Ilmenauer Beiträge zur Wirtschaftsinformatik

Herausgegeben von U. Bankhofer, V. Nissen
D. Stelzer und S. Straßburger

Martin Werchan, Daniel Fischer, Clemens Sauerwein,
Dirk Stelzer

Nutzung von Threat Intelligence Sharing Platforms – eine empirische Untersuchung im DACH-Raum

Arbeitsbericht Nr. 2023-02, Dezember 2023

Technische Universität Ilmenau
Fakultät für Wirtschaftswissenschaften und Medien
Institut für Wirtschaftsinformatik

Autor: Martin Werchan, Daniel Fischer, Clemens Sauerwein, Dirk Stelzer

Titel: Nutzung von Threat Intelligence Sharing Platforms – eine empirische Untersuchung im DACH-Raum

Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2023-02, Technische Universität Ilmenau, 2023

ISSN 1861-9223

ISBN 978-3-938940-67-9

urn:nbn:de:gbv:ilm1-2023200323

Anschrift: Technische Universität Ilmenau, Fakultät für Wirtschaftswissenschaften und Medien, Institut für Wirtschaftsinformatik, PF 100565, D-98684 Ilmenau.

Gliederung

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
AIS	Association for Information Systems
ATX	Austrian Traded Index
AWS	Amazon Web Services
BAR	Schweizerisches Bundesarchiv
BISP	BSI Information Sharing Portal
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CSIRT	Computer Security Incident Response Team
CSV	Comma-separated values
CTI	Cyber Threat Intelligence
CybOX	Cyber Observable Expression
DAX	Deutscher Aktienindex
DNS	Domain Name System
DSG	Schweizer Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
EDR	Endpoint Detection and Response
EJPD	Eidgenössisches Justiz- und Polizeidepartement
IBM	International Business Machines Corporation
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IODEF	Incident Object Description Exchange Format
IPS	Intrusion Prevention System

ISC	Informatik Service Center
IT.NRW	Landesbetrieb Information und Technik Nordrhein-Westfalen
ITZBund	Informationstechnikzentrum Bund
KMU	Kleine und mittlere Unternehmen
MDAX	Mid-Cap-DAX
MISP	Malware Information Sharing Platform
NCSC	Nationales Zentrum für Cybersicherheit
OTX	Open Threat Exchange
SANS	SysAdmin, Audit, Networking and Security
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SIEM	Security Information and Event Management
SMI	Swiss Market Index
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
STIX	Standard Threat Information Expression
TI	Threat Intelligence
TIS	Threat Intelligence Sharing
TTI	Technische Threat Intelligence
TTP	Taktiken, Techniken und Prozeduren
XDR	Extended Detection and Response

Zusammenfassung: Die Bedrohungen der IT-Sicherheit werden häufiger und komplexer. Organisationen tauschen vermehrt Bedrohungs- und Sicherheitsinformationen aus, um sich dieser Herausforderung zu stellen. Dabei unterstützen Threat Intelligence Sharing Platforms die automatisierte Sammlung, Vorverarbeitung, Analyse und Verteilung von Bedrohungs-und Sicherheitsinformationen. Bisher gibt es wenige Erkenntnisse über die Verbreitung und Nutzung dieser Plattformen im deutschsprachigen Raum. Um diese Forschungslücke zu schließen, wird in diesem Arbeitsbericht untersucht, wie verbreitet Threat Intelligence Sharing Platforms im DACH-Raum sind und wie genau diese genutzt werden. Zur Zielerreichung erfolgt zuerst die Durchführung einer multivokalen Literaturanalyse, aus der Hypothesen und Fragen für eine empirische Untersuchung resultieren. Anschließend werden mittels eines Online-Fragebogens 380 Verantwortliche für die IT-Sicherheit in börsennotierten Unternehmen, Bundesbehörden und Universitäten in Deutschland, Österreich und der Schweiz befragt, von denen 69 vollständig antworteten. Mehr als die Hälfte der befragten Organisationen setzen Threat Intelligence Sharing Platforms ein. 84,2 Prozent der Unternehmen verwenden derartige Plattformen und damit signifikant mehr als Behörden (48,3 Prozent) und Universitäten (33,3 Prozent). Je wichtiger der Stellenwert der IT-Sicherheit für die Organisationen ist und je mehr Personen im Bereich der IT-Sicherheit beschäftigt sind, desto häufiger setzen diese Threat Intelligence Sharing Platforms ein. Vier von fünf Organisationen, die ein CERT, SOC oder CSIRT betreiben, setzen Threat Intelligence Sharing Platforms ein. Von den Organisationen, die Threat Intelligence Sharing Platforms einsetzen, nutzen nahezu zwei Drittel Malware Information Sharing Platform (MISP). Diese Plattform ist mit Abstand marktführend im DACH-Raum. Am wichtigsten sind den Organisationen bei der Auswahl von Threat Intelligence Sharing Platforms eine hohe Verbreitung der Plattform, niedrige Lizenzkosten, ein großer Funktionsumfang sowie der Umfang der angebotenen Bedrohungsinformationen. Fast jede zweite Organisation, die Threat Intelligence Sharing Platforms einsetzt, nutzt mehrere Plattformen gleichzeitig. Organisationen nutzen eher externe als interne Threat Intelligence Sharing Platforms und teilen Threat Intelligence eher mit externen als mit internen Stellen. Mehr als zwei Drittel der Organisationen verbinden oder integrieren die Plattformen mit anderen organisationsinternen IT-Sicherheitssystemen, am häufigsten mit SIEM-Systemen.

Schlüsselworte: Threat Intelligence, Sharing Platforms, Nutzung, Verbreitung, Empirische Untersuchung

Hinweis: Ausgewählte Inhalte dieses Arbeitsberichts sind in gekürzten Fassungen bereits in [FSWS2023] und [FWS2023] erschienen.

1 Einleitung

1.1 Problemstellung

Die Sicherheit von IT-Systemen ist einer der zentralen Erfolgsfaktoren der Digitalisierung. Unternehmen, Behörden und Universitäten verfügen aber oft nicht über ausreichende Ressourcen, um in ihren IT-Systemen angemessene Sicherheitsniveaus zu gewährleisten [BrLe2021, 17]. Eine Option zur Verringerung des Ressourcenproblems ist die intensive Automatisierung von Teilaufgaben des IT-Sicherheitsmanagements. Threat Intelligence Sharing Platforms (TIS-Platforms) können hierfür ein wichtiger Baustein sein. Dabei handelt es sich um Internet-basierte Plattformen für den organisationsübergreifenden Austausch von Bedrohungs- und Sicherheitsinformationen. Threat Intelligence Sharing Platforms unterstützen die Sammlung von Daten aus verschiedenen Quellen, deren Aggregation und kooperative Auswertung sowie den Export der Analysedaten in IT-Systemen von Unternehmen, Behörden und Universitäten [DaSe2013, 2]. Sie ermöglichen eine effektive und effiziente Erkennung und Bekämpfung von Sicherheitsvorfällen. Diverse Anbieter bieten dafür Softwarelösungen an, mit teils erheblichen Funktionsunterschieden [SFRR+2021, 7].

Bisher publizierte Studien behandeln im Wesentlichen die Perspektive der Plattform-Anbieter. Es existieren Marktüberblicke und Instrumente, um Threat Intelligence Sharing Platforms zu vergleichen [ToRa2018; BGSe2015; BFSL+2020]. Die Sicht der Anwender ist allerdings deutlich weniger erforscht. Es gibt einzelne Fallstudien, die den Einsatz der Plattformen in Organisationen beschreiben [WDWI2016; SSFi2016; YaKa2019]. Weiterhin existieren vereinzelt globale Untersuchungen zur Nutzung von Threat Intelligence Sharing Platforms. Beispielsweise führt das SANS-Institut[1] jährlich eine Befragung zum Einsatz von Threat Intelligence in Organisationen durch [BrSt2022, 3]. Eine detaillierte Untersuchung für den DACH-Raum ist bisher nicht publiziert worden. Zudem gibt es nur wenige Untersuchungen zur Verbreitung einzelner Plattformen. Auch fehlen detaillierte Erkenntnisse über die Nutzer und die Art und Weise der Nutzung von Threat Intelligence Sharing Platforms in Organisationen.

[1] Das SANS-Institut ist eine genossenschaftlich organisierte Forschungs- und Ausbildungsorganisation mit Schwerpunkt IT-Sicherheit.

1.2 Zielsetzung

Ziel dieser Studie ist es zu untersuchen, wie verbreitet Threat Intelligence Sharing Platforms in Deutschland, Österreich und der Schweiz sind und wie genau sie in Unternehmen, Behörden und Universitäten genutzt werden.[2]

1.3 Methodik

Um das Ziel zu erreichen, wurde eine empirische Untersuchung durchgeführt. Zur Vorbereitung wurde eine Literaturanalyse basierend auf den Methoden von Webster und Watson [WeWa2002] sowie Wohlin [Wohl2014] durchgeführt. Da das Themengebiet praxisnah ist, wurde auch graue Literatur aus einer multivokalen Literaturanalyse berücksichtigt [GFMä2019]. Abb. 1-1 stellt die Durchführung der Literaturanalyse im Überblick dar.

Zuerst erfolgte anhand der Zielsetzung die Festlegung der Suchstrategie. Für die initiale Suche wurde folgender Suchterm verwendet:

(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service* OR tool* OR system*) AND (market OR study OR survey OR overview OR analysis))*.

Als Literaturdatenbanken dienten ACM Digital Library, AIS eLibrary, EBSCOhost, IEEE Xplore, Taylor & Francis Online und Wiley Online Library. Die Suche erfolgte in Titel, Abstract sowie Keywords der Literaturdatenbanken, mit der Eingrenzung auf Veröffentlichungen nach 2018, um die jüngsten Entwicklungen im Forschungsgebiet abzudecken. Zudem wurden führende Publikationen der Informatik und Wirtschaftsinformatik berücksichtigt, wie zum einen Fachzeitschriften, die im Senior Scholars‘ Basket of Journals [Asso2011] gelistet sind. Zum anderen wurden Zeitschriften und Konferenzen berücksichtigt, die im Teilbereich der Wirtschaftsinformatik des VHB-JOURQUAL3-Rankings [Verb2015, 1] mit A+ oder A bewertetet sind.

[2] Weitere, spezifischere Forschungsfragen sind in Anhang 1 aufgelistet.

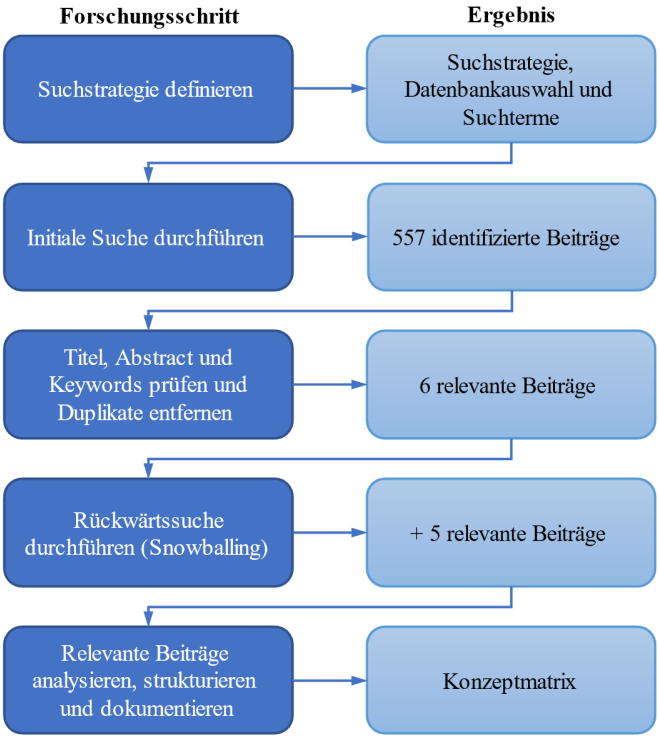

Abb. 1-1: Ablauf der Literaturanalyse

Die initiale Suche ergab 557 Ergebnisse.[3] Im nächsten Schritt fand eine Selektion der Publikationen statt. Entfernt wurden Duplikate und Beiträge, die nicht im Volltext oder nicht in deutscher oder englischer Sprache vorlagen. Bei den verbleibenden Publikationen fand eine Prüfung der Titel, Abstracts, Keywords und gegebenenfalls der Volltexte statt. Nach dieser Selektion verblieben sechs relevante Beiträge. Um weitere Forschungsergebnisse zu ermitteln, erfolgte im nächsten Schritt eine Rückwärtssuche. Daraufhin konnten fünf weitere, relevante Beiträge identifiziert werden.[4] Abschließend wurde aus den elf relevanten Beiträgen eine Konzeptmatrix erstellt, die in Anhang 4 abgebildet ist.

Für die multivokale Literaturanalyse erfolgte eine Google-Suche mit dem folgenden Suchterm:

("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)

[3] Weitere Details zur initialen Suche sind in Anhang 2 dokumentiert.
[4] Die Ergebnisse der Rückwärtssuche sind in Anhang 3 dargestellt.

Die Suche ab dem Jahr 2018 ergab 158.000 Ergebnisse, wovon die ersten hundert Treffer berücksichtigt wurden (Stand: 28.03.2022).

Basierend auf der untersuchten Literatur wurden Hypothesen über die Verbreitung und den Einsatz von Threat Intelligence Sharing Platforms aufgestellt. Danach erfolgte die Ermittlung von Fragen, die zum Bestätigen oder Widerlegen der Hypothesen dienen. Anschließend wurden die ermittelten Fragen in einen Qualtrics Online-Fragebogen überführt. Die Stichprobe umfasst Verantwortliche für Informationssicherheit in Behörden, Universitäten und Unternehmen, die im Deutschen Aktienindex (DAX), dem Austrian Traded Index (ATX) sowie dem Swiss Market Index (SMI) gelistet sind.

Die Auswertung der Befragungsergebnisse erfolgte mittels Microsoft Excel[5]. Abschließend wurden die Ergebnisse der statistischen Analyse unter Berücksichtigung der Resultate aus der Literaturanalyse interpretiert und diskutiert.

1.4 Aufbau

Das folgende Kapitel gibt einen Überblick über Grundlagen, die zur Nachvollziehbarkeit des aktuellen Forschungsstands und der Hypothesenbildung dienen. Im dritten Kapitel wird der derzeitige Forschungsstand zusammengefasst. In Kapitel vier erfolgt die detaillierte Dokumentation der Vorbereitung, Durchführung und Auswertung der empirischen Untersuchung. Abschließend folgen die Zusammenfassung und kritische Würdigung der Arbeit, und es wird ein Ausblick auf zukünftige Fortschungsaufgaben gegeben.

2 Grundlagen von Threat Intelligence Sharing Platforms

Threat Intelligence[6] ist evidenzbasiertes Wissen, einschließlich Kontext, Mechanismen, Indizien und umsetzbaren Ratschlägen, über eine bestehende oder aufkommende Bedrohung oder Gefahr für Vermögenswerte [Gart2013]. Threat Intelligence ermöglicht es, schnelle, fundierte und datengestützte Entscheidungen bezüglich der IT-Sicherheit zu treffen und beim Kampf gegen Bedrohungsakteure proaktiv, statt reaktiv vorzugehen. Der Threat-

[5] Das Umfragetool Qualtrics besitzt unter anderem eine Funktion für den SPSS-Export, allerdings lieferte diese keine zufriedenstellenden Ergebnisse. Für den CSV-Export aus Qualtrics waren nur wenige Anpassungen notwendig, die eine umfassende (Re-)Kodierung ersparten. Zudem bietet Excel freie Gestaltungsmöglichkeiten bei der Visualisierung und einen einfachen Export der Vektorgrafiken.

[6] Threat Intelligence (TI) wird auch als Cyber Threat Intelligence (CTI) bezeichnet. In dieser Arbeit wird das Wort „Bedrohungsinformationen“ als Synonym verwendet.

Intelligence-Lebenszyklus (vgl. Abb. 2-1) ist ein Prozess, um aus Rohdaten anwendbare Threat Intelligence für die Entscheidungsunterstützung zu erhalten [Bake2022].

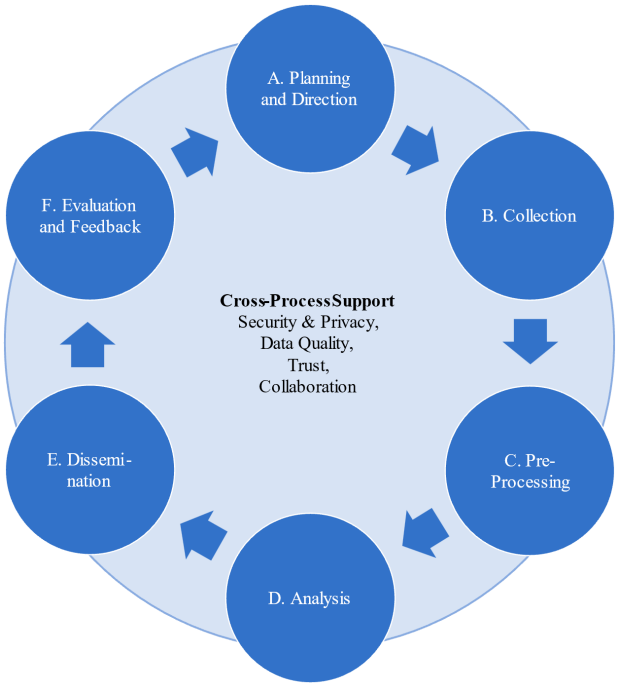

Abb. 2-1: Threat-Intelligence-Lebenszyklus [SFRR+2021, 4]

Im ersten Teilprozess beziehungsweise der Planungsphase werden Anforderungen für die Arbeit mit Bedrohungsinformationen abgestimmt, das heißt Ziele und die Methodik sind festzulegen, basierend auf den Bedürfnissen der Adressaten. Mögliche Fragen in dieser Phase sind: Wer sind die Angreifer und was sind ihre Motive? Welche Elemente in einer Organisation könnten angegriffen werden? Welche Maßnahmen sollten getroffen werden, um auf zukünftige Angriffe besser reagieren zu können? Sobald die Anforderungen festgelegt sind, folgt die zweite Phase. In dieser werden Informationen gesammelt, die dazu dienen, die im ersten Schritt festgelegten Ziele zu erreichen. Üblicherweise werden Logdaten und Informationen aus öffentlich zugänglichen Datenquellen gesammelt. Die dritte Phase umfasst die Vorverarbeitung der gesammelten Daten für die spätere Analyse. Zur Vorverarbeitung zählen unter anderem das Übertragen von Datenpunkten in Datenbanken, die Entschlüsselung von Dateien, die Übersetzung von fremdsprachigen Inhalten oder die Evaluation der Daten nach der Relevanz und Zuverlässigkeit. In der nächsten Phase werden die vorverarbeiteten Daten analysiert, um die Fragen aus der ersten Phase zu beantworten. Aus dem analysierten Datensatz werden in der fünften Phase verständliche Empfehlungen für die Adressaten abgeleitet. In der abschließenden Phase wird eine Rückmeldung auf die erteilten Empfehlungen eingeholt, um Anpassungen für zukünftige Threat-Intelligence-

Aufgaben zu tätigen. Möglicherweise gibt es eine Änderung der Prioritäten, oder die Adressaten wünschen sich eine andere Aufbereitung, Präsentation oder Häufigkeit, mit der Threat Intelligence verbreitet wird [Bake2022]. Zudem gibt es die prozessübergreifende Unterstützung, die alle Prozesse des Threat-Intelligence-Lebenszyklus unterstützt. Sie umfasst Funktionen zur Gewährleistung von Sicherheit und Privatsphäre, der Datenqualität, zum Aufbau von Vertrauen und zur Unterstützung der Zusammenarbeit [SFRR+2021, 5].

