in der Norm ISO 29147:2018 beschrieben.[9] Im Minimum muss klar sein, wie die Hacker die Organisation kontaktieren können. Empfehlenswert sind zusätzlich Informationen über die sichere Kommunikation der Informationen und Angaben darüber, auf welchen Bereich der Organisation sich die Richtlinien beziehen (insbesondere muss transparent gemacht werden, wenn die Suche nach Schwachstellen in bestimmten Systemen oder Anwendungen der Organisation in jedem Fall unerwünscht ist). Um Konflikten über die Veröffentlichung der Schwachstelle vorzubeugen, ist es auch ratsam, in den Richtlinien festzuhalten, wie und in welcher Frist die betroffene Organisation gemeldete Schwachstellen selbst publik macht oder welches Vorgehen sie seitens der Hacker bei der Publikation erwartet. Schliesslich sollten die Richtlinien auch einen Abschnitt zur Würdigung enthalten und können auch Angaben zur möglichen Belohnung für die Meldung von Schwachstellen aufweisen. Eine mögliche Ausprägung von Belohnungen findet sich bei Bug Bounty Programmen.

[9] ISO 29147 :2018-10 (Ausgabedatum 2018-10), S. 35 ff.

2.1.3 Bug Bounty Programme

Bei Bug Bounty Programmen legen Organisationen Prämien fest, welche für das Auffinden von Schwachstellen in den von den Auftraggebern bezeichneten Systemen ausbezahlt werden, und bestimmen, welche Bedingungen für die Suche nach Schwachstellen gelten. Bei offenen Bug Bounty Programmen können sich alle Hacker an der Suche nach Schwachstellen beteiligen, bei geschlossenen Programmen nur eingeladene und ausgewählte Hacker.
Erste Bug Bounty Programme wurden bereits 1995 von der Firma Netscape Communications etabliert[10] und wurden seither auf Grund ihres Erfolgs von zahlreichen Unternehmen eingesetzt. Während manche grösseren Unternehmen eigene Bug Bounty Programme durchführen, nutzen andere die Services von Dienstleistern, die sich darauf spezialisiert haben, Plattformen für Bug Bounty Programme anzubieten. Die Plattformen vereinfachen es den Unternehmen, eigene Bug Bounty Programme aufzuschalten, direkt Hacker einzuladen und sie bei Erfolg zu belohnen. Für die Hacker sind sie attraktiv, weil sie über die Plattformen direkt Aufträge bekommen und so keinen Aufwand betreiben müssen, um festzustellen, ob und in welchen Fällen Unternehmen eine Belohnung bezahlen.

2.2 Die koordinierte Offenlegung von Schwachstellen

Die Programme zur Förderung des ethischen Hackings bieten einen guten Rahmen für die Meldung und Offenlegung von Schwachstellen. Sie werden aber noch längst nicht flächendeckend umgesetzt und viele Unternehmen machen keine Angaben darüber, wie mit bei ihnen gefundenen Schwachstellen umgegangen werden soll. Oft finden Hacker deshalb Schwachstellen, ohne dass Programme oder Richtlinien vorgeben, wie diese bekannt gemacht werden sollen. Auch in diesem Fall gibt es jedoch Grundsätze für das ethische Hacking. Diese sind in den Prozessen der «Coordinated Vulnerability Disclosure» - also der koordinierten Offenlegung von Schwachstellen – definiert. Massgeblich dafür ist die ISO/IEC Norm 29147:2018-10.[11]
Der Prozess zur koordinierten Offenlegung wurde entwickelt, weil die maximale Transparenz über Schwachstellen in den meisten Fällen auf den ersten Blick sinnvoll erscheint, da alle möglichen Betroffenen sofort über die Schwachstelle informiert werden. In der Praxis kann eine sofortige Veröffentlichung jedoch zu grossen Sicherheitsrisiken führen. Hersteller und Entwickler brauchen oft Zeit, bis sie eine Schwachstelle beseitigen können. In dieser Zeit sind alle Nutzenden, welche die betreffenden Produkte aus Unwissen oder mangels Alternativen weiterhin im Einsatz haben, durch die Veröffentlichung der Schwachstelle stark gefährdet.
Der Prozess der koordinierten Veröffentlichung hat als Ziel, eine möglichst hohe Transparenz über Schwachstellen zu ermöglichen, ohne Sicherheitsrisiken zu generieren. Kernelement des Prozesses ist, dass nach dem Finden einer Schwachstelle zunächst die Hersteller informiert werden. Die Hacker vereinbaren mit diesen eine Sperrfrist, innerhalb derer sie keine Informationen zur Schwachstelle öffentlich verbreiten. Dadurch erhalten die Hersteller genügend Zeit, die Schwachstelle zu beheben, bevor sie öffentlich gemacht wird.
Der Ansatz soll sicherstellen, dass keine Informationen zu Schwachstellen veröffentlicht werden, bevor Massnahmen zur Schliessung der Schwachstelle identifiziert wurden. Gleichzeitig wird durch die Vereinbarung einer Frist gewährleistet, dass die Schwachstelle durch die Hersteller nicht ignoriert werden kann.
Das Prinzip der koordinierten Veröffentlichung ist zwar einfach, in der Praxis ist die Kommunikation zwischen den Entdeckern der Schwachstelle und den Herstellern der betroffenen Produkte jedoch oft kompliziert. Um Schwachstellen nachzuweisen und zu dokumentieren, müssen Hacker diese selbst ausnutzen. Dies bedeutet sehr oft, dass sie in fremde Computersysteme eindringen, was wie oben

[10] MATTHEW FINIFTER/DEVDATTA AKHAWE/DAVID WAGNER, An Empirical Study of Vulnerability Rewards Programs, Proceedings of the 22nd USENIX Security Symposium, August 2013, S. 1 ff. (abrufbar unter: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf).
[11] ISO/IEC 29147:2018-10 (Ausgabedatum 2018-10), S. 14.

