Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 184 (2018)

Heft: 7

Artikel: Teile und herrsche : Cyber-Sicherheit durch Informationsaustausch

Autor: Keupp, Marcus M. / Mermoud, Alain / David, Dimitri Percia

DOI: https://doi.org/10.5169/seals-813196

Teile und herrsche: Cyber-Sicherheit durch Informationsaustausch

Cyber-Sicherheit umfasst mehr als nur technische Fragestellungen. Das Teilen von Informationen über Cyber-Bedrohungen ermöglicht es dem Verteidiger überhaupt erst, Investitionen in Cyber-Abwehr richtig zu priorisieren. Dieser Artikel präsentiert die Ergebnisse einer wissenschaftlichen Studie, die die Anreize zu solchem Teilen untersucht hat. Auf der Basis dieser Ergebnisse erarbeiten wir einige Empfehlungen zur organisatorischen Gestaltung.

Marcus M. Keupp, Alain Mermoud, Dimitri Percia David

Moderne Gesellschaften sind in immer stärkerem Masse auf die Nutzung von Informations- und Kommunikationstechnologien angewiesen, um ihre wirtschaftlichen Austauschbeziehungen zu organisieren. Mit dem Ausmass dieser Nutzung geht ein exponentielles Wachstum der Angriffsmöglichkeiten einher. Für Staaten, Unternehmen und Individuen stellt sich nicht länger mehr die Frage, ob sie im Cyber-Raum angegriffen werden, sondern nur noch, wie professionell und in welcher Intensität. Technologische Entwicklungen hin zum «Internet der Dinge», in dem eine Vielzahl autonom agierender Geräte zum Teil des Cyber-Raums geworden ist, verstärken diese Tendenz. Schliesslich sind auch alle kritischen Infrastrukturen über den Cyber-Raum miteinander verbunden, sodass ein Angriff auf eine einzige Struktur einen Kaskadeneffekt auslösen kann, der die Cyber-Sicherheit der gesamten Nation kompromittiert *(contagion risk)*. Auch Armeen können sich diesem Wandel nicht entziehen, da sie mit ihren vielfältigen IT-Systemen selbst Teil des Cyber-Raums sind. Ohne deren Einsatz sind weder die logistische Organisation militärischer Leistung noch die eigentliche Auftragserfüllung im Konflikt möglich.

Teile und herrsche

Die zunehmende Vernetzung des Cyber-Raums bietet aber auch Chancen für die Cyber-Abwehr. Gerade weil alle kritischen Infrastrukturen über den Cyber-Raum verbunden sind, können die Betreiber dieser Infrastrukturen untereinander Informationen austauschen, um sowohl

«Es stellt sich nicht mehr die Frage, ob wir angegriffen werden, sondern nur noch, wie professionell und mit welcher Intensität.»

ihre eigene Cyber-Sicherheit zu verbessern als auch das Risiko von Kaskadeneffekten zu reduzieren. Wird ein bestimmter Betreiber angegriffen, kann er Informationen über Art und Intensität des Angriffs mit anderen Betreibern teilen, sodass diese ihre Abwehr anpassen können. Solches Teilen von Informationen ist daher die nachrichtendienstliche Grundlage der Cyber-Abwehr *(cyber threat intelligence)*. Es verbessert die technische Resilienz des Cyber-Raums insgesamt, da es die Kosten der Informationsbeschaffung signifikant reduziert.[1]

So vorteilhaft dieses Teilen von Informationen auch ist, so stellt es sich dennoch nicht von selbst ein. Ein Betreiber kritischer Infrastrukturen hat einen Anreiz, die Information nur für sich selbst zu verwenden, da ihre Gewinnung kostenintensiv ist. Gleichzeitig ist er daran

«Information Sharing and Analysis Center (ISAC)»

ISACs sind Organisationen, die den Informationsaustausch über sicherheitsrelevante Vorfälle im Cyber-Raum erleichtern sollen. Sie erheben zwar meistens Mitgliederbeiträge, sind jedoch nur selten auf Gewinnerzielung ausgelegt. Ihre Organisation lässt sich danach unterscheiden, ob sie nur im privaten Sektor, als *public-private-Partnership* zwischen dem privaten Sektor und öffentlich-politischen Institutionen oder als Teil der Staatsbürokratie aktiv sind.