Threat Intelligence bzw. Bedrohungs- und Sicherheitsinformationen werden zwischen Organisationen auch unabhängig von Threat Intelligence Sharing Platforms ausgetauscht. Es gibt vier Arten von Threat Intelligence: strategische, operative, taktische und technische Threat Intelligence [ChRu2015; ToRa2018] (vgl. Tab. 2-1).

Strategische Threat Intelligence ist wenig technisch, wird von Entscheidungsträgern genutzt und häufig durch Berichte oder Gespräche übermittelt. Sie dient dazu, aktuelle Risiken zu verstehen und weitere Risiken zu erkennen, die bisher unbekannt sind. Die Informationen können finanzielle Auswirkungen von Cyberangriffen, historische Daten oder Angriffstrends umfassen. Infolgedessen können eine Risikobewertung durchgeführt und Ressourcen für die Abwehr eines möglichen Angriffs bereitgestellt werden [ToRa2018, 215].

	Strategisch	Operativ	Taktisch	Technisch
Technische Abstraktion	Hoch	Hoch	Niedrig	Niedrig
Zielgruppe	Vorstand	Verteidiger der IT-Infrastruktur	IT-Sicherheits-management, Architekten	SOC-Analysten, Incident Response Team
Inhalt	Informationen über sich verändernde Risiken	Details über spezifische, eingehende Angriffe	Taktiken, Techniken und Prozeduren der Angreifer	Indicators of Compromise
Aktualität	Langfristig	Kurzfristig	Langfristig	Unmittelbar

Tab. 2-1: Teilbereiche von Threat Intelligence [Toun2019, 12]

Operative Threat Intelligence sind Informationen über bevorstehende Angriffe auf die Organisation. Diese Informationen werden zum Beispiel von den Verteidigern der IT-Infrastruktur genutzt und helfen vorauszusehen, wann und wo Angriffe stattfinden werden.

Taktische Threat Intelligence enthält Informationen über die Methoden von Angreifern, wird unter anderem vom IT-Sicherheitsmanagement verwendet und umfasst Werkzeuge

bestimmter Bedrohungsgruppen sowie deren Taktiken, Techniken und Prozeduren (TTP). Taktische Threat Intelligence erhält man durch Fachzeitschriften, den Austausch mit anderen Organisationen oder den Kauf bei einem Anbieter.

Technische Threat Intelligence (TTI) sind Informationen, die in der Regel automatisiert verarbeitet werden, zum Beispiel Logdaten aus Firewalls oder E-Mail-Filtern [Toun2019, 11 f.]. Dazu zählen auch Indicators of Compromise (IoCs). Diese dienen als forensische Beweisstücke für ein mögliches Eindringen in ein Hostsystem oder Netzwerk, etwa unüblicher Netzwerkverkehr, unbekannte Dateien, Anwendungen und Prozesse des Systems oder verdächtige Aktivitäten privilegierter Benutzerkonten [Tren2020]. Indicators of Compromise sind eines der am einfachsten anwendbaren Threat-Intelligence-Attribute und stehen im Mittelpunkt der meisten Werkzeuge. Sie werden häufig in Anwendungen wie Intrusion Detection Systems (IDS) [WMPA2019, 7], in Analysewerkzeugen oder zur Visualisierung in Dashboards verwendet. Es gibt verschiedene Formate für den Austausch von IoCs, unter anderem Standard Threat Information Expression (STIX), Cyber Observable Expression (CybOX), Incident Object Description Exchange Format (IODEF) oder OpenIOC. STIX ist der meistgenutzte Standard, allerdings ist die Implementierung dieses Standards komplex [ToRa2018, 224].

Der manuelle Ansatz beim Teilen von Threat Intelligence, zum Beispiel durch E-Mails oder Gespräche, ist weitverbreitet, aber ineffektiv. Zum einen entstehen dadurch Verzögerungen beim Teilen sich schnell ändernder IT-Bedrohungen[7]. Zum anderen können menschliche Fehler bei der Verarbeitung entstehen oder zur unangemessener Filterung führen. Eine Lösung dafür ist, Teile des Prozesses zu automatisieren, beispielsweise mithilfe von Threat Intelligence Sharing Platforms [WMPA2019, 2 f.].

Dandurand und Serrano stellten 2013 das Konzept von Threat Intelligence Sharing Platforms vor und definierten wesentliche Anforderungen an die Plattformen [DaSe2013, 2]. Zum einen sollen diese den Austausch von Informationen erleichtern und die Automatisierung ermöglichen. Zum anderen sollen Threat Intelligence Sharing Platforms die Generierung, Verfeinerung und Verifizierung von Daten erleichtern. Heutige Threat Intelligence Sharing Platforms basieren im Wesentlichen auf diesen Anforderungen und diverse Anbieter bieten

[7] Zum Beispiel detektieren Antivirenprogramme IT-Bedrohungen häufig signaturbasiert, das heißt, auf Basis von in einer Datenbank gespeicherten Hash-Werten. Wird eine Datei mit einer verdächtigen Signatur gefunden, gibt es eine Warnung. Bereits durch die minimale Veränderung einer Datei wird deren Signatur geändert. Angreifer können Malware-Signaturen automatisiert und in kurzen zeitlichen Abständen verändern, sodass diese von signaturbasierten Antivirenprogrammen unentdeckt bleiben.

Plattformen mit erheblichen Funktionsunterschieden an [SSMB2017, 838]. Threat Intelligence Sharing Platforms unterstützen die Sammlung von Daten aus verschiedenen Quellen, deren Aggregation und kooperative Auswertung sowie den Export der Analysedaten in IT-Systeme von Organisationen. Die Plattformen ermöglichen eine effiziente Erkennung und Bekämpfung von Sicherheitsvorfällen und unterstützen verschiedene Teilprozesse des Threat-Intelligence-Lebenszyklus (vgl. Abb. 2-1).

3 Forschungsstand und verwandte Studien

In Deutschland werden Threat Intelligence Sharing Platforms wahrscheinlich auch in der öffentlichen Wahrnehmung eine größere Bedeutung. Bundesinnenministerin Faeser stellte im Juli 2022 die Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat vor. „Kernelemente sind eine neu organisierte Cybersicherheitsarchitektur mit einer führenden Rolle des Bundes, neue Befugnisse für die Sicherheitsbehörden, um Angriffe abwehren zu können, die entschiedene Bekämpfung von Cyberkriminalität sowie die Stärkung der Resilienz des Staates und kritischer Infrastrukturen.“ [Bund2022h] Im sechsten Abschnitt der Agenda wird der Schutz ziviler Infrastrukturen vor Cyberangriffen beschrieben. Das erste Ziel ist der Aufbau des BSI Information Sharing Portal (BISP) in der 20. Legislaturperiode. Dieses Portal soll vor allem kleine und mittlere Unternehmen (KMU) unterstützen. Derzeit findet bereits ein Informationsaustausch in der Allianz für Cyber-Sicherheit, mit mehr als 7.400 teilnehmenden Organisationen, statt [Bund2023].

Der Markt für Threat-Intelligence-Produkte wächst. Gartner prognostiziert, dass die Threat-Intelligence-Ausgaben der Organisationen jährlich um 15,8 Prozent steigen werden und bis 2025 ein Marktvolumen von 2,6 Milliarden Dollar erreicht wird. Es ist ein dynamischer Markt mit regelmäßig neuen Anbietern sowie vielen Akquisitionen. Gartner listet für den Zeitraum März bis November 2021 13 wesentliche Übernahmen auf [CCSL2021].

Im September 2022 stellte die Europäische Kommission den Entwurf für ein Gesetz zur Steigerung der Cybersicherheit (Cyber Resilience Act) vor. Der Gesetzesentwurf enthält zwei Hauptziele: Erstens sollen Voraussetzungen dafür geschaffen werden, dass Anbieter sicherstellen, dass Hard- und Softwareprodukte mit weniger Schwachstellen auf den Markt kommen und die Anbieter während des gesamten Lebenszyklus die Sicherheit eines Produktes überwachen und gegebenenfalls Aktualisierungen veröffentlichen. Zweitens sollen Bedingungen geschaffen werden, die es den Nutzern ermöglichen, bei der Auswahl

und Nutzung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen [Euro2022]. In dem Gesetzesentwurf werden Threat Intelligence Sharing Platforms nicht direkt erwähnt, aber die Umsetzung wird Auswirkungen auf die Anbieter der Plattformen haben.

Hemmnisse beziehungsweise Schwierigkeiten beim Teilen von Threat Intelligence und der Umgang damit, werden in zahlreichen Forschungsarbeiten beschrieben. Rajamäki behandelt Aspekte beim Teilen von Threat Intelligence, zum Beispiel, welche Information mit wem, warum und wie geteilt werden sollen und welche Architekturen, Methoden und Mechanismen beim Teilen verwendet werden [Raja2019, 20 ff.].

In einer Fallstudie zu Cyber-Defense-Übungen ermittelten Brilingatė et al. neun Faktoren, die den Austausch von Threat Intelligence hemmen. Beispielsweise werden die Bewertung und das Teilen von Bedrohungsinformationen vernachlässigt, wenn der Fokus auf technischen Aufgaben, wie der Verteidigung der IT-Systeme, liegt. Zudem hat die Größe der Arbeitsgruppe[8] einen entscheidenden Einfluss darauf, ob Threat Intelligence erfolgreich geteilt wird. In einer kleinen Arbeitsgruppe, mit sechs bis acht Personen, hat jede Person überschneidende Aufgaben, was die Arbeitsbelastung erhöht. Aufgaben, wie das Teilen von Bedrohungsinformationen, werden niedriger priorisiert und gegebenenfalls nicht durchgeführt. In großen Arbeitsgruppen, mit mehr als 15 Personen, sind die Verantwortlichkeiten besser verteilt, allerdings ist die Sammlung von Daten komplizierter, da mit vielen Personen kommuniziert werden muss [BBJK2022, 7].

Koepke definiert ebenfalls verschiedene Hemmnisse des Informationsaustauschs. Technologische Hemmnisse werden größer, wie beispielsweise die Komplexität der Informationen oder die Menge der Daten. Sie kommt zu dem Schluss, dass die Hemmnisse zum Informationsaustausch größer sind als die Anreize und dass mit steigender Unternehmensgröße mehr Bedrohungsinformationen ausgetauscht werden [Koep2017, 7]. Der Austausch von Bedrohungsinformationen ist nicht die einzige Schwierigkeit. Die größere Herausforderung ist, anwendbares Wissen aus den gesammelten Daten zu erlangen [WMPA2019, 2]. Brown et al. zeigen Herausforderungen für die Arbeit mit Bedrohungsdaten aus mehreren Quellen auf, etwa die Normalisierung und die Konsolidierung der gesammelten Daten [BGSe2015, 46]. Es existieren mehrere Standards

[8] Als Arbeitsgruppe ist hier der Personenkreis zu verstehen, der in der Organisation die Aufgabe hat, sich mit Threat Intelligence zu beschäftigten.

für den Austausch von Threat Intelligence [WMPA2019, 5]. Um einen effizienten Austausch von Bedrohungsinformationen zu erreichen, ist es wichtig, dass alle Werkzeuge denselben Standard nutzen [BBJK2022, 2].

Viele Organisationen haben juristische Vorbehalte[9] oder Vertrauensprobleme beim Informationsaustausch, sowohl mit organisationsinternen als auch mit organisationsexternen Stellen oder Partnern [MuLe2015, 27], obwohl bereits kryptografische Techniken für den Informationsaustausch erarbeitet wurden [vPEJ2016, 38] und der DSGVO-konforme Austausch mit vielen Threat Intelligence Sharing Platforms möglich ist [ABLe2019, 12].

Es existieren Unterschiede zwischen den Gesetzen verschiedener Länder bezüglich dessen, welche Informationen legal geteilt werden dürfen, und welche anonymisiert werden müssen. In der Europäischen Union ist die Gesetzeslage durch die Datenschutz-Grundverordnung (DSGVO) überwiegend einheitlich. In der Schweiz gibt es eigene Gesetze, wie das Schweizer Bundesgesetz über den Datenschutz (DSG). Eine Annäherung an die Datenschutz-Grundverordnung ist geplant, aber bisher existieren diverse Unterschiede [Søre2022].

Neben Herausforderungen beim Teilen von Bedrohungsinformationen wird häufig der Nutzen von Threat Intelligence hervorgehoben. Beispielsweise ermittelten Bouwman et al. in einer empirischen Untersuchung den Nutzen von Threat Intelligence für kommerzielle Anbieter. Sie fanden heraus, dass es nahezu keine Überlappung zwischen Threat Intelligence Feeds[10] gibt und diese zu teils hohen Preisen angeboten werden. Zudem kann es mehrere Wochen dauern, ehe Indicators of Compromise den Threat Intelligence Feeds hinzugefügt werden. Dies ist problematisch, da die Analysten die Bedrohungsinformationen zeitnah benötigen, um rechtzeitig darauf reagieren zu können [BGED+2020, 442 f.]. Zibak und Simpson listen eine Reihe von Vorteilen und Hemmnissen beim Austausch von Threat Intelligence auf, die in der Literatur erwähnt werden, um diese anschließend in einer empirischen Untersuchung zu prüfen. Die Befragung von 67 IT-Sicherheitsexperten aus Großbritannien ergab zum Teil Abweichungen zwischen den Ansichten der Experten und vorherigen Forschungsarbeiten. Beispielsweise war für die Befragten mangelnde

[9] Das heißt, Organisationen haben zum Beispiel Bedenken, gegen den Datenschutz oder das Kartellrecht zu verstoßen.

[10] Ein Threat Intelligence Feed ist ein kontinuierlicher Datenstrom, der sich auf potenzielle oder aktuelle Bedrohungen für die IT-Sicherheit eines Unternehmens bezieht und Informationen über Angriffe, Malware, Botnets etc. liefert [Wigm2021].

Standardisierung kein wesentliches Hemmnis beim Austausch von Threat Intelligence [ZiSi2019, 7].

Zudem haben Zibak et al. ein Erfolgsmodell für Informationssysteme auf den Austausch von Threat Intelligence übertragen und empirisch bewertet. Befragt wurden 152 britische IT-Sicherheitsexperten. Anschließend bestimmten die Autoren Faktoren, die für den Erfolg einer Threat Intelligence Sharing Platform entscheidend sind [ZSSi2021, 12].

In einer weiteren Untersuchung untersuchten Zibak et al. das gemeinsame Verständnis der erwarteten Qualität von Bedrohungsinformationen. An ihrer modifizierten Delphi-Studie nahmen 30 europäische Experten für Threat Intelligence teil [ZSSi2022, 4]. Die Autoren ermittelten eine Reihe von Qualitätsdimensionen für Bedrohungsinformationen wie zum Beispiel Aktualität, Vollständigkeit und Genauigkeit [ZSSi2022, 11].

Sauerwein et al. analysierten den Funktionsumfang von neun Threat Intelligence Sharing Platforms im Hinblick auf den Threat-Intelligence-Lebenszyklus (vgl. Abb. 2-1). In ihrer Studie listen sie auf, welche Funktionen implementiert werden sollten, damit die Plattformen den Intelligence-Zyklus unterstützen, um anwendbares Wissen zu generieren. Zudem wird aufgezeigt, dass zwischen den Threat Intelligence Sharing Platforms signifikante Funktionsunterschiede existieren [SFRR+2021, 7]. Wagner et al. beschreiben in ihrer Arbeit die Implementierung der Malware Information Sharing Platform (MISP) und die Funktionen der Plattform, unter anderem die Möglichkeit, nur die wichtigsten Informationen zu erfassen, die einfache Erweiterbarkeit oder die Festlegung von Zugangsstufen für den Informationsaustausch, um die Bedürfnisse verschiedener Akteure in der Organisation zu erfüllen [WDWI2016, 3 ff.]. Zudem untersuchten Wagner et al. in einer Studie 30 Anbieter von Threat Intelligence Sharing Platforms bezüglich des Vertrauens beim Teilen von Bedrohungsinformationen und entwickelten daraus eine Taxonomie. Der wichtigste Faktor für das Vertrauen ist, dass Organisationen in der gleichen Branche tätig sind [WPMA2018, 6].

Neben den erwähnten Forschungsarbeiten gibt es insbesondere privatwirtschaftlich finanzierte, internationale Untersuchungen zur Verbreitung und Nutzung von Threat-Intelligence-Werkzeugen. Die englischsprachigen Untersuchungen haben ihren Fokus auf Organisationen in den USA, Kanada sowie Großbritannien.

Gartner hat bereits mehrfach Marktanalysen zu Threat-Intelligence-Dienstleistungen und -Produkten durchgeführt [LBCo2019; LLCC+2020; CCSL2021]. In diesen werden

Marktentwicklungen analysiert, etwa Akquisitionen oder Prognosen des Marktvolumens. Weiterhin werden Anwendungsfälle für die Arbeit mit Threat Intelligence aufgezeigt. Zudem werden eine Reihe von Threat-Intelligence-Werkzeugen, unter anderem auch Threat Intelligence Sharing Platforms, überblicksartig dargestellt.

Das Ponemon-Institut[11] führt regelmäßig Studien zum Datenschutz und zur Informationssicherheit durch. In einer 2019 bereits zum dritten Mal durchgeführten Befragung wurde der Wert von Threat Intelligence in Organisationen untersucht [Pone2019]. Aus den Ergebnissen wurden Handlungsempfehlungen für die Arbeit mit Threat Intelligence abgeleitet. Über 1.000 Personen nahmen an der Befragung teil, etwa die Hälfte davon aus den USA und Kanada und etwa ein Drittel aus Europa, hauptsächlich aus Großbritannien. Der Einsatz von Threat Intelligence Sharing Platforms spielte in dieser Studie eine untergeordnete Rolle. Erfragt wurde, ob die Organisationen eine Plattform einsetzen, aber nicht welche oder wofür sie diese nutzen.