dargelegt nach Art. 143bis StGB den Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem erfüllen kann. Ihr Eindringen in IKT-Systeme ist nur dann strafrechtlich unbedenklich, wenn es sich entweder um die eigenen Systeme handelt oder die Einwilligung der Betroffenen vorliegt. Nicht immer sind jedoch die Grenzen jener Aktionen, zu welchen die Betroffenen einwilligen, – zum Beispiel in ihren Richtlinien zur Meldung und Veröffentlichung des ethischen Hackings – genügend klar. Es kann hierbei zu Konflikten zwischen den Hackern und den betroffenen Organisationen kommen. Oft entstehen solche Konflikte, wenn es um die Frage geht, wie und wann die Öffentlichkeit oder betroffene Dritte über die gefundene Schwachstelle informiert werden sollen. Die Hacker wollen meist eine möglichst hohe Transparenz, während für Unternehmen der Schritt in die Öffentlichkeit oft schwierig ist, weil damit Reputationsverluste verbunden sein können.
Bei Konflikten mit den betroffenen Unternehmen besteht für die Hacker das Risiko, dass sie sich strafbar machen.
Oft suchen diese deshalb die Vermittlung durch eine koordinierende Stelle. Die Rolle der koordinierenden Stelle besteht darin, Kontakte zwischen den Hackern und den Herstellern zu vermitteln und dabei auf Wunsch der Hacker deren Anonymität sicherzustellen. Weiter können Koordinatoren bei der Verhandlung über die verbindlichen Zeitpläne zur Offenlegung der Schwachstelle helfen, die Meldung und Dokumentation der Schwachstellen unabhängig überprüfen und die Hacker bei der korrekten Offenlegung der Schwachstelle unterstützen.[12]
In vielen Ländern bieten öffentliche Stellen eine solche Vermittlung an. In der Schweiz kann das Nationale Zentrum für Cybersicherheit diese Rolle übernehmen. Diese wird in Kapitel 4.1 genauer beschrieben.

3 Die Förderung des ethischen Hackings im internationalen Kontext

Viele Staaten versuchen, das ethische Hacking zu fördern und haben eigene Programme dafür entwickelt. Diese Programme sind oft in den nationalen Strategien zur Cybersicherheit beschrieben, aber selten in eigenen Rechtserlassen geregelt.
Im Europäischen Umfeld kommt insbesondere der Richtlinie über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union vom 14. Dezember 2022 (NIS-2)[13] eine wichtige Bedeutung zu. Die Richtlinie verlangt von den Mitgliedstaaten der EU, die koordinierte Offenlegung von Schwachstellen zu erleichtern (Art. 12) und die Massnahmen dazu in einer nationalen Strategie festzulegen (Art. 2 Abs. 2 Bst. c). Dazu gehört, dass die Mitgliedstaaten eine ihrer Cybersicherheitsorganisationen als Koordinationsstelle bezeichnen müssen (Art. 11 Abs. 5 Bst. c). Die Cybersicherheitsorganisationen verfügen über die nötigen Kenntnisse, Schwachstellen zu beurteilen und können mit ihrem Netzwerk zu einer raschen Koordination bei der Veröffentlichung der Schwachstelle beitragen.
Neben der staatlichen Förderung des ethischen Hackings sind auch die Aktivitäten von internationalen Organisationen und Nichtregierungsorganisationen von grosser Bedeutung. In erster Linie sind dabei die Normierungs- und Standardisierungsorganisationen zu nennen. Die Normen 29147 und 30111 der Internationalen Organisation für Normierung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) bilden die massgebliche Basis für die meisten Programme zur koordinierten Offenlegung von Schwachstellen und damit für die Zusammenarbeit zwischen Hackern und betroffenen Unternehmen. Auch das amerikanische «National Institute of Standards and Technology»

[12] ISO 29147:2018-10, S. 17.
[13] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) (abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1694072876640).

hat Standards zur Offenlegung von Schwachstellen veröffentlicht,[14] welche auf die ISO/IEC-Normen abgestimmt sind.
Weitere internationale Nichtregierungsorganisationen, die zur Förderung des ethischen Hacking beitragen, sind die Internet Engineering Task Force (IETF) und die Mitre Corporation. Erstere hat den technischen Standard security.txt verabschiedet,[15] welcher die Kontakt- und Meldemöglichkeiten für Schwachstellen und Vorfällen an betroffenen Unternehmen und Organisationen verbessert und vereinheitlicht. Durch Umsetzung des Standards sind die Kontakt- und Meldeangaben sowohl für Maschinen als auch für Menschen lesbar und erleichtern es so, betroffene Unternehmen zu kontaktieren. Die Mitre Corporation hat mit dem «Common Vulnerability and Exposures»- Programm eine Systematik entwickelt, welche es erlaubt, Schwachstellen zu kategorisieren und eindeutig zu identifizieren.[16] Mit diesem Hilfsmittel können Hacker, die eine Schwachstelle gefunden haben und diese melden wollen, einfach feststellen, ob es sich dabei um eine neue oder eine bereits bekannte Schwachstelle handelt.
Zusätzlich zu diesen technischen Standards, welche die Meldung und Behandlung von Schwachstellen erleichtern, hat die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) in einem Bericht aufgezeigt, wie Regierungen Programme zur koordinierten Offenlegung von Schwachstellen effektiv ausgestalten sowie umsetzen können und schlägt dabei auch eine «Good Practice» dafür vor.[17]
Das ethische Hacking spielt hingegen weder bei den Arbeiten des Europarates rund um das Übereinkommen über die Cyberkriminalität[18] noch bei den Verhandlungen der Vereinten Nationen zu einem globalen Cybercrime-Übereinkommen[19] eine wesentliche Rolle. Bei diesen Initiativen stehen die internationale Kooperation sowie eine Harmonisierung der Definition von illegalem Hacking und dessen Bekämpfung im Vordergrund. Verbindliche internationale Regelungen darüber, was als ethisches Hacking betrachtet werden soll, sind daher in naher Zukunft nicht zu erwarten.

