Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Band: 189 (2023)

Heft: 7

Artikel: Mehr Interdisziplinarität für eine bessere Cyberabwehr

Autor: Baschung, David / Muhly, Fabian / Keupp, Marcus Matthias

DOI: https://doi.org/10.5169/seals-1052756

Mehr Interdisziplinarität für eine bessere Cyberabwehr

Wie lassen sich Cyberangriffe schneller erkennen und wirkungsvoll bekämpfen? Und wie können die Angreifer rascher verstanden werden, um die Verteidiger besser ausbilden zu können? Antworten liefert eine verstärkte Interdisziplinarität bei der Cyberabwehr.

David Baschung, Fabian Muhly, Marcus Matthias Keupp

Im Allianz Risk-Barometer[1], einer jährlichen Umfrage von 2000 bis 3000 Spezialisten aus 22 verschiedenen Branchen, steht das Thema «Cyber incidents» regelmässig an der Spitze. Dabei sind Angriffe im Cyberraum in keinerlei Hinsicht etwas Neues. Bereits im 18. Jahrhundert gelang es zwei Brüdern, nicht nur die Übertragungen zwischen (optischen) Telegrafen abzuhören, sondern sie konnten auch versteckte Informationen darin einschleusen.

Doch auch wenn man den Cyberspace auf moderne digitale Informationstechnologien eingrenzt, gab es Diebstähle von Logindaten und Computerviren schon in den 1960er-Jahren.[2] Allan Scherr, damals Doktorand am Baltimore Polytechnic Institute, verschaffte sich Zugang zu den Passwörtern sämtlicher registrierter Benutzer eines Grossrechners, um diesen über das übliche Zeitlimit hinaus nutzen zu können.[3]

Obwohl es dann doch bis 1987 dauerte, bis die ersten kommerziellen Antivirenprogramme zur Verfügung standen, hat sich mittlerweile ein florierender Markt im dreistelligen Milliardenbereich für Cybersicherheitslösungen entwickelt.[4] Doch trotz des technologischen Fortschritts ist das Risiko unverändert hoch. An mangelnder Investitionsbereitschaft liegt es jedenfalls nicht; eine Marktanalyse von Gartner kommt zu dem Schluss, dass die weltweiten Ausgaben für Cybersicherheit in den letzten Jahren im Schnitt jährlich um acht Prozent gestiegen sind. Warum also sind die derzeitigen Bemühungen um Cybersicherheit oftmals ineffektiv oder unzureichend?

Cyberdefense als Wissenschaft

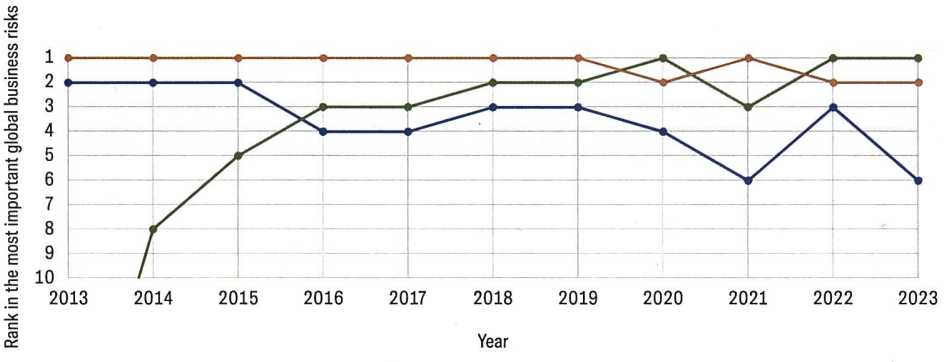
Die technisch-wissenschaftlichen Fachrichtungen beschäftigen sich schon seit Jahrzenten mit den Herausforderungen im Cyberraum; seit Kurzem werden sie auch mit ökonomischen Sichtweisen ergänzt. So haben etwa Lawrence A. Gordon und Martin P. Loeb[5] ein mathematisch-ökonomisches Modell für die Modellierung von Cybersicherheitsinvestitionen entwickelt, das von vielen Wissenschaftlern zitiert und weiter verfeinert wurde.

Andere Forschende haben ökonometrische Ansätze verwendet, um die Reaktion der Aktienmärkte auf kompromittierte Cybersysteme zu analysieren. Dennoch besteht kein Konsens, wie die mittel- und langfristigen Folgen von «Cyber incidents» zu quantifizieren sind. Geistes- und sozialwissenschaftliche Beiträge beschäftigen sich schliesslich mit kontextuellen Fragestellungen wie Datenschutz oder Unternehmensethik, reduzieren dabei jedoch die Umsetzung von Cyberdefense-Massnahmen auf eine Blackbox, die analog zu Gesundheits- und Sicherheitsmassnahmen einfach nur ordnungsgemäss ausgeführt werden muss.