Weiterhin führen einige Anbieter von Threat Intelligence Sharing Platforms, zum Beispiel ThreatConnect[12], Anwenderbefragungen durch. Die 2019 durchgeführte Befragung zum Aufbau eines Threat-Intelligence-Arbeitsbereichs beantworteten 351 Entscheidungsträger der IT-Sicherheit aus den USA [Thre2019, 2]. In dem Bericht werden die Ergebnisse präsentiert und Handlungsempfehlungen gegeben. Dabei wird keine Threat Intelligence Sharing Platform namentlich genannt und es wird nur am Rande auf derartige Plattformen eingegangen.

Die umfangreichste und mit der vorliegenden Arbeit vergleichbare Untersuchung wird vom SANS-Institut durchgeführt. Seit 2015 findet jährlich [Shac2015; Shac2016; Shac2017; Shac2018; BrLe2019; Lee2020; BrLe2021; BrSt2022] eine weltweite Befragung über Threat Intelligence statt. Die Anzahl der teilnehmenden Organisationen variiert zwischen 200 bis über 400 Organisationen. Davon stammen die meisten Organisationen aus den USA. Der Fokus der Untersuchung liegt auf Threat Intelligence und nicht auf Threat Intelligence Sharing Platforms. Die Studie wird von verschiedenen Plattformanbietern finanziert, in der Vergangenheit zum Beispiel von AlienVault, Anomali, EclecticIQ, ThreatConnect oder ThreatQuotient. In den Studien wird explizit keine Threat Intelligence Sharing Plattform

[11] Das Ponemon-Institut ist ein privates Forschungszentrum, das 2002 in Traverse City, Michigan gegründet wurde und Untersuchungen in den Bereichen Datenschutz und Informationssicherheit durchführt [Pone2022].

[12] Das Unternehmen ThreatConnect wurde 2011 in Arlington County, Virginia gegründet und ist der Anbieter der gleichnamigen Threat Intelligence Sharing Platform [Thre2022].

erwähnt. Daher werden keine Angaben zu den Marktanteilen einzelner Plattformen gemacht, aber zum Teil zur Art der Nutzung der Plattformen.

Der Fokus der erwähnten Untersuchungen liegt auf englischsprachigen Ländern, hauptsächlich den USA, Kanada und Großbritannien. Threat Intelligence Sharing Platforms werden in den Anwenderbefragungen meist nicht namentlich erwähnt. Eine namentliche Nennung der Plattformen findet insbesondere in Forschungsarbeiten statt, die einen Vergleich der Plattformen durchführen. Bisher fehlen Erkenntnisse über die Verbreitung und die Art der Nutzung der Plattformen im deutschsprachigen Raum.

4 Empirische Untersuchung zur Nutzung der Plattformen

4.1 Ziel der Untersuchung und Formulierung von Hypothesen

Ziel der empirischen Untersuchung ist es, die zu Beginn gestellten Forschungsfragen[13] zur Verbreitung und Nutzung von Threat Intelligence Sharing Platforms in Organisationen im DACH-Raum zu beantworten. Zur Konkretisierung dieser Fragen wurden 13 Hypothesen[14] [KRSt2016, 47] formuliert, die mithilfe der empirischen Untersuchung bestätigt oder widerlegt werden sollen [KRSt2016, 346].

1. Einsatz von Threat Intelligence Sharing Platforms	
Hypothese 1	Der Einsatz von Threat Intelligence Sharing Platforms hat in den vergangenen vier Jahren zugenommen.
Hypothese 2	In Unternehmen ist im Vergleich zu Behörden und Universitäten der Einsatz von Threat Intelligence Sharing Plattforms verbreiteter.
Hypothese 3	Organisationen, für die der Stellenwert der IT-Sicherheit besonders hoch ist oder die ein CERT[15]/SOC[16]/CSIRT[17] betreiben, setzen Threat Intelligence Sharing Platforms häufiger ein als Organisationen, bei denen dies nicht gegeben ist.

[13] Vgl. Abschnitt 1.2 bzw. Anhang 1.
[14] Die Herleitung der Hypothesen erfolgt in den Abschnitten 4.3.3 und 4.3.4.
[15] Computer Emergency Response Team
[16] Security Operations Center
[17] Computer Security Incident Response Team

Hypothese 4	Die häufigsten Gründe, warum Threat Intelligence Sharing Platforms nicht eingesetzt werden, sind begrenzte Ressourcen sowie Datenschutz- und Compliance-Bedenken.
Hypothese 5	Trotz des zunehmenden Angebots an Threat Intelligence Sharing Platforms gibt es eine Konzentration auf einzelne, marktdominierende Plattformen.
Hypothese 6	Bei der Auswahl von Threat Intelligence Sharing Platforms sind den Organisationen vor allem ein hoher Funktionsumfang, niedrige Lizenzkosten und ein geringer Betriebsaufwand wichtig.
2. Art und Weise der Nutzung von Threat Intelligence Sharing Platforms	
Hypothese 7	Die gleichzeitige Nutzung mehrerer Threat Intelligence Sharing Platforms ist eher selten.
Hypothese 8	Organisationen nutzen eher organisationsexterne Threat Intelligence Sharing Platforms und betreiben keine eigenen (organisationsinternen) Plattformen.
Hypothese 9	Die Mehrheit der Organisationen nutzt die Funktionen ihrer Threat Intelligence Sharing Platforms regelmäßig und nicht nur anlassbezogen.
Hypothese 10	Über die Hälfte der Organisationen verbindet beziehungsweise integriert Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen (zum Beispiel Firewall, SIEM etc.).
Hypothese 11	Threat Intelligence Sharing Platforms werden bevorzugt zur Sammlung, Vorverarbeitung und Analyse und weniger zum Austausch und zur Bewertung von Threat Intelligence genutzt.
Hypothese 12	Organisationen teilen Threat Intelligence mithilfe von Threat Intelligence Sharing Platforms eher organisationsintern als -extern.
Hypothese 13	Am häufigsten nutzen Organisationen Threat Intelligence Sharing Platforms zur Unterstützung im Aufgabenbereich Incident Management.

Tab. 4-1: Hypothesen zur empirischen Untersuchung

4.2 Vorbereitung und Durchführung

Für die Durchführung empirischer Untersuchungen existieren verschiedene Erhebungsmethoden.[18] Die Befragung ist eine der am häufigsten genutzten Methoden [SHEl2018, 292 f.]. Diese kann zum Beispiel als mündliche Befragung, schriftliche Befragung, Telefoninterview oder als Online-Befragung durchgeführt werden. Für diese Untersuchung wurde die Online-Befragung gewählt. Im Vergleich zu anderen Befragungsformen können Daten von einer umfangreichen Teilnehmerzahl zeitnah und mit überschaubarem Aufwand aufgenommen werden. Zudem wird die Auswertung der Befragungsdaten beschleunigt und vereinfacht, da die erhobenen Daten direkt nach der Durchführung elektronisch zur Verfügung stehen.

Für die Befragung wurde ein Fragebogen[19] entwickelt [KRSt2016, 346]. Dieser umfasst 26 Fragen mit mehreren Verzweigungen und ist in drei Teile gegliedert. Im ersten Teil werden Informationen zu den teilnehmenden Organisationen, den IT-Sicherheitskenntnissen der antwortenden Personen sowie der Stellenwert der IT-Sicherheit in den Organisationen ermittelt. Der zweite Teil enthält Fragen zum Einsatz von Threat Intelligence Sharing Platforms, das heißt, ob diese in den Organisationen eingesetzt werden oder deren Einsatz geplant ist. Der letzte Teil enthält Fragen zur Art und Weise der Nutzung von Threat Intelligence Sharing Platforms.

Für die Umsetzung des Fragebogens und die Durchführung der Online-Befragung wurde das Internet-basierte Werkzeug „Qualtrics“ [Qual2022] verwendet. Die Befragung erfolgte in Kooperation mit der Technischen Universität Ilmenau, der Universität Innsbruck sowie dem Informationstechnikzentrum Bund (ITZBund), einem Dienstleister der deutschen Bundesverwaltung. Nach ausführlichen Pretests des Fragebogens fand die Untersuchung von Juli bis September 2022 statt. In den Pretests wurden unter anderem die Gestaltung des Fragebogens überprüft, die Verzweigungslogik in Qualtrics, die E-Mail-Einladungen oder die Darstellung des Fragebogens auf mobilen Endgeräten. Bei der Beantwortung des Fragebogens war jeweils eine Antwort verpflichtend, damit keine befragte Person versehentlich eine Frage übersieht. Es gab für die Befragten die Möglichkeit, mit „keine Angabe“ zu antworten.

[18] Für eine Übersicht empirischer Datenerhebungsmethoden vgl. beispielsweise [SHEl2018, 291; DöBo2016, 322 f.]
[19] Der vollständige Fragebogen ist in Anhang 6 abgebildet.

Befragt wurden Chief Executive Officer (CEOs), Chief Information Officer (CIOs), Chief Information Security Officer (CISOs) sowie Verantwortliche für Informationssicherheit in börsennotierten Unternehmen, Bundesbehörden und Universitäten in Deutschland, Österreich und der Schweiz. In Abb. 4-1 ist die Zusammensetzung der Stichprobe dargestellt.

Unternehmen	
Deutschland	89
Österreich	20
Schweiz	20
	129

Universitäten	
Deutschland	84
Österreich	22
Schweiz	14
	120

Behörden	
Deutschland	92
Österreich	15
Schweiz	24
	131

Gesamt	
Deutschland	265
Österreich	57
Schweiz	58
	380

Abb. 4-1: Zusammensetzung der Stichprobe

Zu den börsennotierten Unternehmen Deutschlands zählen die 40 Standardwerte des Deutschen Aktienindex (DAX) und 49 Nebenwerte des MDAX[20], zudem jeweils die 20 Standardwerte des Austrian Traded Index (ATX) sowie des Swiss Market Index (SMI). Insgesamt wurden 129 Unternehmen befragt. Zu den deutschen Universitäten in der Stichprobe gehören alle, die in der Hochschulrektorenkonferenz vertreten sind [Hoch2022]. Zum Zeitpunkt der Befragung waren dies 84 Universitäten. In Österreich wurde die Liste des Bundesministeriums für Bildung, Wissenschaft und Forschung (BMBWF) genutzt, die 22 Universitäten enthält [Bund2022f]. Die Universitäten der Schweiz listet das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) auf der Internetpräsenz aus [Staa2022]. Diesen hinzugefügt wurde die Eidgenössische Technische Hochschule Zürich, als größte Hochschule des Landes und eine der renommiertesten weltweit [Quac2022] sowie das Switch CERT[21]. Insgesamt wurden 120 Universitäten befragt.

[20] Mid-Cap-DAX, ohne Grand City Properties, da das Unternehmen in mehrheitlichem Besitz von Aroundtown (ebenfalls im MDAX enthalten) ist. Zudem haben beide Unternehmen denselben CISO. Der Stichtag zur Ermittlung der enthaltenen MDAX-Werte ist der 01.08.2022.

[21] Switch betreibt das Schweizer Forschungs- und Bildungsnetzwerk [SWIT2023].

Als Grundlage zur Ermittlung der deutschen Bundesbehörden diente eine Liste des Bundesverwaltungsamtes (BVA) [Bund2022e]. Diese enthält alle Behörden in Deutschland und wurde auf die Bundesministerien und Bundesoberbehörden gefiltert. Das Ergebnis dieser Liste wurde mit einem Python-Skript in eine CSV-Datei extrahiert. Im Anschluss erfolgten die Prüfung, Korrektur und Ergänzung der Datensätze.[22] Es wurden 92 Behörden beziehungsweise IT-Dienstleister von Behörden identifiziert.

In Österreich wurden alle Bundesministerien[23] befragt, die ihre eigene Informationstechnik betreiben[24] sowie die Bundesrechenzentrum GmbH als wichtiger IT-Dienstleister für die österreichische Bundesverwaltung, in Summe 15 Behörden. In der Schweiz wurden 24 Behörden befragt: die Generalsekretariate der Departemente [Bund2022d] sowie Bundesämter, das schweizerische Bundesarchiv (BAR), das nationale Zentrum für Cybersicherheit (NCSC), das Informatik Service Center (ISC-EJPD), als wichtiger Dienstleister und GovCERT.ch, das CERT der schweizerischen Regierung. Die Nachrichtendienste der jeweiligen Länder sind nicht Teil der Stichprobe. Insgesamt wurden 380 Organisationen befragt. Anhang 5 enthält die vollständige Liste der befragten Organisationen.

Nach der Festlegung der Stichprobe fand die Identifikation der Kontaktpersonen in den Organisationen statt. Während etwa zwei Prozent der Stichprobe persönliche Kontakte der Autoren dieses Beitrags waren, stammten die restlichen Kontakte und E-Mail-Adressen aus öffentlich zugänglichen Informationen. Zuerst erfolgte die Ermittlung der Namen und Rollen der Kontaktpersonen, danach deren E-Mail-Adressen. Sofern die börsennotierten Unternehmen CIOs oder CISOs beschäftigen, ließen sich die Namen über eine Google-Suche oder die Suche in dem sozialen Netzwerk LinkedIn [Link2022] identifizieren. Die meisten Universitäten und Behörden stellten Organigramme auf den Internetpräsenzen zur Verfügung oder listeten Verantwortliche für die Informationstechnik oder die IT-Sicherheit

[22] Es wurden alle dem Zoll unterstellten Behörden (regionale Zollfahndungsämter, Bildungs- und Wissenschaftszentrum der Bundesfinanzverwaltung, Zentrales Finanzwesen des Bundes) und der Bundeswehr unterstellte Organisationen (Bundessprachenamt, Panzerdivisionen) entfernt. Die Bundesmonopolverwaltung für Branntwein wurde entfernt, da diese Behörde nicht mehr existiert. Drei Bundesbehörden aus der Stichprobe wurden nach der Bundestagswahl 2021 umbenannt. In die Stichprobe wurden zudem folgende Behörden aufgenommen: Bundesamt für Auswärtige Angelegenheiten, Bundesinstitut für Risikobewertung, Bundesanstalt für Landwirtschaft und Ernährung, Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Bundesagentur für Arbeit, Deutsche Rentenversicherung, die IT-Dienstleister des Bundes sowie die größten drei IT-Dienstleister der Bundesländer.

[23] [Bund2022a] – als Behördentyp „Bundesministerium“ auswählen und auf „Abfragen“ klicken

[24] Alle Ministerien verwalten eigene Informationstechnik, außer das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS), dessen IT durch das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) verwaltet wird [Bund2022c, 25 f.].

auf. Für deutsche Behörden konnten zusätzlich E-Mail-Adressen der Kontaktpersonen über den Verzeichnisdienst der Bundesverwaltung [Bund2022b][25] ermittelt werden. Für die österreichischen Behörden gab es ebenfalls eine Personensuche [Bund2022g][26], die bei der Ermittlung von E-Mail-Adressen nützlich war. Die Internetpräsenzen der schweizerischen Behörden verwendeten häufig Kontaktformulare und es wurden nicht immer Organigramme zur Verfügung gestellt oder in vielen Fällen waren diese ohne Namen. Auch hier konnten die fehlenden Verantwortlichen über LinkedIn identifiziert werden. In weiteren Fällen konnten die E-Mail-Adressen über eine Google-Suche nach den verwendeten E-Mail-Domains und den Namensschemata[27] der Organisationen gefunden werden.

Sofern die Organisationen über CERTs[28] verfügen, wurden diese kontaktiert. In den meisten Fällen wurden möglichst zielgenau Einzelpersonen, vorzugsweise CISOs, adressiert. In Ausnahmefällen konnten keine passenden Kontaktpersonen ermittelt werden, hier wurden Funktionspostfächer verwendet. In wenigen Fällen waren die geeigneten Kontaktpersonen nicht deutschsprachig. Dies kam gehäuft in der Schweiz vor. Für diese Personen wurde der Fragebogen übersetzt und in englischer Sprache zur Verfügung gestellt. Nach der Ermittlung der E-Mail-Adressen erfolgte deren Prüfung[29].

Die Kontakt-E-Mails wurden als Blindkopie an die Adressaten über den E-Mail-Server der Technischen Universität Ilmenau versendet. Auf Textformatierungen wurde überwiegend verzichtet sowie auf Tracking-Pixel, Bilder oder Anhänge, um nach Möglichkeit nicht als Spam markiert zu werden. Die E-Mails enthielten einen anonymen Link zur Umfrage und die Konfiguration der Umfragesoftware erfolgte möglichst datensparsam. Etwa zwei Prozent der E-Mails wurden von den empfangenden Mailservern zurückgewiesen. In diesen Fällen wurden die E-Mail-Namensschemata der Organisationen geprüft und gegebenenfalls neue Kontaktpersonen ermittelt.

In Ausnahmefällen gaben automatische Antworten zu erkennen, dass Personen nicht mehr für die Organisationen tätig oder länger abwesend waren, als der Umfragezeitraum andauerte. In diesen Fällen erfolgte die Ermittlung anderer Kontaktpersonen. Nach der

[25] Die Personensuche ist nur im Intranet der Bundesverwaltung verfügbar.

[26] Für folgende Behörden ist die Personensuche nicht verfügbar: Bundesministerium für Inneres (BMI), Bundesministerium für Landesverteidigung (BMLV) sowie für die Nachrichtendienste.

[27] Am häufigsten wurde das Muster vorname.nachname@organisation.tld verwendet.

[28] Informationen über die CERTs stammen aus folgenden Mitgliederlisten: [Foru2022; DFN-2022a; DFN-2022b]

[29] Die Gültigkeit wurde mittels des folgenden Werkzeuges überprüft: [Byte2022]. Etwa drei Prozent der E-Mail-Adressen waren fehlerhaft und wurden korrigiert.

Hälfte der Befragungsdauer wurde eine Erinnerung an die Zielgruppe versendet, mit Ausnahme von sechs Personen, die darum gebeten haben, den Kontakt zu unterbinden.

4.3 Beschreibung und Auswertung der Ergebnisse

4.3.1 Rücklaufquote

Von den aus 380 Organisationen angefragte Teilnehmer haben sich 69 an der Befragung beteiligt. Dies entspricht einer Rücklaufquote von 18,2 Prozent. 63 Personen beantworteten den Fragebogen vollständig und sechs zu mindestens 75 Prozent. Im Median dauerte die vollständige Beantwortung des Fragebogens vier Minuten und 47 Sekunden. Abb. 4-2 zeigt die Rücklaufquoten für die einzelnen Organisationsformen und die Länder, in denen die Organisationen ihren Hauptsitz haben.