4 Förderung des ethischen Hackings in der Schweiz

Die Förderung des ethischen Hackings hat in den letzten Jahren in der Schweiz deutlich an Bedeutung gewonnen. Während vor einigen Jahren nur wenige Unternehmen und Behörden sich mit Schwachstellenmanagement auseinandergesetzt haben, wurden zwischenzeitlich zahlreiche Richtlinien für die Meldung von Schwachstellen veröffentlicht und es werden Bug Bounty Programme durchgeführt. Nachfolgend werden der die strategischen und rechtlichen Grundlagen sowie der Stand der Umsetzung von Massnahmen zur Förderung des ethischen Hackings in der Schweiz beschrieben.

4.1 Strategische und rechtliche Grundlagen für die Förderung des ethischen Hackings

Wie sich die Förderung des ethischen Hackings in der Schweiz etabliert hat, ist auch in den strategischen und rechtlichen Grundlagen erkennbar. Während die beiden Nationalen Cyberstrategien von 2012-17 und 2018-22 keine eigenen Massnahmen zum Schwachstellenmanagement enthalten, definiert die aktuelle Cyberstrategie in der Massnahme 5 «Schwachstellen erkennen und verhindern» verschiedene Schritte zur Verbesserung der Bedingungen für das ethische Hacking. In der

[14] NIST Special Publication 800-216, Recommendations for Federal Vulnderability Disclosure Guidance, May 2023 (abrufbar unter: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf).
[15] RFC 9116, A File Format to Aid in Security Vulnerability Disclosure, April 2022 (abrufbar unter: https://www.rfc-editor.org/info/rfc9116).
[16] Abrufbar unter: CVE - CVE (mitre.org).
[17] OECD, Encouraging vulnerability treatment: Overview for policy makers, OECD Digital Economy Papers, No. 307, Februar 2021 (abrufbar unter: https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en).
[18] Council of Europe, Details of Treaty No. 185, Convention on Cybercrime (ETS No. 185) (abrufbar unter: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185).
[19] United Nations, Office on Drugs and Crime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Sessions- und Intersessionale Konsultations-Protokolle sind abrufbar unter: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home).

Massnahme wird die Etablierung von Programmen zur koordinierten Offenlegung von Schwachstellen gefordert. Es geht dabei nicht um eine Subventionierung des ethischen Hackings, sondern um die Verbesserung seiner Rahmenbedingungen und um die Erarbeitung von Hilfsmitteln. Konkret sollen Richtlinien definiert und umgesetzt werden und das NCSC soll eine zentrale Rolle bei der Koordination der Offenlegungsprozesse übernehmen. Das ethische Hacking soll über die Durchführung dedizierter Programme (z.B. Bug Bounty) institutionalisiert und die Rechtssicherheit für ethisches Hacking dadurch verbessert werden.[20]
Bei den rechtlichen Grundlagen zeigt sich eine ähnliche Entwicklung. Mit der am 29. September 2023 beschlossenen Revision des Informationssicherheitsgesetzes[21] zur Einführung einer Meldepflicht bei Cyberangriffen für kritische Infrastrukturen werden die rechtlichen Grundlagen für die koordinierte Offenlegung von Schwachstellen durch das NCSC geschaffen.[22] Im künftig geltenden Art. 73*b* Abs. 3 ISG wird festgehalten, dass das NCSC bei Meldungen zu Schwachstellen umgehend die Herstellerin der betroffenen Hard- oder Software informieren und ihr zur Behebung der Schwachstelle eine angemessene Frist setzen muss. Die Hersteller stehen dann in der Pflicht, Massnahmen zu ergreifen. Tun sie dies nicht, darf das NCSC die Schwachstelle unter Nennung der betroffenen Produkte veröffentlichen. Zudem sieht die Vorlage vor, das Bundesgesetz über das öffentliche Beschaffungswesen[23] so zu ergänzen, dass die Missachtung der vom NCSC gesetzten Frist für die Behebung von Schwachstellen im Beschaffungsverfahren zum Ausschluss vom Verfahren oder Widerruf des Zuschlags führen und das NCSC die Schwachstelle nach Fristablauf veröffentlichen kann.[24]
Mit diesen Bestimmungen legt das revidierte ISG die Grundlage dafür, dass das NCSC eine aktive Rolle bei der Förderung des ethischen Hackings übernimmt. Die rechtliche Möglichkeit, eine Schwachstelle dem NCSC zu melden, welches über Instrumente zur Durchsetzung einer Reaktion seitens der Hersteller verfügt, schafft Anreize für Hacker, Schwachstellen zu melden. Das Gesetz selbst sieht aber weder eine Belohnung für solche Meldungen vor, noch verpflichtet es die Unternehmen, mit Hackern zusammenzuarbeiten.
Einen Spezialfall stellen die Systeme für die elektronische Stimmabgabe dar. Die Verordnung über die politischen Rechte (VPR)[25] legt fest, dass die Kantone «Anreize für die Mitwirkung der Öffentlichkeit und der Fachkreise bei der Verbesserung der Systeme der elektronischen Stimmabgabe» setzen (Art. 27*l*ter VPR). Damit wird die rechtliche Grundlage für die Durchführung von öffentlichen Sicherheitstests und von Bug Bounty Programmen der Systeme der elektronischen Stimmabgabe geschaffen.