Beispiele für ISACs im privaten Sektor:

- Financial Services Information Sharing and Analysis Center (FS-ISAC) http://www.fsisac.com/
- Automotive Information Sharing and Analysis Center (AUTO-ISAC) https://www.automotiveisac.com/
- Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) http://ongisac.org/

Beispiele für ISACs als public-private-Partnership:

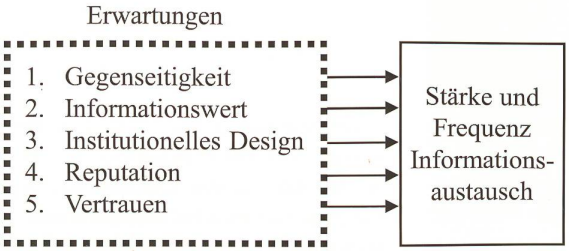
- Melde- und Analysestelle Informationssicherung (MELANI) https://www.melani.admin.ch/
- European Energy – Information Sharing & Analysis Centre (EE-ISAC) http://www.ee-isac.eu
- Water- Information Sharing & Analysis Centre https://www.waterisac.org

Beispiele für ISACs als Teil der Staatsbürokratie mit Zwangsmitgliedschaft:

- Aviation Information Sharing and Analysis Center (A-ISAC) https://www.a-isac.com
- Public Transportation Information Sharing and Analysis Center (PT-ISAC) http://www.apta.com/resources/safetyandsecurity/Pages/ISAC.aspx
- Emergency Services (EMR-ISAC) https://www.usfa.fema.gov/operations/ops_cip_emr-isac.html

interessiert, möglichst günstig oder kostenlos von den Informationen anderer Betreiber zu profitieren. Francis Bacons Maxime *Wissen ist Macht* führt daher zu kontraproduktiven Ergebnissen. Aus diesem Grund wurden in vielen Nationen spezialisierte Zentren gegründet, die das Teilen von Informationen erleichtern sollen (*ISAC,* siehe Kasten). Ohne die Schaffung solcher Zentren kommt kein freiwilliger Informationsaustausch in Gang.

Bestimmungsfaktoren des freiwilligen Teilens von Information



Nicht jeder dieser ISACs erfüllt jedoch auch seinen Zweck. Während der Informationsaustausch in einigen Fällen gut funktioniert, bleibt er in vielen Fällen unbedeutend. Daher hat die Dozentur Militärökonomie der MILAK in Zusammenarbeit mit der Melde- und Analysestelle Informationssicherung (MELANI) eine empirische Untersuchung durchgeführt. Als Resultat ergab sich ein verhaltensökonomisches Modell, das erklären kann, wann und wie Informationen zur Cyber-Sicherheit freiwillig geteilt werden (vgl. Abbildung)[2]. Der mit Abstand stärkste Entscheidungsfaktor in diesem Modell ist das institutionelle Design, das heisst die Art und Weise, wie der ISAC organisiert ist.

Auf die Organisation kommt es an

Es reicht daher nicht, einfach einen ISAC zu schaffen – dieser muss auch zielführend organisiert sein. Anhand der Ergebnisse wird deutlich, dass die Betreiber nicht zum Teilen von Informationen gezwungen werden können – etwa durch Regulierung oder Berichtspflichten. Vielmehr werden sie Information untereinander nur dann austauschen, wenn sie sich gegenseitig einen Nutzen hiervon versprechen und die Organisation des ISAC einen geschützten Rahmen bietet, der zu positiven externen Effekten führt.

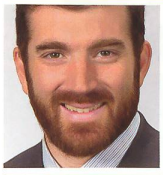
Nur wenn die Organisation des ISACs das individuelle Eigeninteresse des Betreibers aufnehmen und in den Dienst der Sicherheit des Cyber-Raums stellen kann, ist die Cyber-Abwehr effektiv. Der öffentlich-politischen Sphäre kommt hierbei die Verantwortung zu, den ISAC so zu organisieren, dass ein vertrauensvoller Rahmen für den Informationsaustausch geschaffen werden kann. Während sich unsere Studie auf ISACs konzentriert hat, sind die Ergebnisse auch auf andere Aspekte nachrichtendienstlicher Zusammenarbeit übertragbar. In der Fortsetzung dieses Artikels betrachten wir einige Organisationsmodelle, die im heute im privaten Sektor im Bereich big data – Analytik bereits erfolgreich eingesetzt werden, und diskutieren deren Anwendbarkeit im militärischen Bereich. ■

1 Laube S, Böhme R. 2017. Strategic Aspects of Cyber Risk Information Sharing. ACM Comput Surv 50(5).

2 Die vollständige Dokumentation der empirischen Methodik und der Ergebnisse ist verfügbar in Mermoud, A., Keupp, M.M. Huguenin, K., Palmié, M., Percia David, D. 2018. Incentives for Human Agents to Share Security Information: A Model and an Empirical Test. Proceedings of the 17th Workshop on the Economics of Information Security (WEIS).


Marcus M. Keupp
PD Dr. oec. HSG
Dozent Militärökonomie
MILAK
8903 Birmensdorf ZH


Hptm
Alain Mermoud
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH


Hptm
Dimitri Percia David
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH