Informationsaustausch im Bereich Cybersecurity

satw it's all about technology

Herausforderungen für die Schweiz

Kontext

Die Kultur des Digitalen und der Cybersecurity basieren auf dem Austausch von Informationen und dem Bereitstellen der notwendigen Kenntnisse, um die nötigen Kompetenzen in Politik, Wirtschaft, Management, Soziologie, Recht und Technologie aufzubauen (Abbildung 1). Die Informationsaustausch- und Analysezentren (ISACs – Information Sharing & Analysis Center) befassen sich hauptsächlich mit technischen Informationen. Sie sind ein Typ von Informationsaustauschplattformen, die mit Cybersecurity verknüpft sind und die auch davon Kenntnis haben, dass andere existieren können (IE-Plattform - IE für Information Exchanges).

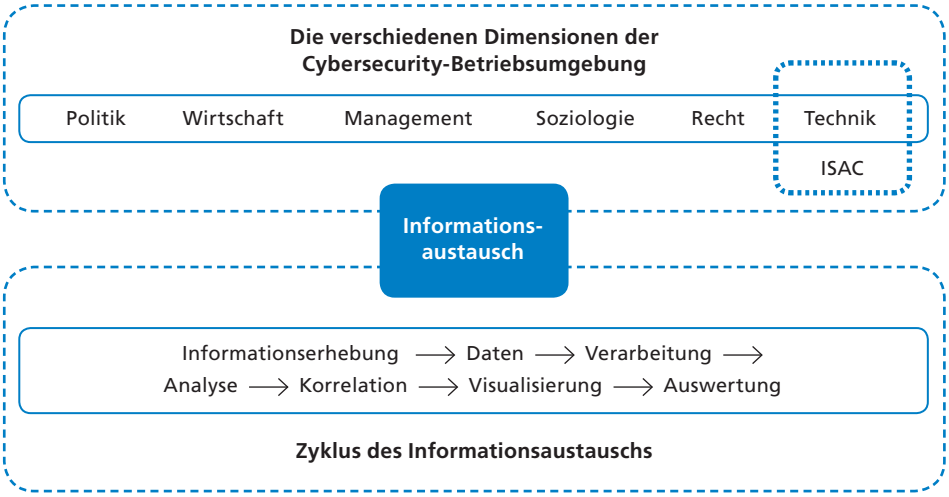

Abbildung 1
Informationsaustausch und die fachübergreifenden Dimensionen der Cybersecurity.

Bei Cyber-Angriffen, die den wirtschaftlichen Interessen einer Organisation schaden können, darf man die nachstehenden Folgen nicht unterschätzen:

- Verlust von immateriellen Vermögenswerten (Reputation, geistiges Eigentum), Verlust von geschäftlichen Chancen;
- Aktionen zur wirtschaftlichen Einflussnahme (Überwachung, Spionage, Sabotage, Terrorismus und Erpressung).

Gute Kenntnisse, wie diese wirtschaftlichen Einflussnahmen vor dem Hintergrund der Möglichkeiten der digitalen Welt funktionieren, tragen dazu bei, die Wettbewerbsvorteile von Unternehmen zu wahren. Dies trägt zu einem angemessenen Schutz des wissenschaftlichen, technischen, wirtschaftlichen und industriellen Kapitals des eigenen Landes und zur guten Gesundheit des wirtschaftlichen Standorts bei. In all diesen Bereichen ist ein entsprechender Informationsaustausch erforderlich, der von Massnahmen zur Risikoprävention und zum Schutz der Vermögenswerte begleitet werden muss.

Auf nationaler Ebene

Einzelpersonen, Organisationen und auch der Staat sind mit Cyber-Risiken und der Notwendigkeit konfrontiert, ihre Sicherheit und ihre Widerstandsfähigkeit zu stärken. Seit einiger Zeit bedingt die Souveränität einer Nation auch die Kontrolle von Cyber-Risiken und die Fähigkeit, Cyber-Angriffe zu verhindern und darauf zu reagieren, vor allem wenn sie die gesamte Gesellschaft betreffen können, einschliesslich den für ein reibungsloses Funktionieren notwendigen Infrastrukturen.