4.2 Umsetzung von Massnahmen im Bund

Der Bund setzt verschiedene Massnahmen zur Förderung des ethischen Hackings um. Wie in den rechtlichen Grundlagen definiert, hat er das NCSC als Anlaufstelle für die Meldung von Schwachstellen positioniert, um so die koordinierte Offenlegung von Schwachstellen zu fördern. Das NCSC veröffentlicht dazu Richtlinien für die Meldung. Zusätzlich hat der Bund auch einzelne öffentliche Sicherheitstests durchgeführt und setzt für die Bundesverwaltung ein Bug Bounty Programm um. Für die Bundesverwaltung ermächtigt der Bundesrat in der Informationssicherheitsverordnung (Art. 43 Abs. 1 Bst. c ISV), welche am 1. Januar 2024 in Kraft tritt, das NCSC (respektive das künftige Bundesamt für Cybersicherheit), im Einvernehmen mit den zuständigen Stellen nach Schwachstellen zu suchen. Es ist dabei explizit erlaubt, dass das NCSC Dritte damit beauftragt.

---

20 Bericht des Bundesrates «Nationale Cyberstrategie (NCS)» vom April 2023, S. 20 (abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf).
21 Bundesgesetz über die Informationssicherheit beim Bund (ISG; SR 128).
22 Vgl. hierzu auch die Medienmitteilung des Bundesrates vom 8. November 2023 (abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98497.html).
23 BöB, SR 172.056.1.
24 Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), BBl **2023** 84, 27.
25 SR 161.11.

4.2.1 Meldungen von Schwachstellen

Seit März 2021 verfügt das NCSC über eine Richtlinie für die Meldung von Schwachstellen.[26] Zentrales Element dieser Richtlinie ist die Klärung der Kontakt- und Meldemöglichkeiten. Das NCSC stellt auf der Internetseite des NCSC ein Meldeformular für Schwachstellen zur Verfügung. Es definiert zudem in den Richtlinien die Rahmenbedingungen für die Meldung von Schwachstellen, namentlich welches Vorgehen von den Hackern beim Umgang mit Schwachstellen verlangt wird und was umgekehrt die Hacker vom NCSC erwarten können.
Die aufgeführten Richtlinien müssen erfüllt sein, damit das NCSC eine Koordinationsrolle übernehmen kann und beispielsweise zwischen den Hackern, die anonym bleiben wollen, und den betroffenen Unternehmen das weitere Vorgehen betreffend Veröffentlichung der Schwachstellen abklärt. Bedingung dafür ist in erster Linie, dass die Schwachstelle von den Hackern nur für ihren eigenen Nachweis ausgenutzt und dokumentiert wird und sich diese keine Privilegien in fremden Systemen zu verschaffen versuchen. Weiter regelt die Richtlinie das Vorgehen zur Veröffentlichung einer gefundenen Schwachstelle. Das NCSC selbst verpflichtet sich, die Koordination zu übernehmen und – falls die Schwachstelle ein System der Bundesverwaltung betrifft – innerhalb von 60 Tagen eine Lösung für die Schwachstelle vorzuschlagen.
Zusätzlich hat das NCSC den security.txt-Standard auf den zentralen Internetseiten der Bundesverwaltung implementiert und umgesetzt[27]. Dieser Internet-Standard ermöglicht es einer Organisation oder Unternehmung, ihren Sicherheitskontakt und ihren Meldevorgang einheitlich im Internet zu publizieren und somit schneller auffindbar zu machen[28].
Bei einem Meldeeingang prüft das NCSC die gemeldete Schwachstelle und weist ihr, wenn es sich um eine neu entdeckte Schwachstelle handelt, einen Identifikator zu. Zu diesem Zweck beteiligt sich das NCSC am weltweiten Netzwerk des «Common Vulnerability and Exposures Programm». Das Programm basiert auf einer Systematik, nach welcher Schwachstellen nummeriert und dadurch eindeutig identifiziert und in den CVE-Katalog aufgenommen werden können. Seit seinem Beitritt zum CVE-Netzwerk hat das NCSC für 41 Schwachstellen eine CVE-Nummer vergeben und veröffentlicht.[29] Die meisten dieser Schwachstellen wurden dem NCSC von Forschern im Rahmen des (CVD)-Programms gemeldet.
Neben dem NCSC können Schwachstellen auch an weitere Stellen in der Bundesverwaltung gemeldet werden. Grundsätzlich sind sie in jedem Fall den Stellen zu melden, die durch die Schwachstelle betroffen sind. Bei Schwachstellen, die gemäss Datenschutzgesetz[30] relevant sind, können Meldungen an den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) gemacht werden. Dieser hat in einem Merkblatt zusammengefasst, welche datenschutzrechtlichen Vorgaben beim ethischen Hacking eingehalten werden müssen.[31] In diesem Merkblatt stellt der EDÖB auch klar, dass Meldungen über Schwachstellen an ihn nicht obligatorisch und auch nicht speziell vorgesehen sind. Der EDÖB ist nicht als koordinierende Stelle zur Veröffentlichung von Schwachstellen vorgesehen. Bei Meldungen kann er aber eine Untersuchung einleiten und mit dem NCSC zur koordinierten Veröffentlichung zusammenarbeiten.