B = Anzahl Befragte | R = Anzahl Rückläufer | % = Rücklaufquote

Unternehmen	B	R	%
Deutschland	89	15	16,9
Österreich	20	3	15,0
Schweiz	20	1	5,0
	129	**19**	**14,7**

Universitäten	B	R	%
Deutschland	84	15	17,9
Österreich	22	4	18,2
Schweiz	14	2	14,3
	120	**21**	**17,5**

Behörden	B	R	%
Deutschland	92	24	26,1
Österreich	15	1	6,7
Schweiz	24	4	16,7
	131	**29**	**22,1**

Gesamt	B	R	%
Deutschland	265	54	20,4
Österreich	57	8	14,0
Schweiz	58	7	12,1
	380	**69**	**18,2**

Abb. 4-2: Rücklaufquoten nach Organisationsform und Herkunftsland

Die Rücklaufquote war für deutsche Organisationen mit 20,4 Prozent höher als in Österreich (14,0 Prozent) und der Schweiz (12,1 Prozent). Behörden antworteten mit 22,1 Prozent Rücklaufquote häufiger als Universitäten mit 17,5 Prozent und Unternehmen mit 14,7 Prozent. Am höchsten war die Rücklaufquote in deutschen Behörden mit 26,1 Prozent. Dies ist wahrscheinlich auf mehrere Gründe zurückzuführen. Zum einen gab es mehr persönliche Kontakte in der deutschen Bundesverwaltung als in den anderen Organisationsformen und Ländern. Des Weiteren ist das Informationstechnikzentrum Bund ein IT-Dienstleister der Bundesverwaltung und als Kooperationspartner dieser Umfrage vielen IT-Verantwortlichen

in den deutschen Behörden bekannt. Weiterhin sind die Bundesbehörden in Deutschland weniger zentral organisiert als in Österreich oder der Schweiz. Die meisten deutschen Bundesbehörden verwalten ihre eigene IT-Infrastruktur, obwohl es eine Reihe von Dienstleistern gibt, wie zum Beispiel das ITZBund für die zivile Bundesverwaltung, die BWI GmbH für die „weiße IT“[30] der Bundeswehr, das IT-Systemhaus für die Bundesagentur für Arbeit oder die IT-Dienstleister der Bundesländer, wie zum Beispiel IT.NRW[31]. Das ITZBund übernimmt unter anderem das Hosting von Webseiten oder IT-Fachverfahren, aber es verbleibt IT-Infrastruktur, die von den Kundenbehörden selbst betrieben wird und für die es Verantwortliche gibt, die kontaktiert werden können. In Österreich und der Schweiz existieren weniger Behörden und die Behörden haben im Durchschnitt weniger Beschäftigte. Zudem sind die Behörden zentraler organisiert, das heißt, nicht alle betreiben eigene Informationstechnik und haben demzufolge nicht immer feste Kontaktpersonen. Ob die Behörden eine eigene IT-Infrastruktur betreiben, konnte nicht immer zweifelsfrei festgestellt werden. Ein Indiz dafür waren umfangreiche IT-Abteilungen in den Organigrammen.

Die Rücklaufquoten an deutschen Universitäten (17,9 Prozent) und österreichischen Universitäten (18,2 Prozent) waren höher als an schweizerischen Universitäten (14,3 Prozent) und jeweils höher als in den Unternehmen.

4.3.2 Angaben zu den befragten Organisationen

Abb. 4-3 zeigt die Zusammensetzung der Stichprobe. Unter den antwortenden Organisationen befinden sich 29 Behörden (42 Prozent), 21 Universitäten (30 Prozent) und 19 Unternehmen (28 Prozent). Die häufigsten Branchen der Unternehmen sind Technologie (32 Prozent), Finanzen (21 Prozent) und Maschinenbau, Verkehr, Logistik (21 Prozent). 78 Prozent der Organisationen stammen aus Deutschland, zwölf Prozent aus Österreich und zehn Prozent aus der Schweiz. Die Organisationen weisen ein weites Spektrum an Beschäftigten auf. Die größte Gruppe bilden mit 29 Prozent Organisationen, die 1.001 bis 5.000 Beschäftigte haben. Weitere Angaben zur Anzahl der Beschäftigten der teilnehmenden Organisationen sind in Abb. 4-4 dargestellt.

[30] *Weiß* steht in diesem Fall für die nichtmilitärische Infrastruktur, zum Beispiel die Logistik. Ein Beispiel für *grüne* IT dagegen ist Informationstechnik, die in Waffensysteme eingebettet ist [Klee2015].
[31] Landesbetrieb Information und Technik Nordrhein-Westfalen

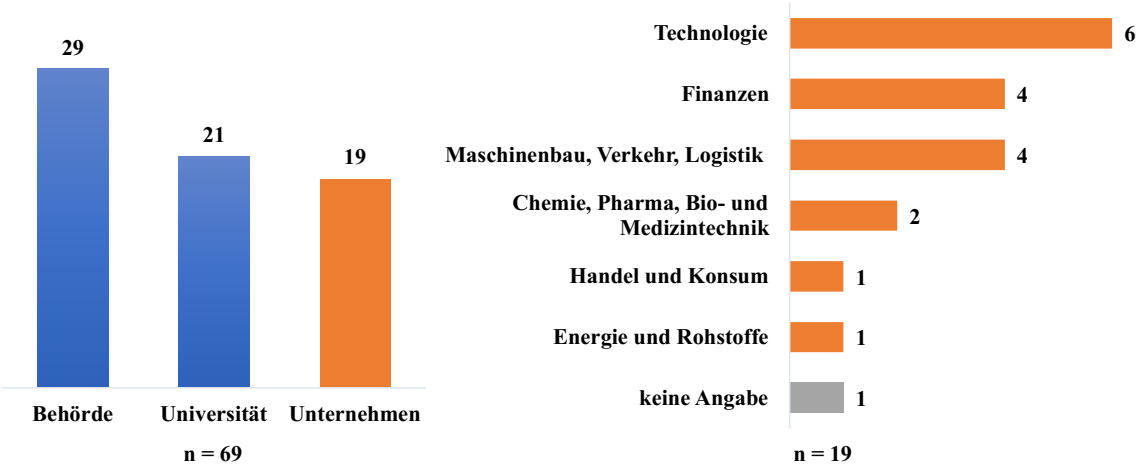

Abb. 4-3: Organisationsart und Branche der Unternehmen

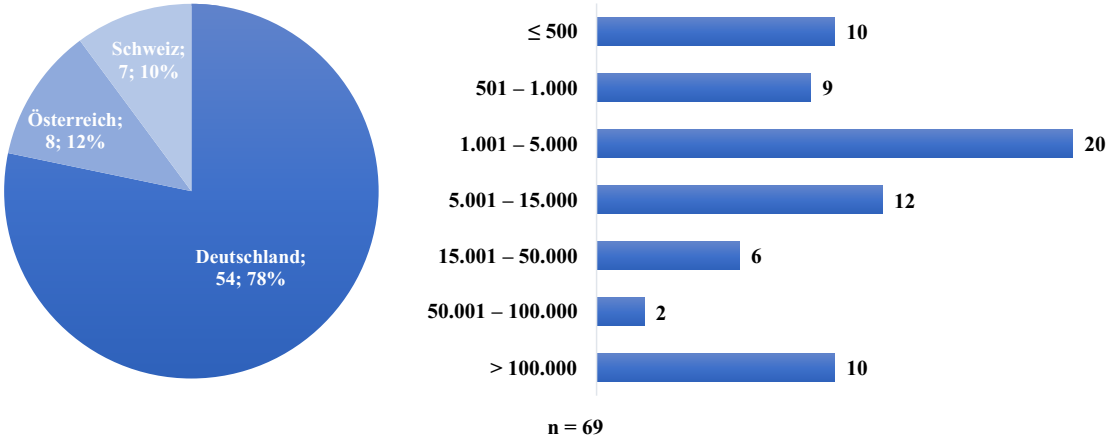

Abb. 4-4: Hauptsitz und Anzahl der Beschäftigten der Organisationen

Fasst man die Angaben zur Anzahl der Beschäftigten zusammen, haben 19 Organisationen (27,5 Prozent) weniger als 1.000 Beschäftigte, 32 Organisationen (46,4 Prozent) haben zwischen 1.001 und 15.000 Beschäftigte und 18 Organisationen (26,1 Prozent) haben über 15.001 Beschäftigte.

Am häufigsten wurden die Fragebögen durch Chief Information Security Officer ausgefüllt (29 Prozent), gefolgt von Analysten, die im Security Operations Center (SOC), Computer Emergency Response Team (CERT) oder Computer Security Incident Response Team (CSIRT) tätig waren (26,1 Prozent). IT-Fachleute bilden den überwiegenden Teil der antwortenden Personen. In Abb. 4-5 ist die Verteilung der Rollen innerhalb der Organisationen dargestellt. Die Rollen der Kategorie „Sonstige“ sind: Informationssicherheits-

risikomanager, stellvertretende Leitung für operative Cybersicherheit und Threat-Intelligence-Analyst.

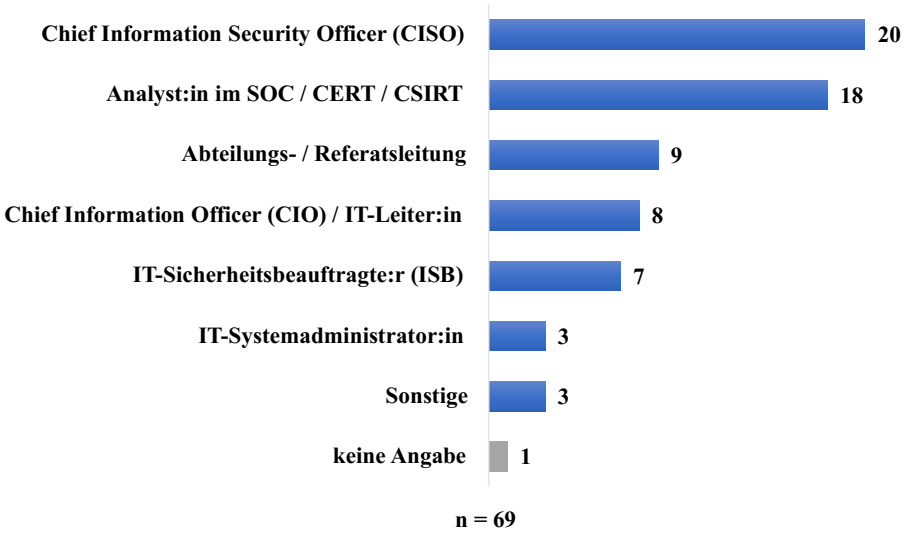

Abb. 4-5: Rolle der Befragten

Viele der Befragten sind sehr erfahren im Bereich der IT-Sicherheit (vgl. Abb. 4-6). 42 Prozent der Umfrageteilnehmer haben über zehn Jahre Berufserfahrung in diesem Bereich. Im Kommentarfeld meldete ein Teilnehmer 30 Jahre Praxiserfahrung. Die häufigsten Qualifikationen beziehungsweise Zertifizierungen der Teilnehmer waren Certified Information Security Manager (CISM), die von zehn Personen erworben wurde sowie Certified Information Systems Security Professional (CISSP), die acht Teilnehmer erwarben. Fünf Personen erwarben die Zertifizierung Certified Information Systems Auditor (CISA). Abgesehen davon spielten Zertifikate eine untergeordnete Rolle für die Stichprobe, die Mehrheit der Befragten überzeugte durch Praxiserfahrung. Alle weiteren genannten Zertifizierungen waren in den meisten Fällen Einzelnennungen, deckten aber ein breites Spektrum der IT-Sicherheit ab.

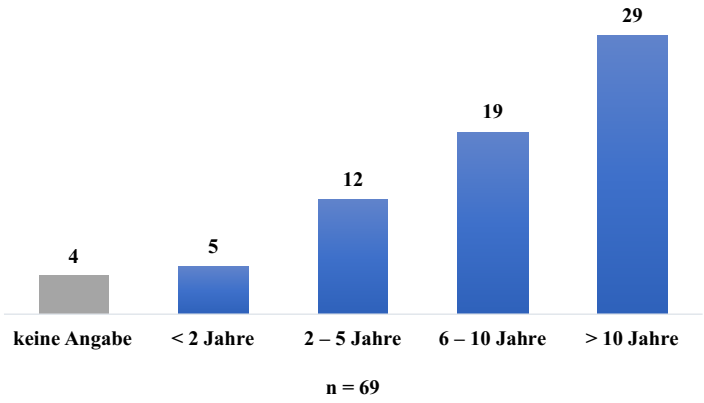

Abb. 4-6: Berufserfahrung der Befragten

Über die Hälfte (58 Prozent) der Organisationen hat eine Abteilung für IT-Sicherheit, abgesehen von einem SOC, CERT oder CSIRT. 44,9 Prozent der Organisationen haben ein SOC, 40,6 Prozent ein CSIRT und 34,8 Prozent ein CERT (vgl. Abb. 4-7). Etwa ein Viertel der Organisationen haben entweder keine IT-Sicherheitsabteilungen oder wollten dazu keine Angabe machen. Da diese Unterscheidung für die Prüfung der Hypothesen unerheblich ist, wurde auf eine detaillierte Erhebung im Fragebogen verzichtet.

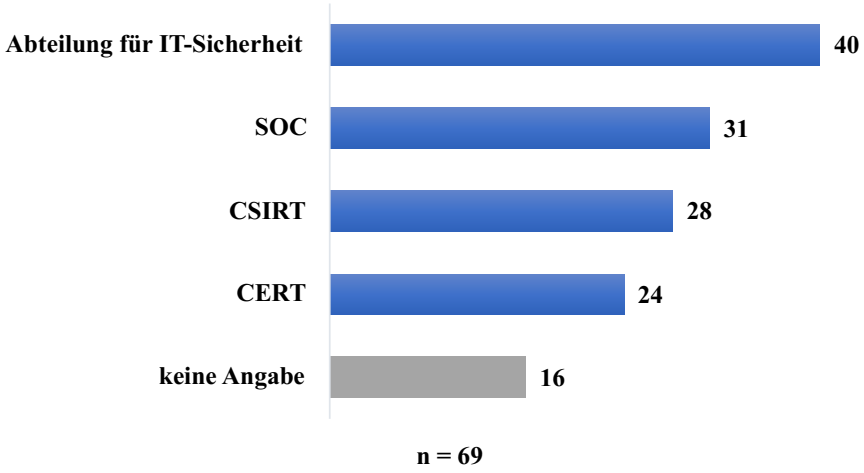

Abb. 4-7: Organisationseinheiten im Bereich der IT-Sicherheit

In mehr als der Hälfte (55,1 Prozent) der befragten Organisationen gibt es weniger als zehn Beschäftigte im Bereich der IT-Sicherheit. 21,7 Prozent der Organisationen beschäftigen 10 bis 50 Personen in diesem Bereich, 10,1 Prozent beschäftigen 51 bis 100 Personen und 11,6 Prozent der Organisationen beschäftigen über 100 Personen in diesem Bereich (vgl. Abb. 4-8).

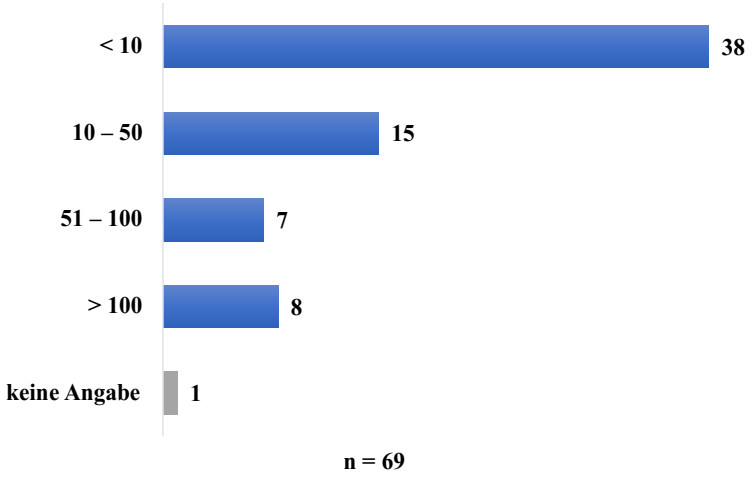

Abb. 4-8: Anzahl der Beschäftigten im Bereich der IT-Sicherheit

Die IT-Sicherheit hat einen besonderen Stellenwert für die meisten Organisationen (vgl. Abb. 4-9). 40,6 Prozent schätzten den Stellenwert der IT-Sicherheit in der Organisation als „sehr wichtig“ ein und 21,7 Prozent als „äußerst wichtig“. Keine Organisation schätzte den Stellenwert der IT-Sicherheit als „unwichtig“ ein. Für jede zehnte Organisation war IT-Sicherheit „nicht sehr wichtig“ und für jede vierte Organisation war IT-Sicherheit „wichtig“.

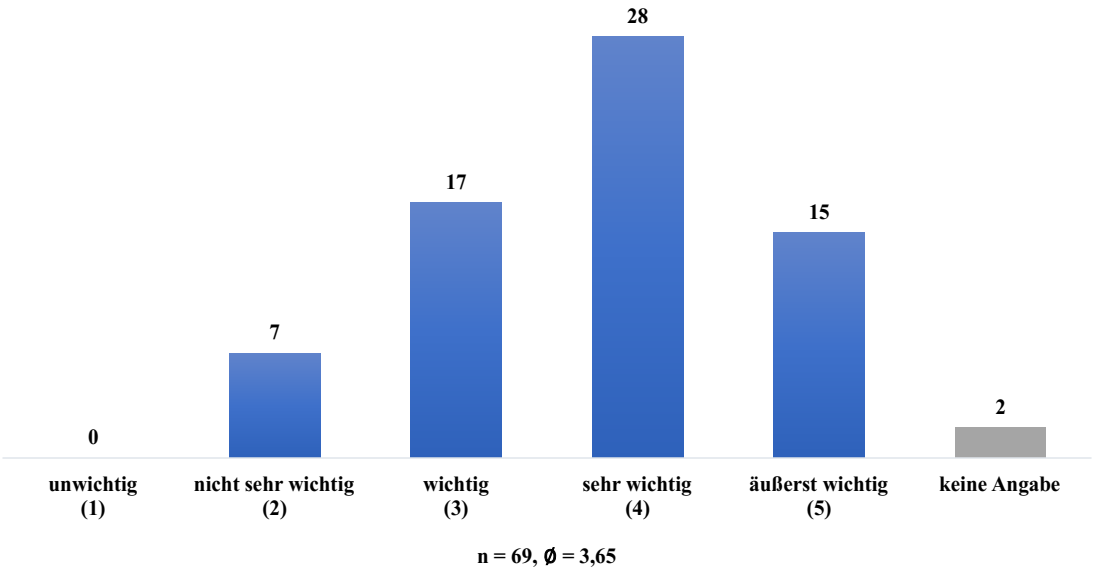

Abb. 4-9: Stellenwert der IT-Sicherheit in den Organisationen

4.3.3 Einsatz von Threat Intelligence Sharing Platforms

Hypothese 1: Der Einsatz von Threat Intelligence Sharing Platforms hat in den vergangenen vier Jahren zugenommen.