Die wichtigen Funktionen eines Staates können durch eine mangelhafte Beherrschung digitaler Herausforderungen und Fragen der Cybersecurity beeinträchtigt werden, vor allem in den Bereichen Landesverteidigung, Diplomatie, Polizei, öffentliche Sicherheit, Demokratie, Schutz kritischer Infrastrukturen, Wirtschaft und Finanzplatz Schweiz. Die Wirtschaftsleistung der Schweiz hängt heutzutage in hohem Masse vom Funktionieren des digitalen Ökosystems und seiner Cybersecurity ab.

Bestimmte Akteure verstehen es je nach Motivation und Umständen, wie sie die im Internet angebotenen Möglichkeiten nutzen können, um Schaden anzurichten, zu destabilisieren, zu beeinflussen, zu kontrollieren, auszuspionieren, zu stehlen, sich illegal zu bereichern, Macht zu gewinnen oder terroristische und konfliktbezogene Aktionen zu unterstützen.

Es ist eine komplexe und schwierige Aufgabe, Werte zu schützen, Störungen und Krisen zu erkennen und zu bekämpfen, Sicherheitsmängel zu beheben sowie Sicherheits- und Verteidigungsmassnahmen so zu optimieren, dass sie wirksam und effizient sind. Für diese Ausgabe ist der Informationsaustausch eines der Reaktionselemente.

Die Cybersecurity steht in einem Kontext wirtschaftlicher Wettbewerbsfähigkeit und geopolitischer Spannungen. In der Schweiz erfolgt der Informationsaustausch zur Gewährleistung wirtschaftlicher und politischer Stabilität auf mehreren Ebenen: auf den Ebenen der Zivilgesellschaft, der privaten Organisationen, des Bundes und der Kantone sowie in einer Logik der nationalen und internationalen Zusammenarbeit. Diese stehen im Jahr 2018 im Mittelpunkt der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), die auf einem dezentralen Ansatz und der Eigenverantwortung aller Akteure basiert.

Dies erfordert organisatorische, technische, prozedurale und menschliche Massnahmen sowie Anreize für Besitzer von «nützlichen Informationen», sich an der Weitergabe zu beteiligen und davon zu profitieren.

Auf internationaler Ebene

Eine nachhaltige Sicherheit nationaler digitaler Infrastrukturen kann nur verbessert werden, wenn die Staaten auf internationaler Ebene zusammenarbeiten und gemeinsam die Spielregeln festlegen, die im Cyberspace allgemein akzeptiert werden. Bei der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022[1] erkennt der Bundesrat an, dass die Schweiz sich international aktiv positionieren muss, um Cyber-Risiken präventiv, reaktiv, effektiv und kohärent zu begegnen. Der Bundesrat setzt so ein starkes Signal, weil er anerkennt, dass der Cyberspace eine neue Dimension in der Sicherheits- und Aussenpolitik geschaffen hat.

Die sicherheits- und aussenpolitischen Aufgaben konzentrieren sich auf eine friedliche Nutzung des Cyberspace. Dazu ist «die Ausarbeitung eines Regelwerks für einen verantwortungsvollen Umgang mit IKT» von erstrangiger Bedeutung. Grundlage dafür sind die Anwendung des Völkerrechts, internationale und regionale Dialogprozesse (UNO, OSZE usw.) sowie internationale und regionale Plattformen für den Dialog über Cybersecurity, in welche die Schweiz aktiv einbezogen ist. Der Informationsaustausch zwischen den Beteiligten trägt dazu bei, Fragen wie die folgenden Punkte anzugehen: Wo liegen die Grenzen für eine Nutzung des Cyberspace zur Konfliktlösung? Wie können Staaten gesetzwidrige Aktivitäten nichtstaatlicher Akteure aus ihrem Hoheitsgebiet heraus verhindern?

Das Eidgenössische Departement für auswärtige Angelegenheiten EDA hat ein «Büro des Sonderbeauftragten für Sicherheits- und Aussenpolitik im Cyberspace» eingerichtet, um die Teilnahme der Schweiz am internationalen Dialog und Informationsaustausch zu institutionalisieren[2].