4.2.2 Öffentliche Sicherheitstests

Öffentliche Sicherheitstests werden vor allem dann durchgeführt, wenn bei einem Projekt von Anfang an grösstmögliche Transparenz über die Sicherheit geschaffen werden soll. Diese Situation traf 2021

---

26 NCSC, **Fehler! Linkreferenz ungültig.**Melden einer Schwachstelle (Coordinated Vulnerability Disclosure, CVD) (abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html).
27 Abrufbar unter: https://www.ncsc.admin.ch/.well-known/security.txt.
28 NCSC, Security.txt – Hinterlegen Sie Ihren Sicherheitskontakt auf Ihrer Webseite (abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html).
29 NCSC, Eingegangene Meldungen, gemeldete Schwachstellen (abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/advisories.html).
30 Bundesgesetz über den Datenschutz (DSG; SR 235.1).
31 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Merkblatt White Hat Hacker/Innen (WHH): Ihre rechtliche Situation, ihre Risiken und die Rolle des EDÖB, vom 27. Juni 2023 (abrufbar unter: https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/datenschutz/MERKBLATT%20White%20Hat%20Hacker%20DE.pdf.download.pdf/MERKBLATT%20White%20Hat%20Hacker%20DE.pdf).

bei der Einführung eines COVID-Zertifikats zu. Das NCSC hat einen öffentlichen Sicherheitstests aller Anwendungen für die Ausstellung und Prüfung dieses Zertifikats durchgeführt. Dabei definierte das NCSC zunächst den Rahmen und die Regeln für den öffentlichen Sicherheitstest[32] und veröffentlichte anschliessend den Quellcode der entwickelten Anwendungen, damit Forscher diese prüfen und dem NCSC über ein spezielles Kontaktformular Schwachstellen melden konnten.
Der Test verlief erfolgreich. Zahlreiche Sicherheitsforscher und Hacker haben sich beteiligt und insgesamt 136 Schwachstellen identifiziert. Das NCSC hat alle ihm gemeldeten Schwachstellen auf seiner Website veröffentlicht.
Weil der öffentliche Sicherheitstest des COVID-Zertifikats ein Erfolg war, führte das NCSC auch zum «SwissCovid Proximity Tracing System» einen öffentlichen Sicherheitstest durch. Am 9. Juni 2021 stellte das NCSC neben dem Testrahmen und den Testregeln auch den Quellcode der Zusatzanwendung der Öffentlichkeit zur Verfügung, damit Forscher sie testen und dem NCSC über ein spezielles Kontaktformular Schwachstellen melden konnten. Auch hier war der Test ein Erfolg und ermöglichte die Einführung der SwissCovid App mit dem «Proximity Tracing System».

4.2.3 Durchführung von Hackathons zur Suche von Schwachstellen

Der Cyber Defence Campus (CYD Campus) der armasuisse W+T führt regelmässig Hackathons durch, die der Suche nach Schwachstellen in ausgewählten, für die Sicherheit der Schweiz besonders wichtigen Systeme dienen. Der Begriff Hackathon ist eine Wortschöpfung zwischen «Hacking» und «Marathon» und beschreibt eine Veranstaltung, bei der gemeinsam Lösungen für technische Probleme gesucht werden. Der CYD Campus hat dieses Instrument seit 2019 eingesetzt, um gezielt nach Schwachstellen in industriellen Kontrollsystemen (Industrial Control Systems, ICS), Autos und den Ladeinfrastrukturen oder Satellitenkommunikationssystemen zu suchen. Es haben sich dabei Fachexpertinnen und Fachexperten aus dem Campus, der Armee, dem NCSC, der Hochschulen und der Wirtschaft engagiert. Im Rahmen dieses Anlasses konnten kritische Schwachstellen in den Systemen gefunden werden.[33]

4.2.4 Bug Bounty Programm des Bundes

Das NCSC führte vom 10. bis 21. Mai 2021 in Zusammenarbeit mit Bug Bounty Switzerland AG, dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und den Parlamentsdiensten (PD) das erste Bug Bounty Programm für die Bundesverwaltung durch.[34] Ziel dieses Pilotprojekts war es, herauszufinden, ob die Einführung eines solchen Programms für die Systeme der Bundesverwaltung machbar ist und welche Vorteile und Grenzen es hat. Insgesamt wurden sechs Computersysteme des EDA und der Parlamentsdiensten von 15 Hackern getestet.
Für dieses Programm stellte das NCSC den Hackern Richtlinien zur Verfügung, die eindeutige Prozesse für die Suche, Erkennung und Meldung von Schwachstellen in den Systemen definieren. Zudem wurde festgelegt, welche Systeme konkret untersucht werden sollen. Im Übrigen wurde es den beteiligten Hackern aber überlassen, mit welchen Methoden sie die Systeme auf Schwachstellen testen.
Im Pilotversuch wurden insgesamt zehn Schwachstellen identifiziert, von denen eine als kritisch eingestuft wurde. Letztendlich wurden CHF 9'240.00 Belohnung an die Hacker ausgezahlt. Die Gesamtzahl der Schwachstellenmeldungen war für einen ersten Test vergleichsweise gering. Die getesteten Systeme hatten bereits vor dem Test einen hohen Sicherheitsreifegrad. Der Versuch hat aber deutlich gemacht, dass auch bei bereits gut geprüften Systemen weitere Schwachstellen gefunden werden können.

---

[32] NCSC, Scope and rules of engagement of the public security test, Regarding the Public Security Test (PST) of the Covid Certificate (abrufbar unter: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/covid-certificate-pst/scope_and_rules.html).
[33] Bundesamt für Rüstung armasuisse, Kollaborativer Ansatz zur Beseitigung von Cyber-Sicherheitslücken, vom 27. April 2023, (abrufbar unter: https://www.ar.admin.ch/de/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.detail.news.html/ar-internet/news-2023/news-w-t/ics-hackathon.html).
[34] Vgl. Medienmitteilung, Erfolgreiches Bug Bounty-Pilotprojekt in der Bundesverwaltung, vom 1. Juli 2021 (abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84304.html).