Aufgrund der Ergebnisse der aktuellen Cyber-Threat-Intelligence-Studie des SANS-Institutes wurde diese Hypothese aufgestellt. Festgestellt wurde in der Studie unter anderem, dass viele Organisationen erst beginnen, ihre Threat-Intelligence-Fähigkeiten aufzubauen und dafür Prozesse entwickeln [ZSSi2021, 7; BrSt2022, 2]. Weiterhin zeigt die Studie, dass Threat Intelligence Sharing Platforms bisher nicht zu den am meisten eingesetzten Werkzeugen[32] im Bereich Threat Intelligence gehören [BrSt2022, 11], das heißt, es existieren viele potenzielle Kunden für diese Plattformen.

Die zugehörige Frage, um diese Hypothese zu bestätigen oder zu widerlegen, lautet: „Seit wann nutzt Ihre Organisation Threat Intelligence Platforms?“. Um eine Aussage über die zukünftige Entwicklung treffen zu können, wurde zudem folgende Frage gestellt: „Planen Sie in den nächsten fünf Jahren den Einsatz einer Threat Intelligence Sharing Plattform?“

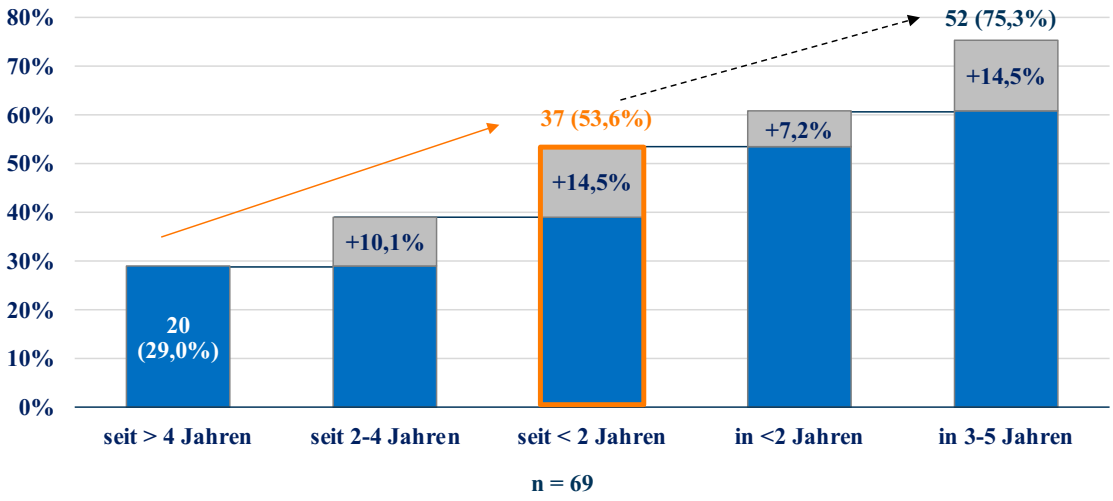

Abb. 4-10: Zunahme des Einsatzes von Threat Intelligence Sharing Platforms

37 der 69 Organisationen (53,6 Prozent) gaben an, Threat Intelligence Sharing Platforms einzusetzen (vgl. Abb. 4-10). 20 Organisationen (29,0 Prozent) setzen diese Plattformen bereits seit über vier Jahren ein, weitere sieben Organisationen (10,1 Prozent) seit zwei bis vier Jahren und weitere zehn Organisationen (14,5 Prozent) seit weniger als zwei Jahren.

[32] In der Studie werden Bedrohungsinformationen im Wesentlichen über E-Mail, als Office-Dokument oder über Gespräche verteilt.

Fünf Organisationen (7,2 Prozent) planen den Einsatz einer Plattform innerhalb der nächsten zwei Jahre und weitere zehn Organisationen (14,5 Prozent) planen den Einsatz innerhalb der nächsten drei bis fünf Jahre.

Die Ergebnisse der Befragung bestätigen die erste Hypothese und stimmen mit der SANS-Studie überein. Threat Intelligence Sharing Platforms sind in der Praxis angekommen und es ist zu erwarten, dass die Verbreitung der Plattformen zunehmen wird.

Hypothese 2: In Unternehmen ist im Vergleich zu Behörden und Universitäten der Einsatz von Threat Intelligence Sharing Plattforms verbreiteter.

Mehrere Studien [BGED+2020, 439; Pone2019, 21; BrSu2010, 4; ZSSi2022, 7; ZSSi2021, 7; BrSt2022, 3; BrLe2021, 4; Shac2018, 5] deuten auf eine stärkere Verbreitung von Threat-Intelligence-Werkzeugen in Unternehmen im Vergleich zu Behörden hin.

Um die Hypothese zu prüfen, wurden drei Fragen gestellt. Zum einen wurde gefragt: „In welcher Art von Organisation sind Sie tätig?“ und „Setzt Ihre Organisation für den Austausch von Informationen über IT-Bedrohungen ein oder mehrere Threat Intelligence Sharing Platforms ein?“. Zum anderen wurden Unternehmen nach der Branche gefragt.

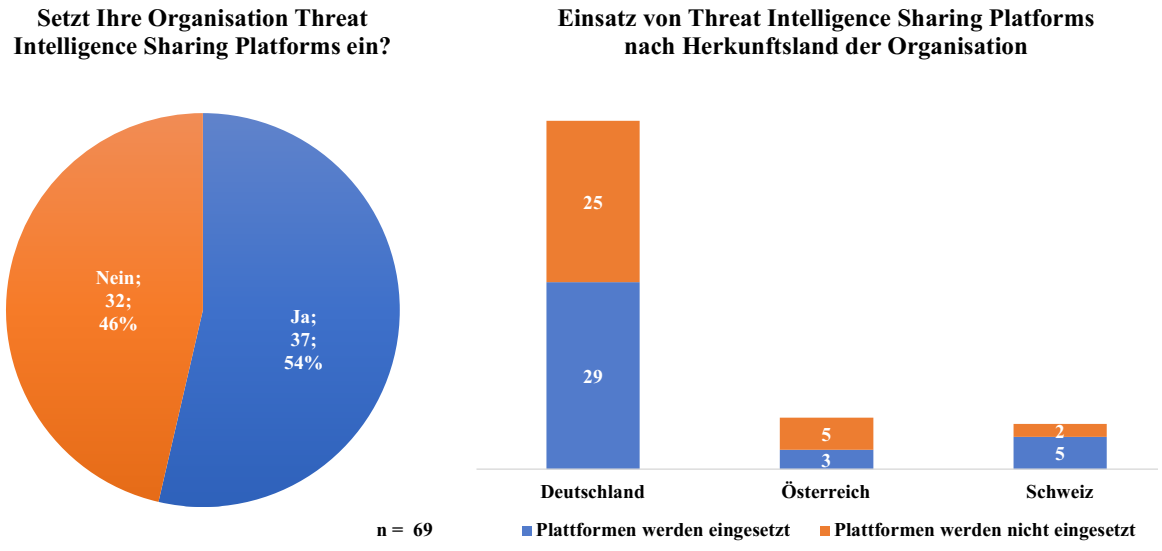

Abb. 4-11: Einsatz von Threat Intelligence Sharing Platforms

Von den 69 Teilnehmern gaben 37 Teilnehmer (54 Prozent) an, dass ihre Organisation Threat Intelligence Sharing Platforms nutzen und 32 Teilnehmer (46 Prozent), dass ihre Organisation diese Plattformen nicht nutzen (vgl. Abb. 4-11). 37,5 Prozent der österreichischen Organisationen, 53,7 Prozent der deutschen Organisationen und 71,4 Prozent

der schweizerischen Organisationen verwenden Threat Intelligence Sharing Platforms. Dabei stammt der Großteil der Antworten (78,3 Prozent) von deutschen Organisationen.

Bei der Befragung antworteten 29 Behörden, 21 Universitäten und 19 Unternehmen. 33,3 Prozent der Universitäten und 48,3 Prozent der Behörden setzen Threat Intelligence Sharing Platforms ein (vgl. Abb. 4-12). Unternehmen verwenden mit 84,2 Prozent deutlich häufiger Threat Intelligence Sharing Platforms als die anderen Organisationen. Dies bestätigt die oben genannten Hypothese. Behörden und Universitäten planen aber, in den nächsten Jahren aufzuholen.

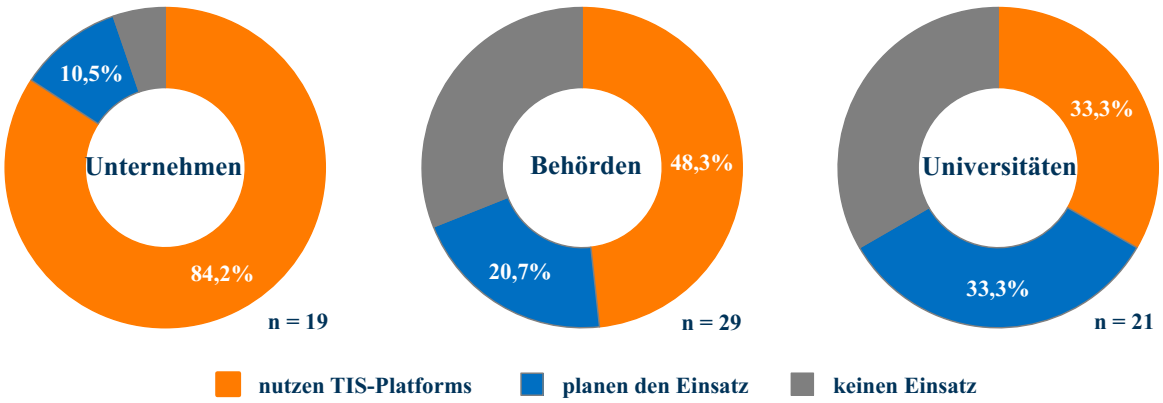

Abb. 4-12: Anteil der Organisationen, die TIS-Platforms einsetzen bzw. deren Einsatz planen

Aufgrund weniger Rückläufer aus den Unternehmen und der hohen Verbreitung von Threat Intelligence Sharing Platforms innerhalb der Unternehmen, ist nur eine bedingte Aussage zur Verbreitung der Plattformen in den einzelnen Branchen möglich. In mehreren Branchen geben 100 Prozent der Teilnehmer an, Threat Intelligence Sharing Platforms zu nutzen (vgl. Tab. 4-2). Unternehmen der Branchen Maschinenbau, Verkehr, Logistik und Technologie nutzen in dieser Studie Threat Intelligence Sharing Platforms häufiger als Unternehmen der Finanzbranche[33].

[33] Wenn man Branchen betrachtet, die mindestens so viele Rückläufer erzielten wie die Finanzbranche.

Branche	Anzahl der Unternehmen	Unternehmen, die TIS-Platforms einsetzen	Anteil (%)
Finanzen	4	3	75
Maschinenbau, Verkehr, Logistik	4	4	100
Technologie	6	5	83,3
Chemie, Pharma, Bio- und Medizintechnik	2	2	100
Handel und Konsum	1	1	100
Energie und Rohstoffe	1	1	100
keine Angabe	1	0	0
	19	**16**	**84,2**

Tab. 4-2: Einsatz von Threat Intelligence Sharing Platforms in Unternehmen

Hypothese 3: Organisationen, für die der Stellenwert der IT-Sicherheit besonders hoch ist oder die ein CERT/SOC/CSIRT betreiben, setzen Threat Intelligence Sharing Platforms häufiger ein als Organisationen, bei denen dies nicht gegeben ist.

Der erste Teil der Hypothese basiert auf der Annahme, dass Organisationen, für die IT-Sicherheit eine größere Rolle spielt, eher in IT-Sicherheit investieren und Softwareunterstützung in diesem Bereich einsetzen. Wie zu Beginn dieser Arbeit erwähnt, könnte zudem die Größe der Arbeitsgruppe einen Einfluss auf das Teilen von Threat Intelligence haben, da in größeren Gruppen jede Person abgegrenzte Aufgaben beziehungsweise Verantwortlichkeiten hat [BBJK2022, 7]. Größere Organisationen betreiben eher dedizierte Abteilungen für IT-Sicherheit, wie ein CERT, SOC oder CSIRT, da ihnen mehr Personal zur Verfügung steht als kleineren Organisationen.

Folgende Fragen dienen zum Bestätigen oder Widerlegen der Hypothese: „Verfügt Ihre Organisation über eine oder mehrere der folgenden Organisationseinheiten [aus dem Bereich der IT-Sicherheit]?“, „Wie viele Personen sind in Ihrer Organisation insgesamt im Bereich IT-Sicherheit (CERT, CSIRT, etc.) beschäftigt?“, „Welchen Stellenwert hat IT-Sicherheit in Ihrer Organisation?“ und „Setzt Ihre Organisation für den Austausch von Informationen über IT-Bedrohungen ein oder mehrere Threat Intelligence Sharing Platforms ein?“.

Mit der Zunahme des Stellenwertes der IT-Sicherheit steigt der Anteil an Organisationen, die Threat Intelligence Sharing Platforms einsetzen. 53,6 Prozent der Organisationen, für die IT-Sicherheit „sehr wichtig“ ist und 86,7 Prozent der Organisationen, für die IT-Sicherheit „äußerst wichtig“ ist, setzen Threat Intelligence Sharing Platforms ein (vgl. Tab. 4-3).

Der erste Teil der dritten Hypothese ist damit bestätigt, je wichtiger die IT-Sicherheit für die Organisationen ist, desto häufiger setzen diese Threat Intelligence Sharing Platforms ein.

Stellenwert der IT-Sicherheit	Anzahl der Organisationen	Organisationen, die TIS-Platforms einsetzen	Anteil (%)
unwichtig	0	0	0
nicht sehr wichtig	7	2	28,6
wichtig	17	6	35,3
sehr wichtig	28	15	53,6
äußerst wichtig	15	13	86,7
keine Angabe	1	1	100
	69	**37**	**53,6**

Tab. 4-3: Stellenwert der IT-Sicherheit und Einsatz von TIS-Platforms

Die Wörter Computer Emergency Response Team und Computer Security Incident Response Team werden häufig als Synonyme verwendet, sind aber technisch unterschiedlich [Moyl2021]. Während das primäre Ziel eines Computer Emergency Response Teams ist, IT-Sicherheitsinformationen zu sammeln und zu verteilen, liegt der Fokus eines Computer Security Incident Response Teams bei der Reaktion auf IT-Sicherheitsvorfälle. Ein Security Operations Center hat hingegen die Hauptaufgabe, die IT-Infrastruktur der Organisation zu überwachen und zu verteidigen [Matt2022]. Zwischen den Verantwortungsbereichen von CERT, SOC und CSIRT bestehen oft Überlappungen (vgl. Abb. 4-13). Des Weitren ist es möglich, dass CERT, SOC und CSIRT in den Organisationen unterschiedliche Funktionen beziehungsweise Aufgaben haben.

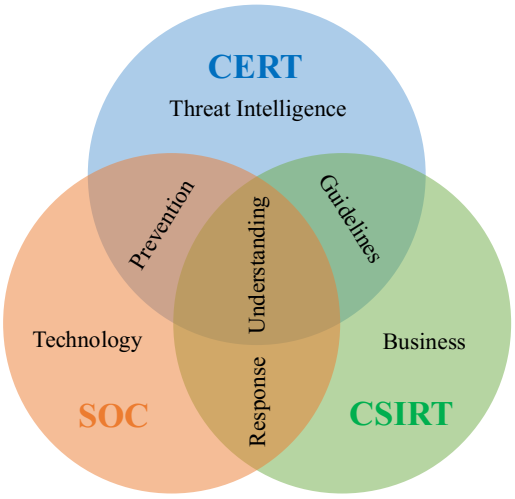

Abb. 4-13: Mengendiagramm CERT, SOC und CSIRT [Matt2022]

Vier von fünf Organisationen, die ein CERT, SOC oder CSIRT haben, setzen Threat Intelligence Sharing Platforms ein. Bei Organisationen, die eine Abteilung für IT-Sicherheit (abseits von CERT, SOC oder CSIRT) haben, ist der Anteil mit 67,5 Prozent geringer. Nur jede vierte Organisation, die bei der Frage nach den eingesetzten Organisationseinheiten im Bereich der IT-Sicherheit „keine Angabe“ gemacht haben, setzen Threat Intelligence Sharing Platforms ein (vgl. Tab. 4-4). Es wurde nicht explizit danach gefragt, ob keine Organisationseinheit für IT-Sicherheit in den Organisationen existiert. Allerdings ist davon auszugehen, dass die meisten Rückläufer mit „keiner Angabe“ keine dedizierte Organisationseinheit für IT-Sicherheit haben. Die Annahme basiert auf den Antworten auf die darauffolgende Frage. Bei 14 Teilnehmern folgte auf „keine Angabe“ bei der Organisationseinheit die Angabe „unter 10 Beschäftigte“ im Bereich der IT-Sicherheit. Dabei wäre es möglich, dass gar keine Mitarbeiter in diesem Bereich arbeiten beziehungsweise der Bereich nicht existiert. Bei einer weiteren Person folgte auf „keine Angabe“ zu den Organisationseinheiten ebenfalls „keine Angabe“ auf die Frage nach der Anzahl der Beschäftigten im Bereich der IT-Sicherheit. Auch hier wäre es möglich, dass keine Abteilung für IT-Sicherheit existiert. Nur eine Person antwortete nach „keine Angabe“ auf die Frage nach den Organisationseinheiten mit „51 bis 100 Beschäftigte“ im Bereich der IT-Sicherheit. Bei der Frage nach den eingesetzten Organisationseinheiten der IT-Sicherheit war eine Mehrfachauswahl möglich.

Organisationseinheit	Anzahl der Organisationen	Organisationen, die TIS-Platforms einsetzen	Anteil (%)
Abteilung für IT-Sicherheit	40	27	67,5
SOC	31	25	80,6
CSIRT	28	23	82,1
CERT	24	19	79,2
keine Angabe	16	4	25,0

Tab. 4-4: Organisationseinheiten der IT-Sicherheit und Einsatz von TIS-Platforms

Organisationen, die ein CERT, SOC oder CSIRT betreiben, setzen eher Threat Intelligence Sharing Platforms ein als Organisationen, die dies nicht tun. Der zweite Teil der oben genannten Hypothese ist damit ebenfalls bestätigt.

Die Anzahl der Beschäftigten im Bereich der IT-Sicherheit ist ebenfalls eng mit der Frage verbunden, ob Threat Intelligence Sharing Platforms eingesetzt werden (vgl. Tab. 4-5). Während Organisationen mit weniger als zehn Beschäftigten im Bereich der IT-Sicherheit

zu 28,9 Prozent eine Threat Intelligence Platform einsetzen, steigt der Anteil auf 73,3 Prozent bei Organisationen mit 10 bis 50 Beschäftigten und auf 85,7 Prozent bei Organisationen mit 51 bis 100 Beschäftigten im IT-Sicherheitsbereich. Alle Organisationen, die über 100 Beschäftigte in diesem Bereich haben, setzen Threat Intelligence Sharing Platforms ein.

Beschäftigte IT-Sicherheit	Anzahl der Organisationen	Organisationen, die TIS-Platforms einsetzen	Anteil (%)
< 10	38	11	28,9
10 – 50	15	11	73,3
51 – 100	7	6	85,7
> 100	7	7	100
keine Angabe	1	1	100
	69	**37**	**53,6**

Tab. 4-5: Beschäftigte im Bereich IT-Sicherheit und Einsatz von TIS-Platforms

Mit steigender Organisationsgröße nimmt der Einsatz von Threat Intelligence Sharing Platforms ebenfalls zu (vgl. Tab. 4-6). Dies bestätigt das Ergebnis einer anderen Studie, nach der größere Organisationen eher Threat Intelligence teilen als kleinere Organisationen [Koep2017, 8].

Anzahl der Beschäftigten	Anzahl der Organisationen	Organisationen, die TIS-Platforms einsetzen	Anteil (%)
≤ 1.000	19	6	31,6
1.001 – 15.000	32	15	46,9
> 15.001	18	16	88,9
	69	**37**	**53,6**

Tab. 4-6: Anzahl der Beschäftigten und Einsatz von TIS-Platforms

Hypothese 4: Die häufigsten Gründe, warum Threat Intelligence Sharing Platforms nicht eingesetzt werden, sind begrenzte Ressourcen sowie Datenschutz- und Compliance-Bedenken.

Mehrere Studien führen den Mangel an Personal und fehlende Finanzierung als wesentliche Schwierigkeiten für die Arbeit mit Threat Intelligence an [Pone2019, 24; Thre2019, 9;

ZSSi2022, 1; BrLe2021, 17; Lee2020, 15; Shac2018, 11; Koep2017, 10; Shac2016, 20; Shac2015, 17].

In internationalen Publikationen wird zudem die Einhaltung des Datenschutzes als Herausforderung angesehen [ZiSi2019, 8; Toun2019, 19]. Für den DACH-Raum wird vermutet, dass dieses Kriterium eine wichtigere Rolle spielt als im internationalen Vergleich, aufgrund hoher Datenschutzstandards und Strafen bei Verstößen.[34] Viele Organisationen haben juristische Vorbehalte oder Vertrauensprobleme beim Informationsaustausch [MuLe2015, 27], obwohl bereits verschiedene Zugriffsstufen für den organisationsübergreifenden Austausch zum Beispiel in MISP implementiert sind [MISP2022]. Zudem ist, wie bereits erwähnt, der DSGVO-konforme Austausch von Bedrohungsinformationen mit vielen Plattformen möglich.

Um die Hypothese zu bestätigen oder zu widerlegen, wurde gefragt: „Was sind Gründe dafür, dass auf den Einsatz einer Threat Intelligence Sharing Plattform verzichtet wird?“.

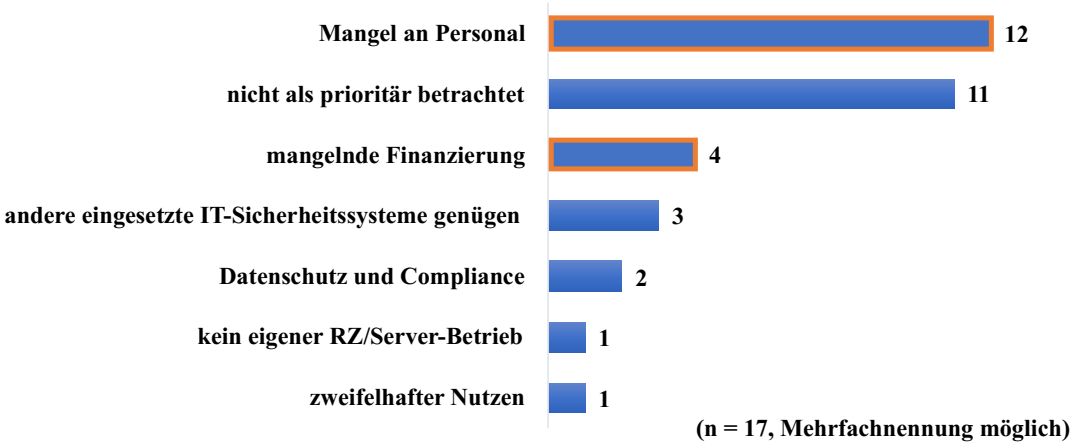

Abb. 4-14: Was sind Gründe dafür, dass auf den Einsatz einer TIS-Platforms verzichtet wird?

Die häufigsten Gründe, warum Organisationen auf den Einsatz von Threat Intelligence Sharing Platforms verzichten, sind Personalmangel (für 70,6 Prozent der Organisationen) und dass sie ihre Prioritäten bei anderen Technologien sehen (für 64,7 Prozent der Organisationen). Mangelnde Finanzierung (23,5 Prozent) folgt mit Abstand an dritter Stelle (vgl. Abb. 4-14). Begrenzte Ressourcen, insbesondere an Personal und finanziellen Mitteln,

[34] Eine Übersicht der bisherigen Bußgelder: [Comp2022]. Je nach Organisationsgröße können die Bußgelder dreistellige Millionenbeträge überschreiten. Bisher wurde keine Strafe im Zusammenhang mit der Nutzung von Threat Intelligence Sharing Platforms verhängt (Stand: Dezember 2023).

sind demnach tatsächlich wesentliche Gründe für den Nichteinsatz der Plattformen, was für den ersten Teil der oben genannten Hypothese spricht.

Bedenken im Hinblick auf Datenschutz und Compliance spielen jedoch eine untergeordnete Rolle. Nur zwei Befragte (11,8 Prozent) wählten diesen Grund für den Nichteinsatz einer Threat Intelligence Sharing Platform. Damit ist der zweite Teil der Hypothese nicht bestätigt. Zu beachten ist, dass die antwortenden Personen überwiegend einen fachlichen Hintergrund haben (vgl. Abb. 4-5) und die getätigten Angaben von der Sicht des Managements abweichen könnten. Interoperabilitätsprobleme war eine weitere, vorgegebene Antwortmöglichkeit, die aber niemand als Grund angegeben hat, Threat Intelligence Sharing Platforms nicht einzusetzen.

Hypothese 5: Trotz des zunehmenden Angebots an Threat Intelligence Sharing Platforms gibt es eine Konzentration auf einzelne, marktdominierende Plattformen.

Über die Marktanteile einzelner Threat Intelligence Platforms existieren bisher wenige Erkenntnisse [Shac2016, 13]. Ein möglicher Grund könnten Geheimhaltungsvereinbarungen einiger Plattformanbieter sein. Für die entgeltfreien Plattformen sind gegebenenfalls Nutzerzahlen ermittelbar. Open Threat Exchange (OTX) des Anbieters AlienVault beziehungsweise AT&T Cybersecurity hat weltweit über 200.000 registrierte Personen [Alie2023] und 7.000 registrierte Organisationen [BFSL+2020, 1953]. Malware Information Sharing Platform (MISP) nutzen über 800 Organisationen weltweit [BFSL+2020, 1952].

Eine Studie identifizierte im Jahr 2017 eine Vielzahl an Threat Intelligence Sharing Platforms [SSMB2017, 838]. Es ist zu erwarten, dass es Marktführer unter diesen Plattformen gibt. Neben diesen Threat Intelligence Sharing Platforms existieren weitere, von den Anwender-Organisationen selbst entwickelte Plattformen.

Zur Bestätigung oder Widerlegung der oben genannten Hypothese wurden Organisationen, die bereits Threat Intelligence Sharing Platforms einsetzen, gefragt: „Welche Threat Intelligence Sharing Platform(s) setzt Ihre Organisation ein?“. Organisationen, die planen Threat Intelligence Sharing Platforms einzusetzen, wurden gefragt, welche Plattformen sie einzusetzen planen.

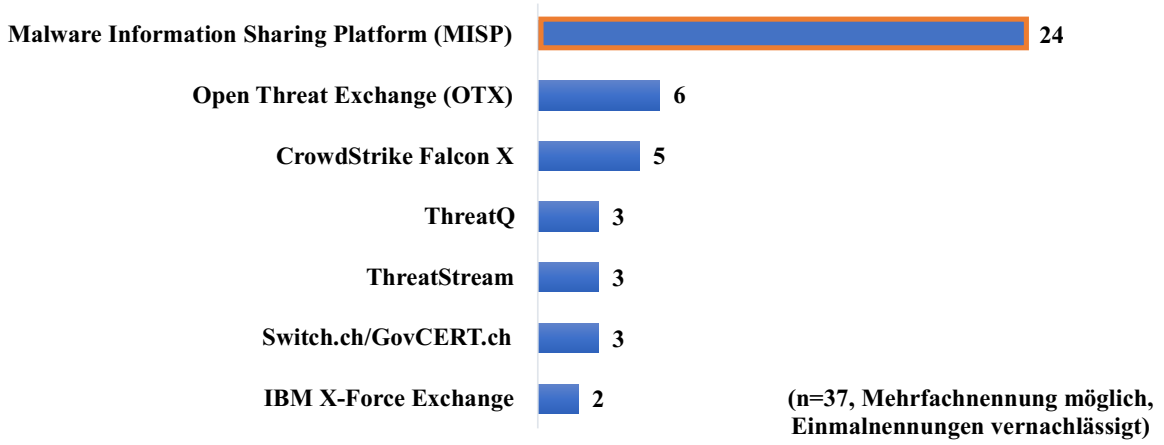

Abb. 4-15: Welche TIS-Platform(s) setzen Organisationen ein?

Über die Hälfte der Organisationen (64,9 Prozent), die Threat Intelligence Sharing Platforms einsetzen, verwenden MISP (vgl. Abb. 4-15). Diese quelloffene Plattform ist unter den Studienteilnehmern mit Abstand am weitesten verbreitet, gefolgt von der entgeltfreien Plattform Open Threat Exchange (16,2 Prozent). Die hohe Verbreitung beider Plattformen ist möglicherweise auf die entfallenden Lizenzkosten zurückzuführen, die ein wesentliches Kriterium für die Auswahl einer Threat Intelligence Sharing Platform sind.[35] Die Marktführerschaft von MISP unter den Teilnehmern dieser Studie könnte darauf zurückzuführen sein, dass Open Threat Exchange in der Cloud des Anbieters gehostet wird oder die Organisationen gegebenenfalls eine quelloffene Threat Intelligence Sharing Platform bevorzugen. Da die hohe Verbreitung einer Plattform, zum Beispiel unter Partnern, im Rückblick das wichtigste Auswahlkriterium ist[36], wird MISP vermutlich mittelfristig im DACH-Raum die am weitesten verbreitete Plattform bleiben. Die am weitesten verbreitete entgeltpflichtige Plattform ist CrowdStrike Falcon X (13,5 Prozent) an dritter Stelle.

Organisationen, die derzeit keine Threat Intelligence Sharing Platform einsetzen, aber planen eine einzusetzen, haben in den meisten Fällen (66,7 Prozent) keine (Vor-)Auswahl getroffen. Jede vierte Organisation gab an, den Einsatz von MISP zu planen. Eine Organisation plant entweder den Einsatz von IBM X-Force Exchange und Open Threat Exchange oder hat die Vorauswahl auf diese Plattformen eingeschränkt (vgl. Abb. 4-16).

[35] Vgl. Ergebnisse von Hypothese 6.
[36] Vgl. Ergebnisse von Hypothese 6.

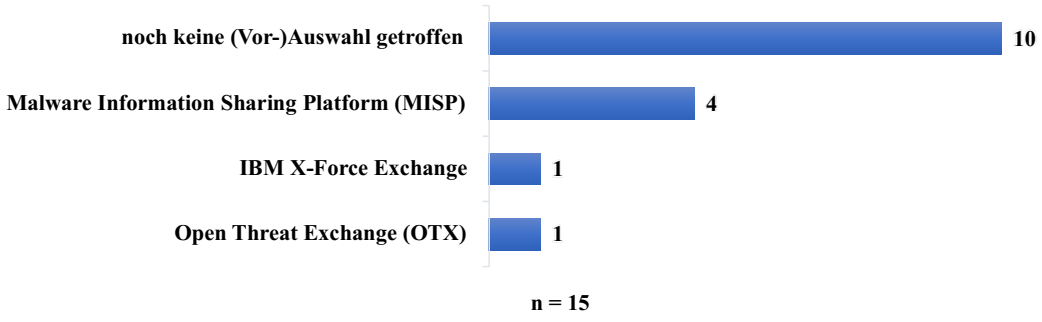

Abb. 4-16: Welche TIS-Platforms planen die Organisationen einzusetzen?

Hypothese 5 ist damit bestätigt, trotz des zunehmenden Angebots an Threat Intelligence Sharing Platforms gibt es eine Konzentration auf einzelne, marktdominierende Plattformen. Der Marktführer in dieser Studie ist mit Abstand die Malware Information Sharing Platform.

Hypothese 6: Bei der Auswahl von Threat Intelligence Sharing Platforms sind den Organisationen vor allem ein hoher Funktionsumfang, niedrige Lizenzkosten und ein geringer Betriebsaufwand wichtig.

Es gibt erhebliche Funktionsunterschiede zwischen den Threat Intelligence Sharing Platforms [SFRR+2021, 7]. Um einen möglichst großen Nutzen aus der Verwendung der Plattformen zu ziehen, definieren Organisationen im Voraus Anforderungen. Eine Threat Intelligence Sharing Platform mit größerem Funktionsumfang kann die Anforderungen meist besser erfüllen. Deshalb ist davon auszugehen, dass für die Organisationen der Funktionsumfang der Plattform einen großen Stellenwert besitzt. Die Lizenzkosten sind ebenfalls von besonderer Bedeutung, da es entgeltfreie Plattformen gibt, die in Konkurrenz zu den entgeltpflichtigen Plattformen stehen. Der Preis für die Nutzung entgeltpflichtiger Threat Intelligence Sharing Platforms kann pro Jahr mehrere zehntausend bis mehrere hunderttausend Euro betragen[37]. Aufgrund der begrenzten Ressourcen, besonders des Personals[38], ist zudem ein geringer Betriebsaufwand für den Betrieb der Threat Intelligence Sharing Platforms erstrebenswert.

Um die Hypothese zu bestätigen oder zu widerlegen, wurde folgende Frage an Organisationen gestellt, die bereits Threat Intelligence Sharing Platforms einsetzen: „Welche der folgenden Kriterien waren für die Auswahl einer Threat Intelligence Sharing

[37] Die Preise für die Nutzung der Plattformen sind in der Regel nicht öffentlich. Ein Anhaltspunkt sind bei Amazon Web Services (AWS) veröffentlichte Preise. Für 3.500 Beschäftigte beträgt die Jahresgebühr der Anomali Plattform $520.000 und für ThreatStream Enterprise $150.000. Zusätzlich können weitere Gebühren und Steuern anfallen [AWS2023].

[38] Vgl. Hypothese 4

Platform wichtig?“. Für Organisationen, die planen eine solche Plattform einzusetzen, wurde die Frage leicht variiert: „Welche der folgenden Kriterien sind für die Auswahl einer geplanten Threat Intelligence Sharing Platform wichtig?“

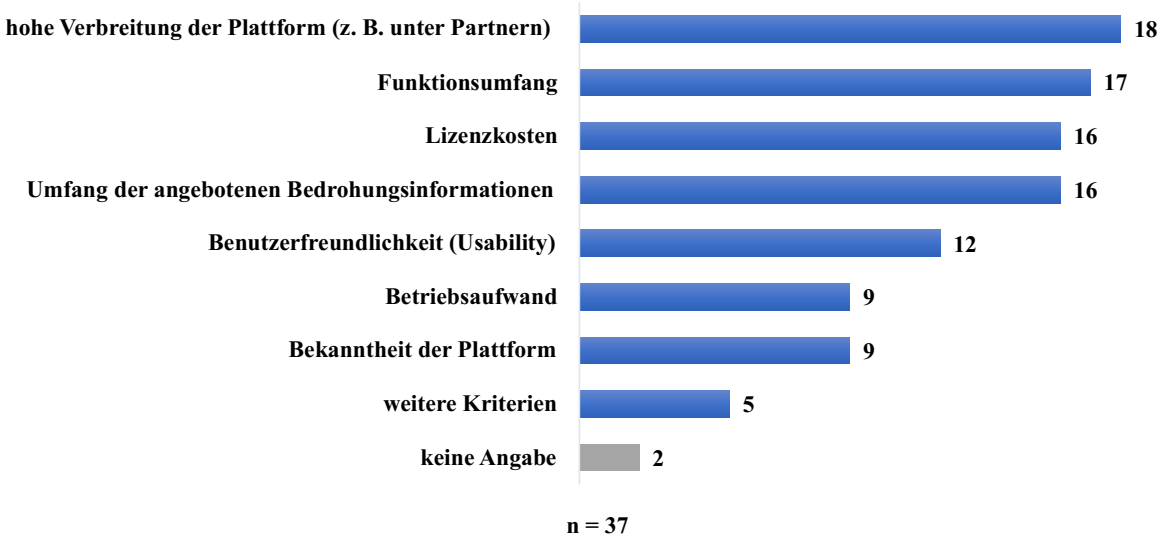

Abb. 4-17: Welche Kriterien waren für die Auswahl einer TIS-Platform wichtig?

Wie bei Hypothese 4 hängen die getätigten Angaben von der Position beziehungsweise der Perspektive der antwortenden Person ab. Das wichtigste Kriterium für die Auswahl einer Threat Intelligence Sharing Platform war für 48,6 Prozent der Befragten die hohe Verbreitung der Plattform (zum Beispiel unter Partnern), gefolgt von dem Funktionsumfang (45,9 Prozent), den Lizenzkosten (43,2 Prozent) sowie dem Umfang der angebotenen Bedrohungsinformationen (43,2 Prozent). Weniger wichtig war der Betriebsaufwand für die Nutzung und den Betrieb der Plattform für 24,3 Prozent der Befragten (vgl. Abb. 4-17). Es gab weitere Kriterien, die für die Befragten für die Auswahl einer Threat Intelligence Platform relevant waren: unkomplizierter Zugang, Austausch innerhalb des CERT-Verbundes, Zuverlässigkeit, Flexibilität, das heißt, Vermeidung von Lock-in-Effekten sowie Qualität der Bedrohungsinformationen.