---

[1] Nationale Schutzstrategie der Schweiz gegen Cyber-Risiken 2018-2022
https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

[2] https://www.staatskalender.admin.ch/navigate.html?dn=ou=Cyber-Aussen-%20und%20-Sicherheitspolitik,ou=Abteilung%20Sicherheitspolitik,ou=Politische%20Direktion,ou=Staatssekretariat,ou=Eidg.%20Dep.%20fuer%20auswaertige%20Angelegenheiten,ou=bundesrat&localeString=Deutsch

Fünf Anwendungen für den Informationsaustausch im Bereich Cybersecurity

Sensibilisierung und Schulung
Die Sensibilisierung der Akteure des digitalen Ökosystems für Bedrohungen und Risiken sowie die Bereitstellung von Mitteln für verantwortungsbewusstes Verhalten sowie Vorsorge-, Schutz- und Verteidigungsmassnahmen sind jeweils Teil des Informationsaustauschs. Dies trägt insgesamt zur Verbesserung der Cybersecurity, zur Widerstandsfähigkeit und zum Kampf gegen Cyber-Bedrohungen bei.

Informationsmassnahmen für die Öffentlichkeit sind möglich, wenn es darum geht, Informationen generell über Sicherheit, öffentliche Sicherheit und den Schutz der Bevölkerung zu vermitteln, vor allem in Fällen eines Krisenmanagements mit Cyber-Dimension. In einigen Fällen können soziale Medien als Plattform für den Informationsaustausch dienen, insbesondere wenn es darum geht, schnell mit der Bevölkerung zu interagieren. Sie tragen zur Sensibilisierung sowie zur Verbreitung von Warnungen oder Sicherheitshinweisen bei.

Die Fortbildung von Schülern und Studierenden, angehenden Fachleuten (Ingenieuren, Technikern, Juristen, Polizisten, Administratoren, Managern und Akteuren im öffentlichen und privaten Sektor), arbeitenden und nicht-arbeitenden Menschen sowie Senioren ist für die Cybersecurity wichtig. Somit gilt diese Fortbildung als erste Grundlage des Informationsaustauschs. Sie ist ein Ansatzpunkt, um hinsichtlich Sicherheit von Computern, Telekommunikationsnetzen, Informationssystemen und den damit verbundenen Objekten zu einer Cybersecurity «by design» beizutragen.

Beteiligung an einer Kultur der Cybersecurity
Einige private, im Bereich der Cybersecurity tätige Organisationen tauschen innerhalb der Gesellschaft Informationen ad hoc oder regelmässig in Form kostenloser oder kostenpflichtiger Abonnements aus. Sie alle tragen zur Verbreitung einer Kultur der Cybersecurity bei, mit welcher der Kenntnisstand der Beteiligten verbessert wird, sei es in Form von Newslettern, Berichten, strategischen oder operativen Überwachungsdiensten beispielsweise einem technischen oder rechtlichen Monitoring.

Neben diesen Ansätzen gibt es Massnahmen vor allem von Verbänden, Hochschulen, Lösungsanbietern, der Versicherungswirtschaft oder auch von Veranstaltern, Medien und Handelskammern. Sie organisieren Treffen, Konferenzen, Foren, Ausstellungen und verbreiten Informationsmaterialien zum Thema Cybersecurity. Dies trägt dazu bei, Informationen auszutauschen und das Bewusstsein für die Notwendigkeit zu schärfen, mit Cyber-Risiken umzugehen, und den Kenntnisstand und die Fähigkeiten zu verbessern, um die für die wirtschaftliche Entwicklung des Landes erforderlichen menschlichen Ressourcen aufzubauen.

Bekämpfung der Cyber-Kriminalität

In der Schweiz[3] ist die vom Bund und den Kantonen gemeinsam finanzierte Nationale Koordinierungsstelle zur Bekämpfung der Internetkriminalität (KOBIK) seit 2003 tätig[4].

Das den Opfern bereitgestellte Formular, um Straftaten, Betrugsfälle, Verbrechen oder verdächtige Inhalte an das Bundesamt für Polizei (Fedpol) zu melden, ist ein Instrument für den Informationsaustausch[5] und ein bevorzugter Kommunikationskanal zur Berücksichtigung der ständig wachsenden Opferzahlen. Diese Kommunikationsplattformen sind jedoch keine Plattformen, um Opfer von Cyber-Verbrechen zu unterstützen.