Des Weiteren hat der Pilotversuch zudem gezeigt, dass Bug Bounty Programme für die öffentliche Verwaltung sehr gut funktionieren und einen hohen Mehrwert bei einem vergleichsweise geringen finanziellen Aufwand erzeugen. Verschiedene weitere Verwaltungseinheiten haben nach dem Pilotversuch Interesse an einer Teilnahme an Bug Bounty Programmen beim NCSC angemeldet. Das NCSC hat sich auf Grund der positiven Erfahrungen und des hohen Interesses der Verwaltung entschieden, definitiv Bug Bounty Programme für die Bundesverwaltung einzuführen.
Auf der Plattform der Bug Bounty Switzerland AG publiziert das NCSC seit Herbst 2022 die Programme des Bundes.[35] Seit Sommer 2023 wurde der Umfang des NCSC Bug Bounty Programms erweitert, und die Hacker können dabei Schwachstellen in allen öffentlich exponierten Systemen der zentralen Bundesverwaltung suchen und melden. Das NCSC wird regelmässig über den Verlauf des Programms, die gefundenen Schwachstellen und ausbezahlten Prämien berichten.

4.2.5 Bereitstellung von Hilfsmitteln und Sensibilisierung

Der Bund nutzt nicht nur das Potential des ethischen Hackings, um die eigene Sicherheit zu verbessern, er fördert auch dessen Einsatz in der Wirtschaft und Gesellschaft. Das NCSC hat auf seiner Webseite einen Leitfaden veröffentlicht, um es Unternehmen einfacher zu machen, Richtlinien über die Offenlegung von Schwachstellen zu definieren. Dieser zeigt auf, was bei der Publikation von Richtlinien für das ethische Hacking zu beachten ist.[36] Der Leitfaden erläutert den Nutzen von Richtlinien für ethisches Hacking und zeigt auf, wie die Vorgaben der ISO/IEC Norm 29147:2018-10 praktisch umgesetzt werden können.
Das NCSC gibt auch detailliert Auskunft über die nötigen Schritte bei der Umsetzung des Pilotprojekts «Bug Bounty Programm der Bundesverwaltung», welche Kosten anfielen und welche Wirkung das Programm entfaltet hat. Damit legt es interessierten Unternehmen dar, dass solche Programme sich mit einem verhältnismässig tiefen Aufwand umsetzen lassen und rasch Erfolge erzielt werden können.
Schliesslich sensibilisiert das NCSC auch zielgruppenorientiert über einfach umsetzbare Massnahmen zur Förderung des ethischen Hackings. So hat es im ersten Quartal 2023 verschiedene Anlässe zur Cybersicherheit für Schweizer Gemeinden durchgeführt und dabei den Teilnehmenden aufgezeigt, wie die Erstellung von Kontaktmöglichkeiten für ethische Hacker über den security.txt-Standard umsetzbar ist. Seither ist der Prozentsatz der Gemeinden, welche diesen Standard umsetzen, von 11.5% (Stand Ende 2022) auf 38% (Stand September 2023) gestiegen. Dieser Erfolg zeigt, dass über die Sensibilisierung zu einfach umsetzbaren Massnahmen viel erreicht werden kann.

4.3 Umsetzung in der Wirtschaft

Wenn das ethische Hacking zur Sicherheit der Schweiz beitragen soll, genügt es nicht, wenn der Bund Massnahmen umsetzt. Es ist entscheidend, dass die Wirtschaft entsprechende Massnahmen umsetzt. Im Folgenden wird aufgezeigt, welche Massnahmen heute schon bei Unternehmen umgesetzt werden. Insbesondere wird auf die bundesnahen Betriebe eingegangen, da dies ein Fokus des Postulats ist. Schliesslich wird auch aufgezeigt, wie sich das Angebot für Dienstleistungen im Bereich des ethischen Hackings in der Schweiz entwickelt.

4.3.1 Massnahmen der Unternehmen

Unternehmen haben das Potential des ethischen Hackings erkannt, und viele Unternehmen nutzen es schon länger. Es gibt bisher keine umfassende statistische Analyse darüber, wie viele Unternehmen Instrumente zur Förderung des ethischen Hackings einsetzen und welcher Art diese Instrumente sind.

[35] Vgl. Medienmitteilung, Bug-Bounty-Programm für das zentrale Zugriffssystem eIAM des Bundes durchgeführt, vom 18. Oktober 2922 (abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90725.html).
[36] NCSC – Schwachstellenmanagement, Vulnerability Disclosure Management, Ein Leitfaden für Organisationen und Unternehmen, vom 13. Oktober 2022 (abrufbar unter: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/infos-it-spezialisten/Vulnerability_Disclosure_Management-Leitfaden_V1-0-DE.pdf.download.pdf/Vulnerability_Disclosure_Management-Leitfaden_V1-0-DE.pdf).

Die Erfahrungen des NCSC und der starke Ausbau an Angeboten über die letzten Jahre lassen aber darauf schliessen, dass Sicherheitsteste insbesondere von grösseren Unternehmen häufig angewendet werden.[37] Auf diese Art lässt sich das Potential des ethischen Hackings gezielt und zeitlich klar eingegrenzt nutzen, was die Planbarkeit für die Unternehmen erhöht. Sicherheitstests gehören heute zum Portfolio der Dienstleistungsunternehmen für die Cybersicherheit und können problemlos und bedarfsgerecht beschafft werden.
Erstaunlicherweise ist die Publikation von Richtlinien für die Meldung und Veröffentlichung von Schwachstellen – welche mit sehr wenig Aufwand und Kosten verbunden ist – in vielen Unternehmen noch nicht umgesetzt. Den Unternehmen scheint noch zu wenig bewusst zu sein, dass sie mit solchen Richtlinien auf einfache Weise mehr Klarheit für ethisches Hacking schaffen können. Das NCSC empfiehlt daher allen Unternehmen, mindestens eine Kontaktangabe für Sicherheitsmeldungen zu definieren. Mit solchen einfachen Massnahmen kann der für die Cybersicherheit entscheidende Informationsaustausch gestärkt werden.

4.3.2 Umsetzung in bundesnahen Betrieben

Von den bundesnahen Betrieben[38] sind einige Unternehmen Vorreiter bei der Förderung des ethischen Hackings. Die Swisscom beispielsweise betreibt bereits seit 2015 ein Bug Bounty Programm.[39] Auch andere bundesnahe Betriebe wie die Post[40] oder die SBB[41] verfügen über Bug Bounty Programme. Diese Betriebe agieren auch als Vorbilder bei der Veröffentlichung von Richtlinien über die koordinierte Veröffentlichung von Schwachstellen. Die Post,[42] die Swisscom[43] und die SBB[44] haben solche Richtlinien veröffentlicht.
Die beiden ETH-Einrichtungen haben zwar keine Richtlinien publiziert, bieten aber für die Meldung von Schwachstellen eine Kontaktadresse respektive eine Kontaktmöglichkeit über das security.txt an. Andere bundesnahe Betriebe haben – wie die überwiegende Mehrheit der Unternehmen – keine Richtlinien für die Offenlegung von Schwachstellen und keine spezifischen Kontaktstellen für Meldungen zu Sicherheitsvorfällen und Schwachstellen definiert. Sie setzen auch keine Bug Bounty Programme ein.
Es stellt sich die Frage, über welche Massnahmen sie dazu gebracht werden können, das ethische Hacking stärker zu fördern. Zunächst ist festzuhalten, dass es für viele Unternehmen ohne spezifisches Fachwissen bisher nicht einfach war, die richtigen Massnahmen zur Förderung des ethischen Hackings zu identifizieren und umzusetzen. Diese Situation hat sich aber grundlegend verbessert. Die Beispiele für Richtlinien zur Offenlegung von Schwachstellen des NCSC oder von anderen Organisationen vereinfachen die Erarbeitung von eigenen Richtlinien stark. Die in den letzten Jahren entstandenen Angebote an Bug Bounty Plattformen in der Schweiz ermöglichen es den Unternehmen, ohne grossen eigenen Aufwand solche Programme durchzuführen. Es besteht daher Anlass zur Annahme, dass sich die Förderung des ethischen Hackings in der Schweiz generell und bei Verwaltungen und bundesnahen Betrieben im Speziellen positiv entwickeln wird.
Im Unterschied zu Organisationen der zentralen Bundesverwaltung kann der Bundesrat nicht für die bundesnahen Betriebe bestimmen, ob sie Massnahmen zur Förderung des ethischen Hackings durchführen sollen. Er kann aber über die Staatsvertreter in den Verwaltungsräten oder über die strategischen Zielvorgaben Einfluss nehmen, sollte er feststellen, dass die Betriebe trotz der nun vorhandenen Möglichkeiten keine solchen Massnahmen umsetzen. Die Finanzierung von

---

37 Stefan Hunziker/Armand Portmann/Viviane Trachsel/Fernand Dubler, Cyber Risk Management in grösseren Schweizer Unternehmen, Luzern 2022 (abrufbar unter: https://economiesuisse.ch/sites/default/files/articles/downloads/Cyber%20Risk%20Management%20Studie%202022.pdf).
38 Hier verstanden als Betriebe, bei welchen der Bund Mehrheitsaktionär ist.
39 Swisscom, Bug Bounty Programme (abrufbar unter: https://github.com/swisscom/bugbounty#5-bug-bounty-programme).
40 Schweizerische Post, Bug Bounty Post, Securing Digital Trust (abrufbar unter: https://www.post.ch/de/ueber-uns/verantwortung/bug-bounty-post).
41 Schweizerische Bundesbahnen (SBB), Bug Bounty Program (abrufbar unter: https://app.intigriti.com/programs/sbb/sbbglobal/detail).
42 Schweizerische Post, Vulneratilbity Disclosure Policy (VDP) (abrufbar unter: https://vdp.post.ch/p/Information-Security).
43 Swisscom, Bug Bounty Programme, Responsible Disclosure Policy (abrufbar unter: https://github.com/swisscom/bugbounty#3-responsible-disclosure-policy).
44 Schweizerische Bundesbahnen (SBB), Vulnerability Disclosure Policy (abrufbar https://company.sbb.ch/en/sbb-as-business-partner/services/vulnerability-disclosure-policy.html).

Programmen zur Förderung des ethischen Hackings, insbesondere auch zur Ausrichtung von Belohnungen von Hackern, liegt in der Kompetenz der betroffenen Unternehmen.

4.3.3 Angebote für Dienstleistungen im Zusammenhang mit ethischem Hacking

In den letzten Jahren hat sich auch das Angebot von Dienstleistungen im Bereich von Bug Bounty Programmen stark entwickelt. Es gibt heute sowohl in der Schweiz wie auch im Ausland verschiedene Unternehmen, welche Plattformen und Dienstleistungen für Bug Bounty Programme anbieten und es so den Unternehmen erleichtern, solche Programme durchzuführen. Viele dieser Programme werden nicht öffentlich publiziert, weshalb nicht festgestellt werden kann, wie oft Bug Bounty Programme von Schweizer Unternehmen eingesetzt werden. Sicher ist, dass sich die Voraussetzungen für die Durchführung solcher Programme dank den Anbietern von Plattformen in der Schweiz stark vereinfacht haben. Es ist deshalb davon auszugehen, dass die Nutzung dieses Instruments zur Förderung des ethischen Hackings durch Unternehmen weiterwachsen wird.
Neben den Bug Bounty Plattformen leistet auch das Nationale Testzentrum für Cybersicherheit im Kanton Zug einen Beitrag zur Förderung des ethischen Hackings in der Schweiz. Das Testzentrum prüft digitale Produkte auf Schwachstellen. Es engagiert sich dadurch direkt für das ethische Hacking und arbeitet mit den Produzenten, den Betreibern der Systeme sowie mit dem NCSC zusammen.[45]

[45] Nationales Testinstitut für Cybersicherheit, Auftrag (abrufbar unter: https://www.ntc.swiss/auftrag).

5 Schlussfolgerungen

Im Bericht wurde aufgezeigt, dass die Förderung des ethischen Hackings in der Schweiz in den letzten Jahren grosse Fortschritte gemacht hat. Mit der Vorlage zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen hat das Parlament die gesetzlichen Grundlagen für die koordinierte Offenlegung von Schwachstellen geschaffen. Damit besteht nun ein Rahmen für das korrekte Vorgehen bei Meldungen von Schwachstellen an den Bund. Gleichzeitig sind viele privatwirtschaftliche Initiativen entstanden, welche das ethische Hacking in der Schweiz stark voranbringen. Die neuen Plattformen für Bug Bounty Programme beispielsweise erleichtern es interessierten Unternehmen stark, solche Programme umzusetzen. Die Bundesverwaltung hat in den letzten Jahren zahlreiche Massnahmen des ethischen Hackings umgesetzt und nimmt innerhalb der Schweiz eine Vorreiterrolle ein.

Ethisches Hacking ist dadurch in den letzten Jahren zu einem Faktor geworden, der die Cybersicherheit der Schweiz nachhaltig verbessert hat und auch künftig verbessern wird. Es ist heute ein Kernelement zur Umsetzung der Massnahme 5 der Nationalen Cyberstrategie «Schwachstellen erkennen und verhindern». Es darf davon ausgegangen werden, dass der Trend zur stärkeren Nutzung des ethischen Hackings in den nächsten Jahren weiter steigen wird. Je offensichtlicher der Erfolg dieser Programme ist, desto mehr Unternehmen und Organisationen werden die vorhandenen Instrumente ebenfalls einsetzen.

Der Bund wird diese Entwicklung weiter fördern, indem das NCSC bzw. das künftige Bundesamt für Cybersicherheit eine aktive Rolle bei der koordinierten Offenlegung von Schwachstellen übernimmt, die Verwaltung selbst die Umsetzung von Massnahmen zur Förderung des ethischen Hackings weiter ausbaut und der Bund mithilft, der Wirtschaft das Potential der Massnahmen aufzuzeigen und sie dabei unterstützt solche umzusetzen.

Direkte staatliche Eingriffe zur Förderung des ethischen Hackings über regulatorische Massnahmen – zum Beispiel die Verpflichtung von Unternehmen zur Durchführung von Massnahmen zur Förderung des ethischen Hackings – sind angesichts der positiven Entwicklung nicht nötig. Sie könnte im Gegenteil sogar kontraproduktiv sein, wenn sie die Interaktionen zwischen den Hackern und den Unternehmen durch formelle Anforderungen komplizieren. Die im Bericht erwähnten Massnahmen können so umgesetzt werden, dass sie die strafrechtlichen Grenzen wahren. Wesentlich ist dabei insbesondere, dass sie auf einem Auftrag oder zumindest auf der Einwilligung der Systemeigner beruhen. Es wurde zudem aufgezeigt, dass weiteres Potential besteht, diese bestehenden Massnahmen stärker zu nutzen. Es ist daher aktuell nicht nötig, das Strafrecht anzupassen, um ethisches Hacking weiter zu stärken. Es ist aber klar, dass es weitere Anstrengungen aller beteiligter Akteure braucht, um die Cybersicherheit unter Nutzung des ethischen Hackings weiter zu verbessern. Entscheidend ist, dass die gemeldeten und bekanntgemachten Schwachstellen auch wirklich geschlossen werden. Leider dauert es oft zu lange, bis bekannte Schwachstellen bei den Endkunden geschlossen werden, auch wenn die Hersteller Sicherheits-Patches zur Verfügung stellen.[46] Werden Schwachstellen nicht geschlossen, nützt es wenig, wenn sie zuvor von ethischen Hackern gefunden und über einen Prozess der koordinierten Offenlegung korrekt bekannt gemacht wurden. Es besteht dann auch das Risiko, dass Hacker die Motivation verlieren, Schwachstellen zu suchen und zu melden.

Zudem besteht viel Potential für einen verbesserten Austausch über Schwachstellen. Das Parlament hat bei der Diskussion über die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen auch darüber debattiert, eine generelle Meldepflicht für Schwachstellen einzuführen. Es hat diese schliesslich abgelehnt. Ein Argument dabei war, dass zunächst der freiwillige Austausch zu Schwachstellen gefördert werden soll.[47] Dieser Austausch wird mit der Förderung des ethischen Hackings noch wichtiger. Wenn über ethisches Hacking bei einem Unternehmen bisher unbekannte

[46] Vgl. NCSC, Medienmitteilung, Höchste Zeit, die Sicherheitslücken bei Microsoft Exchange-Server zu schliessen, vom 16. Februar 2022 (abrufbar unter: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/schwachstelle-exchange-server.html).

[47] 22.073 | Informationssicherheitsgesetz. Änderung (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) | Geschäft | Das Schweizer Parlament

Schwachstellen gefunden werden, hilft es allen anderen möglicherweise betroffenen Unternehmen, wenn sie über die Schwachstelle informiert werden. Das NCSC wird gemeinsam mit den Unternehmen sowie Organisationen, insbesondere den Betreiberinnen kritischer Infrastrukturen, daran arbeiten, diesen Informationsaustausch zu verstärken.
Abschliessend lässt sich festhalten, dass die Entwicklung des ethischen Hackings in der Schweiz zuversichtlich stimmt. Die Voraussetzungen, dass das grosse Potential des ethischen Hackings künftig besser genutzt wird, sind gegeben. Gelingt dies, ist zu erwarten, dass die Prävention gegen Cyberangriffe deutlich verbessert werden kann und die Behörden und Unternehmen sich deutlich besser schützen können als dies aktuell der Fall ist.