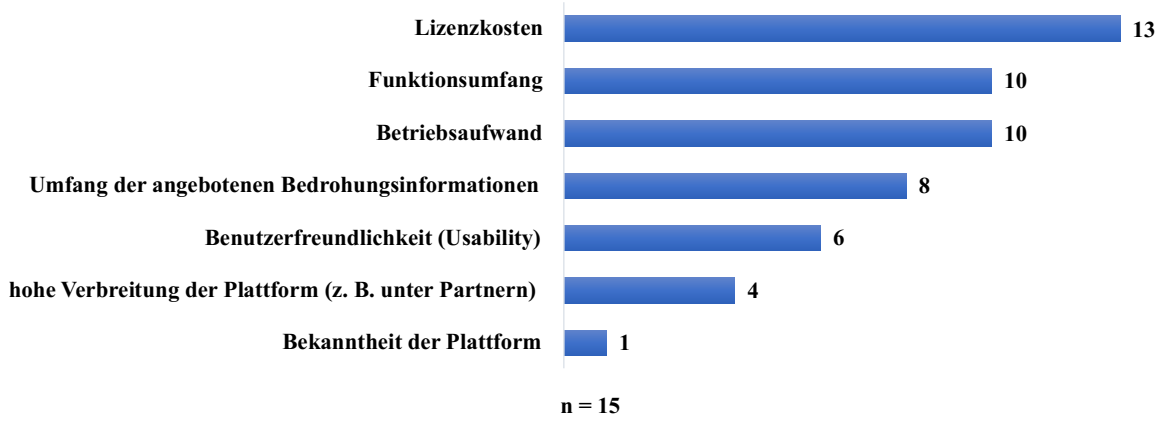

Abb. 4-18: Welche Kriterien sind für die Auswahl der geplanten TIS-Platform wichtig?

Für die Organisationen, die den Einsatz eine Plattform planen, wird die oben genannte Hypothese bestätigt. Lizenzkosten sind vor dem Einsatz von Threat Intelligence Sharing Platforms für 86,7 Prozent der Befragten das wichtigste Auswahlkriterium, gefolgt von dem Funktionsumfang und dem Betriebsaufwand der Plattformen, die für jeweils zwei Drittel der Befragten von Bedeutung sind (vgl. Abb. 4-18).

Der Betriebsaufwand ist für die Organisationen, die bereits Threat Intelligence Sharing Platforms einsetzen, deutlich weniger wichtig als für Organisationen, die planen, diese Plattformen einzusetzen. Umgekehrt ist die hohe Verbreitung der Plattformen für erstgenannte Organisationen wichtiger als für die Organisationen, die planen, eine Threat Intelligence Sharing Platform einzusetzen. Damit ist Hypothese 6 überwiegend bestätigt.

4.3.4 Art und Weise der Nutzung von Threat Intelligence Sharing Platforms

Hypothese 7: Die gleichzeitige Nutzung mehrerer Threat Intelligence Sharing Platforms ist eher selten.

Wie bereits erwähnt, zeigen bisherige Studien, dass viele Organisationen erst beginnen, ihre Threat-Intelligence-Fähigkeiten aufzubauen [ZSSi2021, 7; BrSt2022, 2] und dass Threat Intelligence Sharing Platforms dabei nicht zu den am meisten genutzten Hilfsmitteln gehören [BrSt2022, 11]. Das spricht eher dafür, dass eine Nutzung mehrerer solcher Plattformen in der Praxis nicht stark verbreitet ist. Allerdings belegen andere Untersuchungen, dass es große funktionale und inhaltliche Unterschiede zwischen den Threat Intelligence Sharing Platforms gibt [SFRR+2021; SSMB2017]. Durch die gleichzeitige Nutzung mehrerer Plattformen wäre es Organisationen möglich, Defizite einzelner Plattformen zu

kompensieren bzw. deren Vorteile zu bündeln. Aufgrund dessen wird angenommen, dass es durchaus bei einigen Organisationen eine Mehrfachnutzung gibt, dies aber eher selten ist.

Die Frage zur Bestätigung oder Widerlegung der Hypothese lautet: „Welche Threat Intelligence Sharing Platform(s) setzt Ihre Organisation ein?“. Hier konnten die Befragten ein oder auch mehrere Plattformen angeben.

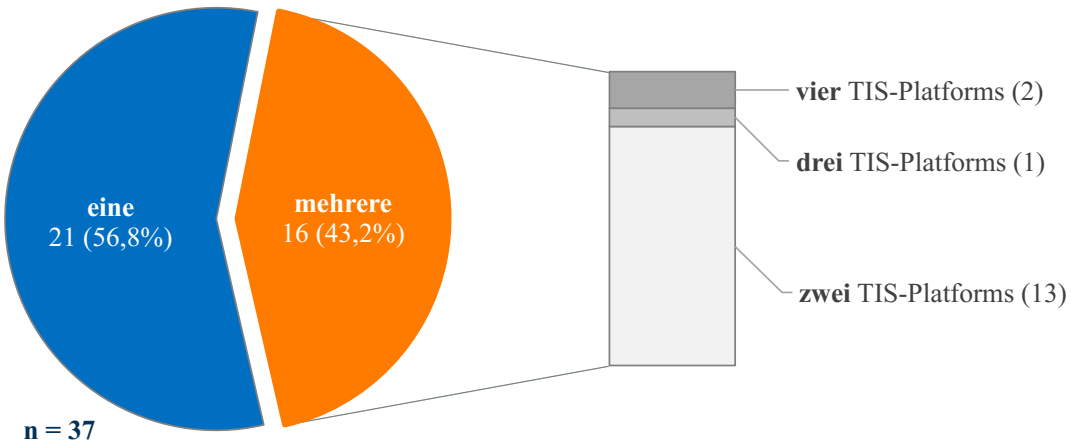

Abb. 4-19: Wie viel Prozent der Organisationen nutzen mehrere TIS-Platforms?

Die Untersuchung ergab, dass 21 der 37 Organisationen (56,8 Prozent) eine Plattform und 16 Organisationen (43,2 Prozent) mehrere Plattformen gleichzeitig einsetzen (vgl. Abb. 4-19). Dabei nutzen 13 Organisationen zwei Threat Intelligence Sharing Platforms gleichzeitig, eine Organisation nutzt drei Plattformen parallel und zwei Organisationen nutzen sogar vier Plattformen gleichzeitig. Hypothese 7 ist damit nicht bestätigt, da fast jede zweite Organisation mehr als eine Threat Intelligence Sharing Platform gleichzeitig nutzt.

Hypothese 8: Organisationen nutzen eher organisationsexterne Threat Intelligence Sharing Platforms und betreiben keine eigenen (organisationsinternen) Plattformen.

Mehrere Studien kommen zu dem Ergebnis, dass Organisationen eher Threat Intelligence konsumieren als produzieren [ZSSi2022, 7; BrSt2022, 9; Lee2020, 8; BrLe2019, 10]. Zudem ist Open Threat Exchange als international verbreitete Plattform eine externe Threat Intelligence Sharing Platform. Weiterhin ist der Ressourcenaufwand, abgesehen von den Lizenzkosten, für die Nutzung einer externen Plattform geringer als bei dem Betrieb einer internen Threat Intelligence Sharing Platform. Gegen den Einsatz einer externen Plattform sprechen gegebenenfalls der Verlust der eigenen Datenhoheit sowie höhere Lizenzkosten verglichen mit einer internen, quelloffenen Plattform. Untersuchungen belegen, dass ein

großer Anteil der Organisationen auf geteilte Threat Intelligence von externen Behördenplattformen zurückgreifen [Lee2020, 16; Thre2019, 11].

Zur Bestätigung oder Widerlegung der Hypothese wurde folgende Frage gestellt: „Werden Threat Intelligence Sharing Platforms selbst betrieben oder organisationsexterne Plattformen genutzt?“.

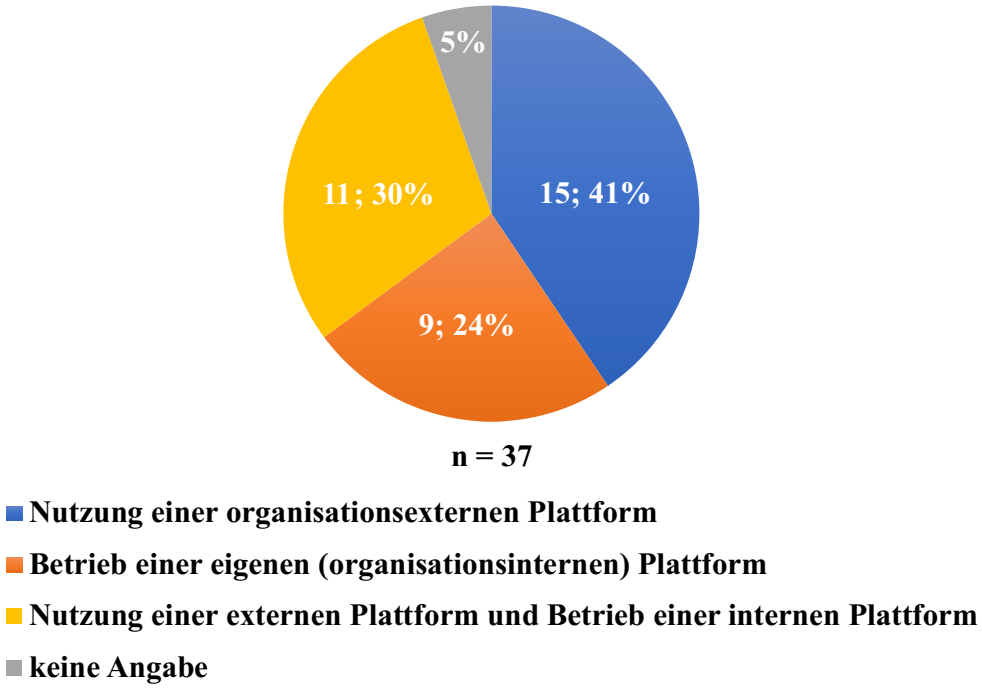

Abb. 4-20: Werden Threat Intelligence Sharing Platforms selbst betrieben?

Neun Organisationen (24 Prozent) betreiben eine eigene (organisationsinterne) Threat Intelligence Sharing Platform. 15 Organisationen (41 Prozent) nutzen eine organisationsexterne Plattform. Elf Organisationen (30 Prozent) betreiben sowohl eine eigene Plattform und nutzen zudem eine organisationsexterne Plattform (vgl. Abb. 4-20). Zwei Organisationen antworteten nicht auf die Frage. In Summe nutzen 71 Prozent der Organisationen eine externe Plattform und nur 54 Prozent eine interne Plattform. Damit ist oben genannte Hypothese bestätigt. Sofern Organisationen nur eine externe oder nur eine interne Threat Intelligence Sharing Platform nutzen, ist dies häufiger eine externe Plattform.

Hypothese 9: Die Mehrheit der Organisationen nutzt die Funktionen ihrer Threat Intelligence Sharing Platforms regelmäßig und nicht nur anlassbezogen.

Informationen über IT-Bedrohungen veralten schnell. Es ist wichtig, diese zeitnah zu erhalten. Bis Informationen über IT-Bedrohungen in den Threat-Intelligence-Feeds veröffentlicht werden, kann es mehrere Wochen dauern [BGED+2020, 441]. Um mit möglichst aktuellen Informationen zu arbeiten, ist es ratsam, Threat-Intelligence-Werkzeuge täglich zu verwenden. Eine Umfrage eines Anbieters einer Threat Intelligence Sharing Platform ergab, dass 41 Prozent der Organisationen durchgängig mit Threat Intelligence agieren [Thre2019, 10]. Es ist zu erwarten, dass die Mehrheit der befragten Organisationen ihre Threat Intelligence Sharing Platforms regelmäßig nutzen.

Um die Hypothese zu bestätigen oder zu widerlegen, wurde folgende Frage gestellt: „Wie häufig werden die folgenden Funktionen von Threat Intelligence Sharing Platforms in Ihrer Organisation genutzt?“

	überhaupt nicht	unregelmäßig	monatlich	wöchentlich	täglich	keine Angabe
Sammlung von Threat Intelligence	○	○	○	○	○	○
Vorverarbeitung von Threat Intelligence	○	○	○	○	○	○
Analyse von Threat Intelligence	○	○	○	○	○	○
Austausch/Verbreitung von Threat Intelligence	○	○	○	○	○	○
Bewertung und Feedback von Threat Intelligence	○	○	○	○	○	○

Abb. 4-21: Wie häufig werden TIS-Platform-Funktionen genutzt? (Fragebogen)

Anhand einer Likert-Skala, die von „überhaupt nicht“ über „unregelmäßig“[39] bis „täglich“ reicht, sollten die Befragten angeben, wie häufig sie die Funktionen der Plattformen nutzen (vgl. Abb. 4-21). Die vorgegebenen Funktionen [SFRR+2021, 4 f.] der Threat Intelligence Sharing Platforms orientieren sich an den Prozessen beziehungsweise Phasen des Threat-Intelligence-Lebenszyklus (vgl. Abb. 2-1). Die Planungsphase ist nicht enthalten, da diese anbieterabhängig ist und die zugehörigen Funktionen nicht von jeder Plattform unterstützt

[39] Im Online-Fragebogen wurde diese Auswahlmöglichkeit präzisiert durch die Ergänzung „anlassbezogen (zum Beispiel bei Sicherheitsvorfällen)“.

werden. Weiterhin wurde die prozessübergreifende Unterstützung nicht berücksichtigt, da in dieser alle Prozesse unterstützt werden und kein spezifischer Prozess.

Am häufigsten werden Threat Intelligence Sharing Platforms für die „Sammlung von Threat Intelligence“ genutzt. 22 Befragte (59,2 Prozent) gaben an, die Plattformen dafür täglich zu nutzen. Niemand gab an, die Plattformen dafür überhaupt nicht zu verwenden (vgl. Abb. 4-22). Für die „Vorverarbeitung, Analyse und Austausch/Verbreitung von Threat Intelligence“ werden die Plattformen auch eher regelmäßig als anlassbezogen oder überhaupt nicht verwendet.

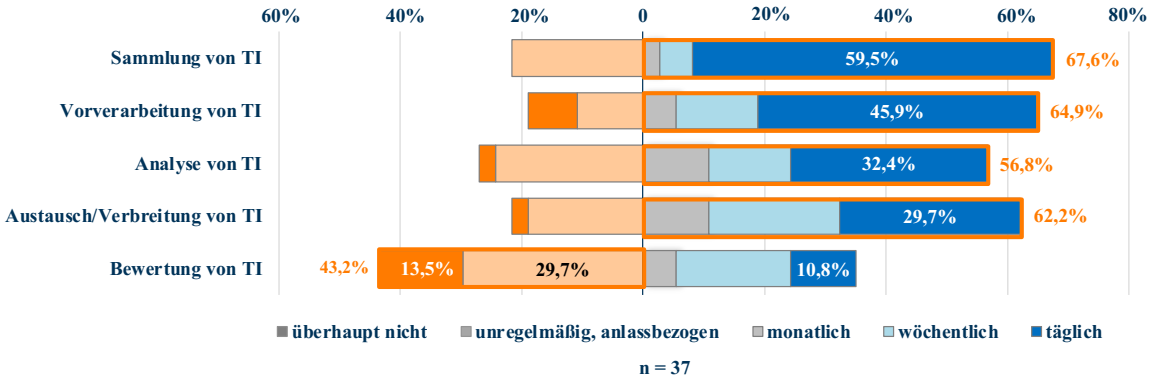

Abb. 4-22: Wie häufig werden welche Funktionen einer TIS-Platform genutzt?

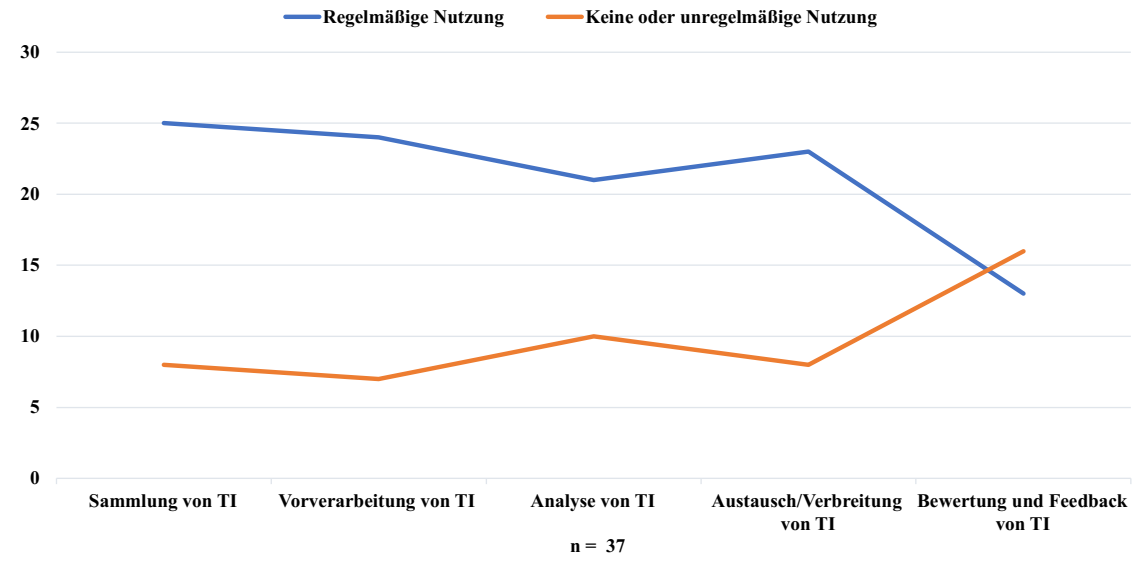

Abb. 4-23: Kumulierte Nutzungshäufigkeit der Funktionen von TIS-Platforms

Für „Bewertung und Feedback von Threat Intelligence“ gaben fünf Befragte (13,5 Prozent) an, die Plattformen überhaupt nicht zu nutzen und 11 Personen (29,7 Prozent) gaben an, sie nur anlassbezogen zu nutzen. Diese Funktionen werden bei Threat Intelligence Platforms eher nicht oder unregelmäßig als regelmäßig genutzt. Möglicherweise gibt es in diesem

Funktionsbereich Verbesserungspotenzial für die Anbieter von Threat Intelligence Sharing Platforms. Andernfalls könnten hier die Prozesse oder die Umsetzung bei der Arbeit mit Threat Intelligence in den Organisationen verbessert werden. Hypothese 9 ist damit überwiegend bestätigt. Mit Ausnahme der Funktionsgruppe „Bewertung und Feedback von Threat Intelligence“ werden Threat Intelligence Sharing Platforms von den befragten Organisationen regelmäßig genutzt (vgl. Abb. 4-23).