Die Schweiz verfügt über eine Melde- und Analysestelle für die Informationssicherung (MELANI)[6], die im Bereich der Informationssysteme und der Cybersecurity zum Informationsaustausch beiträgt. Dies geschieht vor allem durch verschiedene Dokumentationen, Newsletter und eine Präsentation häufig auftretender Fälle oder Störungsmeldungen. Die Aufgabe von MELANI kann ohne einen Informationsaustausch zwischen verschiedenen privaten und öffentlichen Einrichtungen und mit privilegierten Partnern nicht erfüllt werden.

Für eine wirksame Bekämpfung der Cyber-Kriminalität ist ein präventiver Ansatz erforderlich, mit dem der Cyberspace weniger Boden für jede Art von Kriminalität bietet und kriminelle Möglichkeiten verringert werden. Daher müssen die Durchführung von Cyber-Angriffen erschwert – durch Erhöhen des Aufwands in Bezug auf Kompetenzen und Ressourcen für Verbrecher und durch Verringern der zu erwartenden Gewinne – und das Risiko für Kriminelle erhöht werden, dass diese identifiziert, lokalisiert, verhaftet und verfolgt werden[7]. Alle diese Massnahmen können nur konzipiert und umgesetzt werden, wenn zwischen allen Akteuren des digitalen Ökosystems ein effizienter Informationsaustausch stattfindet.

Schaffung von Cybersecurity

Die von der ISO (International Organization for Standardization) oder der ITU (International Telecommunication Union) entwickelten internationalen Normen tragen zur Entwicklung der Cybersecurity bei.[8, 9] Sie müssen als Mechanismen und Hebel für den Informationsaustausch betrachtet werden, beispielsweise die Normenfamilie ISO/IEC 27000, die sich mit verschiedenen Bereichen des Sicherheitsmanagements von Informationssystemen befasst.

Der private und der Verbandssektor sind auch ein Vektor für die Weitergabe von Empfehlungen und von bewährten Verfahren mit möglicherweise sektoraler, nationaler oder internationaler Reichweite, die technische oder betriebswirtschaftliche Bereiche betreffen. Egal ob Standards oder Benchmarks aus der Privatwirtschaft: Diese Dokumente werden meist mit Beteiligung verschiedener Vertreter der Berufswelt und der Zivilgesellschaft erstellt. Dies hat die vorherige Einführung eines Mechanismus erfordert, um Informationen in einem angepassten Format abzufragen, zu erheben und zu übermitteln sowie Informationen auszutauschen und die Ergebnisse dieses Austauschs zurückzugeben.

Beherrschung der Schwachstellen und der Sicherheitsvorfälle
Jede Komponente eines Informationssystems kann Schwachstellen enthalten und ausgenutzt werden, um die Sicherheit zu beeinträchtigen. Regelmässig werden neue Sicherheitslücken und Schwachstellen gemeldet und weitergegeben, um sie zu beheben.

Die amerikanische private und gemeinnützige Organisation MITRE, die sich seit 1958 mit Forschung und Entwicklung moderner Technologien in strategischen und wichtigen Bereichen befasst (Verteidigung, Sicherheit, Cyberspace usw.), führt seit 1999 das Register der Sicherheitslücken namens CVE (Common Vulnerabilities and Exposures).[10, 11] Das US-CERT (United States Computer Emergency Response Team National Cyber Awareness System – Homeland Security) erstellt daraus eine wöchentliche Zusammenfassung und teilt diese Lücken in vier Kategorien ein (hohe, mittlere, niedrige und noch nicht zugewiesene Schwere), beschreibt sie und benennt den anzuwendenden Sicherheitspatch. Die meisten Länder haben CERT-Einheiten (Computer Emergency Response Teams), die manchmal auch CSIRT (Computer Security Incident Response Team) genannt werden[12]. CERTs können privat oder öffentlich sein und sich auf bestimmte Tätigkeitsbereiche (akademisch, militärisch, öffentliche Verwaltung usw.) konzentrieren. Sie sind in einem Netzwerk organisiert und arbeiten zusammen, um bestimmte Informationen nach vordefinierten Regeln, Rollen, Verantwortlichkeiten, Kanälen und Kommunikationsformaten auszutauschen.