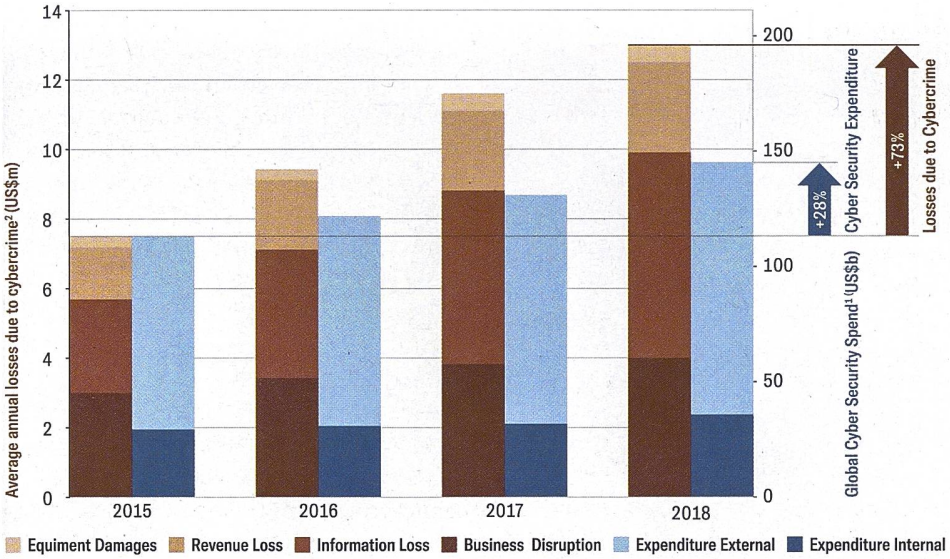
Cyberdefense als Handwerkskunst

Trotz formaler Zertifizierungen wie etwa ISO 27001, trotz behördlicher Auflagen und kommerziell erhältlicher Cyber-Assessments sind Unternehmen immer wieder von Sicherheitsverletzungen geplagt. Gemäss Accenture ist die absolute Zahl erfolgreicher Cyberangriffe auf private oder öffentliche Organisationen seit 2014 um 67 Prozent und seit 2018 um 11 Prozent gestiegen[6] – was die Frage aufwirft, ob diese «Cyber incidents» nur aus dem akzeptierten Restrisiko resultieren, ob die aktuellen Leistungsindikatoren und Kennzahlen die angestrebte Risikominderung nicht effektiv messen können, oder ob die Cyberabwehr dieser Unternehmen den Angriffen einfach nicht gewachsen ist.

Während sich formale Zertifizierungen und regulatorische Anforderungen hauptsächlich auf die ordnungsgemässe Umsetzung von (Risiko-)Managementprozessen beziehen, beschränkt sich die Bewertung der effektiven Cyberabwehr mehrheitlich auf sogenannte Penetrationstests. Aber auch deren Ergebnisse sind aufgrund von operativen Beschränkungen nur eigenschränkt verlässlich. Um beispielsweise negative Auswirkungen auf die Verfügbarkeit der produktiven Systeme zu minimieren oder die Integrität und Vertraulichkeit von Kundendaten und/oder Geschäftsgeheimnissen zu bewahren, werden solche simulierten Angriffe häufig auf Testsystemen ausgeführt. Konfigurationsfehler und spezifische Systemeigenschaften von Produktionssystemen bleiben dabei unentdeckt oder gar bewusst unberücksichtigt. Und es ist letztlich eine budgetäre Frage, wie sorgfältig, hartnäckig und technisch kompetent solche Angriffe simuliert werden. Somit dienen Penetrationtests eher der Verifizierung als der Validierung von Cyberdefense-Fähigkeiten.



◀ Die wichtigsten globalen Geschäftsrisiken im Verlauf zwischen 2013 bis 2023.
Grafik: Allianz Risk-Barometer/David Baschung



◀ **Gegenüberstellung von Investitionen in Cybersicherheit und Verlusten durch Cyberkriminalität in US-Dollar zwischen 2015 und 2018.** Grafik: David Baschung

Schwer abschätzbare Wahrscheinlichkeiten für seltene Ereignisse, monetäre Verluste[7] und Kostentransparenzen[8] hindern Organisationen daran, verlässliche Leistungsindikatoren und Metriken für ihre Cyberverteidigung festzulegen. Fehlanreize, Informationsasymmetrien, vorgefasste Strategien und Hintergedanken bleiben somit meist unentdeckt.[9] Bei militärisch motivierten Cyberangriffen kommen weitere Problemdimensionen hinzu. Während konventionelle militärische Konflikte öffentlich ausgetragen werden und daher gut zu beobachten sind, ist es bei Cyberangriffen auf kritische Infrastrukturen, Regierungssysteme oder militärische Einrichtungen meist gar nicht erwünscht, dass der Angriff überhaupt bemerkt respektive publik wird.

Selbst wenn ein Angriff erkannt wird, kann nicht abschliessend beurteilt werden, was genau die Absichten des Angreifers waren. Hat man überhaupt alle Zugriffe und Lücken erkannt oder nur Teile davon? Ist man einer absichtlich gelegten falschen Spur nachgegangen? Solange die Absichten und Zielsetzungen des Angreifers unbekannt sind, ist auch keine abschliessende Aussage über die Effektivität der Abwehr möglich. Entsprechend ähnelt Cyberdefense derzeit eher einer Handwerkskunst als einer exakten Wissenschaft. Einig ist man sich jedoch darüber, dass Forschung im Bereich der Cyberrisiken eines interdisziplinären Ansatzes bedarf.[10] Das Buch «Cyberdefense – The Next Generation» der Dozentur Militärakademie an der MILAK versucht diesem Aufruf gerecht zu werden, indem es neue Methoden und eine interdisziplinäre Perspektive auf Cyberdefense präsentiert. Der von Marcus Matthias Keupp herausgegebene Band vereint die Fachkompetenz von über 20 Wissenschaftlern und Praktikern. Es wird in der zweiten Jahreshälfte 2023 im Springer Nature-Verlag[11] erscheinen.

Ein interdisziplinärer Ansatz zu Cyberdefense in drei Akten

Viele Cyberangriffe bleiben über einen längeren Zeitraum unbemerkt. Im Jahr 2019 benötigten Unternehmen im Durchschnitt 230 Tage, um durch böswillige Angriffe verursachte Datenschutzverletzungen zu erkennen. Weitere 84 Tage dauerte es von der Identifizierung bis zur Eindämmung.[12] Im ersten Teil des Buches werden daher verschiedene Ansätze präsentiert, wie sich die Erkennung und Behebung von Cyberangriffen beschleunigen lässt.

Der zweite Teil des Buches befasst sich mit dem systematischen Problem, dass die Cyberdefense dem Angriff stets hinterherhinkt. Damit ein Hersteller überhaupt das unternehmerische Risiko eingeht, eine bestimmte Cyberdefense-Technologie zu kommerzialisieren, muss heute eine Nachfrage bereits existieren oder zumindest unmittelbar absehbar sein. Entsprechend können kommerziell verfügbare Cyberdefense-Technologien nur verzögert auf neue Bedrohungen reagieren. Der zweite Teil des Buches präsentiert daher unterschiedliche Konzepte, wie sich diese Reaktion beschleunigen lässt.

Der dritte Teil des Buches widmet sich der Effektivität der Cyberverteidigung. Er präsentiert Ansätze jenseits formaler Zertifizierungen und klassischer Testverfahren. Es geht darum, das Verhalten des Angreifers besser zu verstehen, neue, spielerische Ansätze bei der Ausbildung der Verteidiger einzusetzen und völkerrechtliche Fragen bei der Schaffung eines globalen Cyberdefense-Regimes anzugehen. Das Ziel ist klar: unsere Position im Kampf gegen Angriffe im Cyberraum nachhaltig zu stärken. ■

1 https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
2 Raymond, E. S. (Ed.). (1996). The New Hacker's Dictionary (3rd ed.). MIT Press.
3 Walden, D., & Van Vleck, T. (2011). Compatible Time-Sharing System (1961-1973), Fiftieth Anniversary Commemorative Overview. IEEE Computer Society.
4 https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/
5 Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438–457.
6 Accenture. (2019). Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
7 Böhme, R. (2010). Security Metrics and Security Investment Models. In I. Echizen, N. Kunihiro, & R. Sasaki (Eds.), Advances in Information and Computer Security (pp. 10–24). Springer.
8 Brecht, M., & Nowey, T. (2013). A Closer Look at Information Security Costs. In R. Böhme (Ed.), The Economics of Information Security and Privacy (pp. 3–24). Springer.
9 Anderson, R., & Moore, T. (2006). The Economics of Information Security. Science, 314(5799), 610–613.
10 Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. Science, 366(6469), 1066–1069.
11 Marcus Matthias Keupp (Hg.), Cyberdefense – The Next Generation, International Series in Operations Research & Management Science, Springer Cham 2023, 978-3-031-30190-2 (ISBN)
12 IBM Security. (2019). 2019 Cost of a Data Breach Report.

David Baschung
Chair of Technology and Innovation Management, ETH Zürich

Fabian Muhly
Dr.
Dozentur Militärökonomie, Militärakademie MILAK an der ETH Zürich, École des Sciences Criminelles, Université de Lausanne

Marcus Matthias Keupp
PD Dr.
Dozent Militärökonomie der MILAK an der ETH Zürich
8903 Birmensdorf