Ein Informationsaustausch- und Analysezentrum (ISAC) ist in der Regel eine Reaktion auf die Notwendigkeit, dass private und öffentliche Akteure zusammenarbeiten, um den Austausch von Informationen und bewährten Verfahren über eine vertrauenswürdige Stelle zu fördern (Abbildung 2). Der private und der öffentliche Bereich, die einige der nützlichen Informationen (Zwischenfälle, Bedrohungen, Schwachstellen, Sicherheitsmassnahmen, Störfallmanagement, Parameter, Trends usw.) kennen, müssen effizient zusammenarbeiten, um die Auswirkungen von Cyber-Risiken in der virtuellen oder physischen Welt einzudämmen und eine bessere Vorbereitung auf Bedrohungen zu gewährleisten.

---

[3] https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html

[4] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-23881.html

[5] https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/meldeformular.html

[6] https://www.melani.admin.ch/melani/de/home.html

[7] S. Ghernaouti, « La cybercriminalité, les nouvelles armes de pouvoir ». Le savoir suisse, PPUR 2017.

[8] https://www.iso.org/home.html

[9] https://www.itu.int/en/Pages/default.aspx

[10] https://www.mitre.org/

[11] https://cve.mitre.org/

[12] CERT ist eine in den USA von der Carnegie-Mellon-Universität eingetragene Marke. Es bedarf einer vorherigen Genehmigung, um diesen Namen zu verwenden, was beim Begriff CSIRT aber nicht der Fall ist.

Abbildung 2
Beispiele, um die Schaffung eines ISAC («Information Sharing & Analysis Center») zu begründen.

Es kann sektorspezifische ISACs in den Bereichen Finanzen, Energie, Luftfahrt, Verkehr oder auch Gesundheit geben. Nützliche Informationen werden geteilt, wenn Zeiträume, Art der Informationen, Analyse und die sich daraus ergebenden Sicherheitsmassnahmen an die erforderlichen Sicherheitsbedürfnisse angepasst werden müssen.

Ähnlich wie bei CERTs und CSIRTs liegt der Mehrwert eines ISAC in seiner Fähigkeit, Informationen zu erheben, zu verarbeiten und zurückzugeben, um die Sicherheit insbesondere hinsichtlich störfallbezogener Kenntnisse, Erkennung und Reaktionen zu stärken. Diese Prozesse zur Verbesserung der Sicherheit können je nach Herkunft, Relevanz, Geschwindigkeit von Erhebung und Verarbeitung der Daten mehr oder weniger effektiv sein. Aufgrund des globalen Vorkommens von Cyber-Angriffen und der Vernetzung der gemeinsamen Ziele ist eine Zusammenarbeit mit dem ISAC notwendig, um eine gute Reaktionsfähigkeit zu erreichen sowie grenz- und sektorübergreifende Cyber-Angriffe zu bekämpfen. So können die Identifizierung der Opfer, die Erkennung und Verbreitung der Wege und der Zwecke von Angriffen sowie die Anpassung der Schutz- und Abwehrmassnahmen optimiert werden. Die vernetzte Architektur von ISACs trägt dazu bei, ein globales Überwachungszentrum für die Sicherung digitaler Infrastrukturen zu schaffen. Dies kann beispielsweise Frühwarnungen für Länder und Systeme ermöglichen, die weit vor den ersten Auswirkungen der Cyber-Angriffe erfolgen und somit eine bessere Reaktionsfähigkeit unterstützen. Angesichts von Cyber-Epidemien, des massiven Ausmasses bestimmter Cyber-Angriffe wie Wannacry und NotPetya im Jahr 2017 und der Möglichkeit, diese schnellstmöglich abzustellen und gleichzeitig die Verbreitung von bösartigem Code zu begrenzen, sind eine schnelle Organisation und Reaktionsfähigkeit erforderlich. Die ISACs können diesen Bedarf abdecken, wenn sie richtig konzipiert, verwaltet, implementiert und genutzt werden. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sieht die Zusammenarbeit zwischen privatem und öffentlichem Sektor («Public Private Partnerships» oder PPPs) als grosse Herausforderung für die Inbetriebnahme eines ISAC[13].

[13] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Schlussfolgerung und Empfehlungen

Förderung eines Ansatzes für den Informationsaustausch

Die Herausforderung des Austauschs liegt vor allem darin, die Beteiligten davon zu überzeugen, dass sie ihre Informationen auch mit anderen einschliesslich möglicher Wettbewerber teilen sollen. Der erwartete Nutzen des Austauschs muss in einem unmittelbaren Verhältnis zu den anfallenden direkten und indirekten Kosten stehen. Wenn es um den Austausch von Informationen mit hohem Mehrwert geht (und nicht Wiederholung von weit verbreiteten und über verschiedene Kanäle zugänglichen Informationen) müssen die Teilnehmer motiviert werden, ein gemeinsames Spiel mit Anreizen und Belohnungen einzugehen und Interessenkonflikte möglicherweise zu lösen. Somit müssen die Beteiligten nicht nur für den Wert des Informationsaustauschs sensibilisiert und davon überzeugt werden, sondern es sollte auch der Mehrwert des Austauschs durch greifbare Vorteile hinsichtlich Stärkung der Cybersecurity und Haltungen der Cyber-Widerstandskraft (Vorteile in Bezug auf Leistung, aber zum Beispiel auch Qualität, Kosten, Komfort, Kenntnisse, Einfluss oder Reputation) aufgezeigt werden.

Überzeugen oder Zwingen

Der Trend, Probleme der Cybersecurity durch Künstliche Intelligenz zu lösen, die aus riesigen Datensammlungen (grosse Datenmengen, Deep Learning usw.) entwickelt wurde, ermutigt private Akteure nicht unbedingt, ihre Informationen auszutauschen. Diese Informationen können genutzt werden, um die Sicherheitslage der Gemeinschaft zu stärken, ebenso aber, um ein kommerzielles Angebot zu entwickeln. Dies verschafft oder ermöglicht einen Wettbewerbsvorteil für die Akteure, die wissen, wie sie die richtigen Informationen zur rechten Zeit nutzen können. Tatsächlich müssen Daten über Sicherheitsvorfälle gesammelt, erhoben, mit Daten über frühere Vorfälle korreliert und analysiert werden, um die Wissensdatenbank zu den Unsicherheitsfaktoren (Zwischenfälle, Schwachstellen, Angriffe, Konzepte und Begriffe, die mit dem Konzept der Intelligenz von Cyber-Angriffen allgemein identifiziert werden) zu erweitern. So können Sicherheitslösungen angepasst und Sicherheitsarchitekturen entsprechend verbessert werden.

Sollte jemand von einem freiwilligen Ansatz des Informationsaustauschs nicht überzeugt werden können, so ist es manchmal notwendig, die Akteure auf juristischem Wege zu zwingen, eine bestimmte Art von Informationen zu übermitteln (beispielsweise die gesetzliche Verpflichtung, Cyber-Angriffe zu melden). Dazu müssen ein passender und anwendbarer Rechtsrahmen sowie eine Organisationsstruktur vorhanden sein.

Solidarität und Gegenseitigkeit

Etwas mit jemandem auszutauschen bedeutet, einem Dritten einen Teil dessen zu geben, was man besitzt, erwirbt oder erhält. Es bedeutet ebenso etwas zu teilen, aber auch an etwas gleichzeitig mit anderen teilzunehmen, also auf eine verantwortungsvolle Weise teilzunehmen. Das setzt eine Solidarität zwischen den Akteuren, eine gewisse Gegenseitigkeit, Respekt und Vertrauen voraus. Es geht darum, einen kollektiven Informationsdienst zu entwickeln und zu schaffen, der durch eine angepasste Sicherheitspolitik unterstützt wird. Die Tabelle in Abbildung 3 fasst die Empfehlungen für die Schaffung eines Zentrums für den Informationsaustausch im Bereich Cybersecurity zusammen.

Strategische Empfehlungen

- Identifizieren der Akteure, der Zwecke und der Vorteile eines kurz-, mittel- und langfristigen Informationsaustauschs (Anbieter von Infrastrukturen oder von Diensten, Nutzergruppen, Bündelung von Ressourcen usw., siehe Abbildung 2).
- Festlegen der Bewertungsmittel für die erwarteten Vorteile und Definieren der Leistungsbewertungsindikatoren (Leistungs- und Steuerungsindikatoren).
- Definieren des Austauschumfangs (innerhalb der Organisation, zwischen Organisationen, sektorweite Organisationen, nationale bzw. internationale Ebene).
- Schaffen der notwendigen Partnerschaften durch Festlegung der Massnahmen, mit denen diese Partnerschaften unter Berücksichtigung der rechtlichen, ordnungspolitischen und haushaltspolitischen Zwänge geschaffen werden können.
- Identifizieren und Anpassen bestehender Organisationsstrukturen, die zum Informationsaustausch beitragen oder neue IT-Strukturen und -Infrastrukturen für einen effektiven und effizienten Informationsaustausch schaffen können.
- Bestimmen, wem die Austausch- und Weitergabeplattform gehört sowie wie sie gesichert, betrieben und gewartet wird.
- Definieren der Verantwortlichkeiten, Rechte und Pflichten jedes Beteiligten.
- Unterstützen von Austauschansatz und -infrastruktur durch strategische und operative Sicherheits- und Verteidigungsmassnahmen.

Abbildung 3
Zusammenfassung der Empfehlungen für die Schaffung eines Zentrums für den Informationsaustausch im Bereich Cybersecurity.

Technische Empfehlungen

- Identifizieren der Art und Weise, wie Informationen auszutauschen sind (Art, Herkunft, Format, Qualität, Zuverlässigkeit, Wahrhaftigkeit und Lebensdauer).
- Definieren der Art und Weise, wie Informationen erhoben, gespeichert, verarbeitet, präsentiert, zurückgegeben und gesichert werden.
- Definieren der für die Austauschplattform notwendigen IT-Infrastruktur (Hardware, Software, Telekommunikationsnetze).

Personelle, betriebswirtschaftliche und wirtschaftliche Empfehlungen

- Einrichten der erforderlichen Kompetenzen (personelle Ressourcen in den Bereichen Recht, Management, Organisation, Kommunikation, Technik, Datenanalyse und Datenvisualisierung usw.).
- Zuweisen der notwendigen Mittel und Ressourcen (finanzielle, organisatorische, prozedurale und technische Kapazitäten).
- Identifizieren und Kommunizieren der Anreize, die den Informationsaustausch fördern (Vorteile, Belohnungen usw.).

Zusammenfassung

Diese Publikation beleuchtet die Praktiken des Informationsaustauschs im Bereich Cybersecurity. Sie fasst zusammen und analysiert den Kontext, die Bedürfnisse und die Einschränkungen des Informationsaustauschs, um Sicherheit und Widerstandsfähigkeit sowie die Bekämpfung der Cyber-Kriminalität sicherzustellen. Die Publikation identifiziert die verschiedenen Arten von Informationen, die ausgetauscht werden können, sowie die wichtigsten Vektoren für den Informationsaustausch in der Schweiz und auf internationaler Ebene. Sie zeigt Anwendungen des Informationsaustauschs im Bereich der Cybersecurity und zeigt die Vor- und Nachteile eines Informationsaustausch- und Analysezentrums (ISAC) und die wichtigsten Erfolgsfaktoren eines solchen Systems auf.

Abschliessend werden vorrangige Empfehlungen für die Einrichtung einer Plattform für Informationsaustausch und -analyse ausgesprochen.

Impressum

Autoren: Solange Ghernaouti, Laura Crespo,
Bastien Wanner – Universität Lausanne,
Swiss Cybersecurity Advisory & Research Group
(www.scarg.org)

satw it's all about technology

Schweizerische Akademie der Technischen Wissenschaften SATW
St. Annagasse 18 | 8001 Zürich | 044 226 50 11 | info@satw.ch | www.satw.ch