Hypothese 10: Über die Hälfte der Organisationen verbindet beziehungsweise integriert Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen (zum Beispiel Firewall, SIEM etc.).

Um den sicheren Betrieb der IT-Infrastruktur zu gewährleisten, setzen die meisten Organisationen Netzwerkanalysewerkzeuge oder Security-Information-and-Event-Management-Software ein [BrSt2022, 11; Lee2020, 7; LLCC+2020, 20; Thre2019, 10; Pone2019, 3; Shac2018, 8; Shac2017, 13; Shac2016, 12; Shac2015, 11]. Threat Intelligence Sharing Platforms profitieren von organisationsinternen Informationen, wie zum Beispiel Schwachstellendaten, da diese spezifisch für die Organisation erhoben werden und damit auf die Organisation zugeschnitten sind, im Gegensatz zu Daten aus Threat Intelligence Feeds.

Um oben genannte Hypothese zu bestätigen, wurde folgende Frage gestellt: „Sind Threat Intelligence Sharing Platforms in Ihrer Organisation mit anderen IT-Sicherheitssystemen verbunden beziehungsweise mit diesen integriert?“

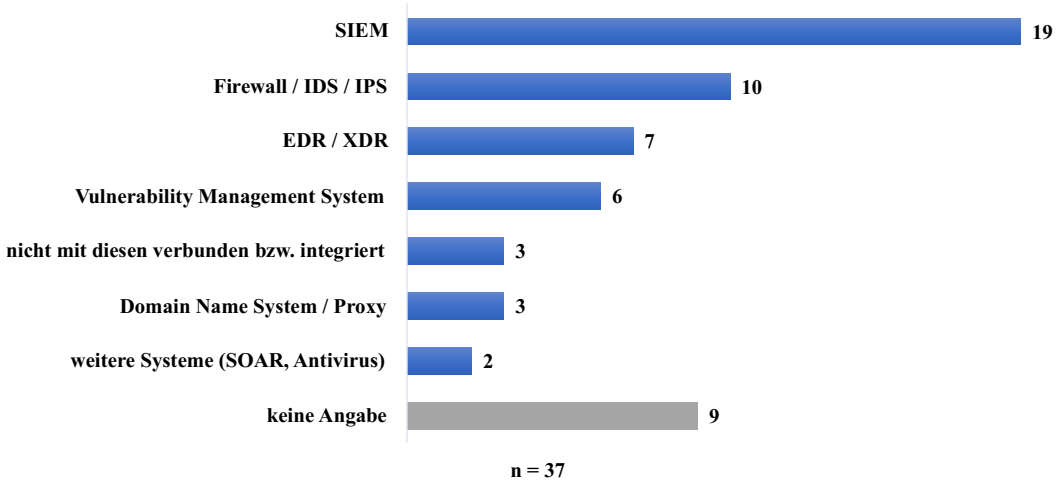

Abb. 4-24: Sind TIS-Platforms mit anderen IT-Sicherheitssystemen verbunden?

Über die Hälfte der Befragten (51,4 Prozent) gab an, ihre Threat Intelligence Sharing Platform in Verbindung mit einem SIEM zu nutzen (vgl. Abb. 4-24). Etwa ein Drittel (27,0

Prozent) nutzt die Plattform in Verbindung mit einer Firewall, einem Intrusion Detection System (IDS) oder einem Intrusion Prevention System (IPS) und 18,9 Prozent verknüpfen die Plattform mit einer Software für Endpoint Detection and Response (EDR) oder Extended Detection and Response (XDR). Knapp jede zwölfte Organisation (8,1 Prozent) gab an, ihre Threat Intelligence Sharing Platform nicht mit IT-Sicherheitssystemen zu verbinden oder zu integrieren. Der gleiche Anteil Organisationen verbindet die Plattformen mit einem Domain Name System (DNS) oder Proxy[40]. Weiterhin wurden folgende IT-Sicherheitssysteme zur Verbindung oder Integration mit Threat Intelligence Sharing Platforms genannt: SOAR-Technologien (Security Orchestration, Automation and Response) und Antivirus-Software.

25 Organisationen (67,6 Prozent) integrieren Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen, drei Organisationen tun dies nicht. Damit ist Hypothese 10 bestätigt, etwa vier von fünf Organisationen integrieren Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen.

Hypothese 11: Threat Intelligence Sharing Platforms werden bevorzugt zur Sammlung, Vorverarbeitung und Analyse und weniger zum Austausch und zur Bewertung von Threat Intelligence genutzt.

Beginnt eine Organisation mit der Nutzung von Threat Intelligence Sharing Platforms, müssen zuerst Daten in die Plattformen gelangen. Aufgrund dessen ist zu erwarten, dass Organisationen, die seit Kurzem Threat Intelligence Sharing Platforms nutzen, diese bereits zur Sammlung und Vorverarbeitung von Threat Intelligence verwenden. Durch Nutzung der Plattformen erschließen sich den Anwendern weitere Funktionen, wie zum Beispiel die Analyse von Threat Intelligence. Die meisten Funktionen bieten Threat Intelligence Sharing Platforms im Bereich der Analyse [SFRR+2021, 7]. Es wird angenommen, dass die Plattformen zur Sammlung, Vorverarbeitung und Analyse am häufigsten genutzt werden, weil einige Organisationen erst seit Kurzem Threat Intelligence Sharing Platforms nutzen (vgl. Hypothese 1). Organisationen, die den Umgang mit Threat Intelligence Sharing Platforms beherrschen, werden in der Lage sein, Threat Intelligence zu verbreiten und zu bewerten. Für die Prüfung der Hypothese wurden die Organisationen gefragt: „Wie häufig werden die folgenden Funktionen von Threat Intelligence Sharing Platforms in Ihrer Organisation genutzt?“ beziehungsweise für Organisationen, die planen, diese Plattformen

[40] Dabei können zum Beispiel Logdaten eines Proxy-Servers ausgewertet werden.

zu nutzen: „Welche der folgenden Funktionen von Threat Intelligence Sharing Platforms planen Sie zu nutzen?“.

Abb. 4-22 zeigt, dass Threat Intelligence Sharing Platforms etwa gleich häufig zur Sammlung, Vorverarbeitung, Analyse und Austausch beziehungsweise Verbreitung von Threat Intelligence und weniger zur Bewertung und Feedback von Threat Intelligence genutzt werden. Damit ist oben genannte Hypothese widerlegt, nur die Funktionen aus dem Bereich Bewertung und Feedback werden bei den Plattformen weniger genutzt als andere Funktionen.

Für Organisationen, die planen, Threat Intelligence Sharing Platforms einzusetzen, wäre die Hypothese tendenziell bestätigt. Diese Organisationen würden die Plattformen eher zur Sammlung, Vorverarbeitung und Analyse von Threat Intelligence nutzen, als zum Austausch und zur Bewertung von Threat Intelligence (vgl. Abb. 4-25).

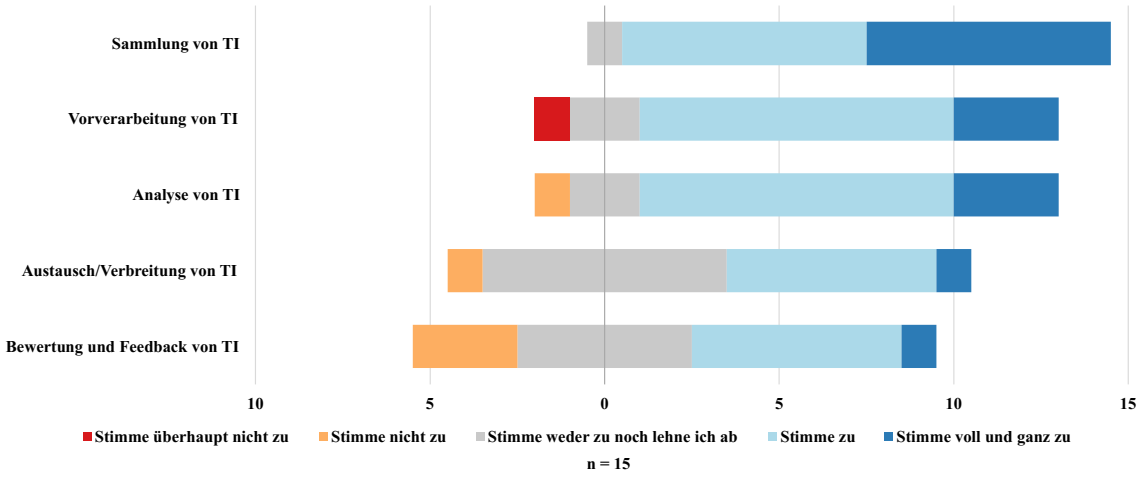

Abb. 4-25: Welche Funktionen von TIS-Platforms planen Organisationen zu nutzen?

Hypothese 12: Organisationen teilen Threat Intelligence mithilfe von Threat Intelligence Sharing Platforms eher organisationsintern als -extern.

Der Austausch von Threat Intelligence ist pandemiebedingt weniger geworden [BrSt2022, 2]. Zudem gibt es Gründe, die gegen den Austausch von Threat Intelligence sprechen, zum Beispiel Bedenken, dass geteilte Daten missbraucht werden könnten [Pone2019, 6] oder Datenschutzbedenken[41]. Weiterhin teilen viele Organisationen Threat Intelligence nicht mit externen Gruppen [Thre2019, 12].

[41] Vgl. Kapitel 4.3.5

Um Hypothese 12 zu bestätigen oder zu widerlegen, wurde folgende Frage gestellt: „Mit wem werden in Ihrer Organisation Bedrohungsinformationen (Threat Intelligence) geteilt?“ 15 der 37 Organisationen (40,5 Prozent) teilen Bedrohungsinformationen sowohl organisationsintern als auch -extern. Sieben Organisationen (18,9 Prozent) teilen Threat Intelligence nur mit organisationsinternen Stellen und fünf Organisationen (13,5 Prozent) nur mit organisationsexternen Stellen beziehungsweise Partnern (vgl. Abb. 4-26). In Summe teilen über die Hälfte der Organisationen Threat Intelligence extern, damit ist die oben genannte Hypothese nicht bestätigt.

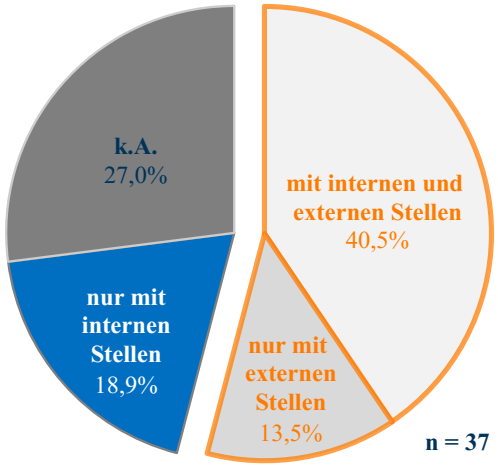

Abb. 4-26: Mit wem wird Threat Intelligence über TIS-Platforms geteilt?

Hypothese 13: Am häufigsten nutzen Organisationen Threat Intelligence Sharing Platforms zur Unterstützung im Aufgabenbereich Incident Management.

In ähnlichen Studien gehören die meisten Befragten dem Security Operations Center an. Dieses deckt viele Aufgabengebiete ab, beispielsweise die Erkennung von IT-Bedrohungen und IT-Angriffen. In dieser Studie wurden viele Chief Information Security Officer befragt, mit der Erwartung, dass die Unterstützung des Incident Managements zu den wichtigsten Aufgabengebieten einer Threat Intelligence Sharing Platform gehört.

Eine weitere Gruppe, die zu den häufigsten Vertretern in ähnlichen Studien zählt, sind Mitarbeitende des Bereiches Incident Response [BrSt2022, 3; BrLe2021, 4; Lee2020, 4; BrLe2019, 8; Shac2018, 6; Shac2017, 8; Shac2016, 15]. Des Weiteren ist Incident Response beziehungsweise Incident Management ein wesentlicher Anwendungsfall für Threat Intelligence [BrLe2021, 14; LLCC+2020, 6; Shac2018, 4].

Zum Bestätigen oder Widerlegen der oben genannten Hypothese wurde folgende Frage gestellt: „Welche Aufgabenbereiche werden in Ihrer Organisation durch Threat Intelligence Sharing Platforms unterstützt?“.

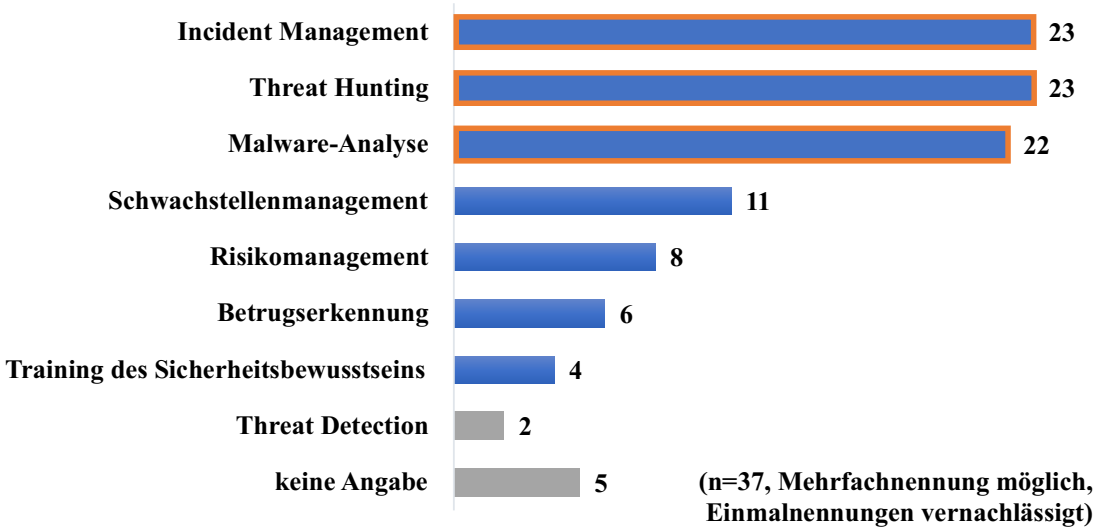

Abb. 4-27: Welche Aufgabenbereiche werden durch TIS-Platforms unterstützt?

Jeweils 23 der Befragten (62,1 Prozent) nutzen ihre Threat Intelligence Sharing Platforms zur Unterstützung der Aufgabenbereiche Threat Hunting[42] und Incident Management. 22 der Befragten (59,4 Prozent) nutzen die Plattformen für die Analyse von Malware. Mit signifikantem Abstand folgen Schwachstellenmanagement (29,7 Prozent), Risikomanagement (21,6 Prozent), Betrugserkennung (16,2 Prozent) und Training des Sicherheitsbewusstseins (10,8 Prozent) (vgl. Abb. 4-27).

Threat Detection wurde von zwei Personen als weiterer Aufgabenbereich erwähnt, der durch Einsatz der Plattformen unterstützt wird. Wäre dieser Aufgabenbereich als Antwortmöglichkeit vorgegeben gewesen, hätten vermutlich weitere Organisationen diesen ausgewählt. Es ist nicht auszuschließen, dass einzelne Befragte Threat Hunting und Threat Detection gleichbedeutend interpretiert haben, obwohl Threat Hunting eher eine proaktive Aufgabe ist als die häufig automatisierte Detektion. Andererseits nutzen viele Organisationen die Plattformen für die Malware-Analyse, die neben dem Threat Hunting ebenfalls eine technisch anspruchsvolle Aufgabe ist, da umfassende Kenntnisse über die Funktionsweise von IT-Angriffen und das Verhalten der Angreifer Voraussetzung sind. Dass

[42] Threat Hunting ist eine proaktive Vorgehensweise zur Identifizierung von bisher unbekannten oder noch nicht behobenen Bedrohungen im Netzwerk einer Organisation [IBM2023].

die Malware-Analyse zu den häufigsten, durch die Plattformen unterstützten Aufgabengebieten zählt, zeigt, wie erfahren die Mehrheit der teilnehmenden Organisationen im Umgang mit den Plattformen ist.

Hypothese 13 ist damit bestätigt. Incident Management gehört zu den häufigsten Aufgabenbereichen, die durch Threat Intelligence Sharing Platforms unterstützt werden. Weitere wichtige Aufgabenbereiche für die Plattformen sind das Threat Hunting und die Malware-Analyse.

4.3.5 Weitere Erkenntnisse

Gründe für den Verzicht auf das Teilen von Threat Intelligence

Auf die Frage, warum Organisationen auf das Teilen von Threat Intelligence verzichten, gab es wenige Antworten, da nur wenige der befragten Organisationen keine Threat Intelligence austauschen. Genannt wurden folgende Gründe: eine zu große Herausforderung im Hinblick auf Datenschutz und Compliance, mangelnde Qualität der Threat Intelligence, der benötigte Mehraufwand für das Teilen von Threat Intelligence und, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) derzeit keinen Austausch anbietet.

Zufriedenheit mit Threat Intelligence Sharing Platforms

Zum Abschluss der Befragung wurde die Zufriedenheit mit der Nutzung von Threat Intelligence Sharing Platforms ermittelt (vgl. Abb. 4-28). Keiner der Befragten äußerte sich „äußerst unzufrieden“. Zwei Teilnehmer (5,4 Prozent) waren mit der Nutzung der Plattformen „unzufrieden“ und fünf weitere (13,5 Prozent) „weder zufrieden noch unzufrieden“. Knapp die Hälfte der Teilnehmer (48,6 Prozent) äußerte sich „zufrieden“ mit der Nutzung von Threat Intelligence Sharing Platforms und vier Befragte (10,8 Prozent) waren „äußerst zufrieden“. Acht Befragte machten keine Angabe zur Zufriedenheit, davon antworteten sechs Teilnehmer nicht mehr auf diese Frage. Mehr als zwei Drittel der Befragten waren mit der Nutzung von Threat Intelligence Sharing Platforms „zufrieden“ oder „äußerst zufrieden“. Im Durchschnitt waren die Befragten mit der Nutzung von Threat Intelligence Sharing Platforms eher zufrieden als unzufrieden. Die Zufriedenheit mit einzelnen Funktionen von Threat-Intelligence-Werkzeugen wurde in mehreren Studien [BrLe2021, 13 ff.; BrLe2019, 14; Shac2018, 10; Shac2017, 16] untersucht und könnte Grundlage für einen Vergleich mit den Ergebnissen dieser Studie sein.

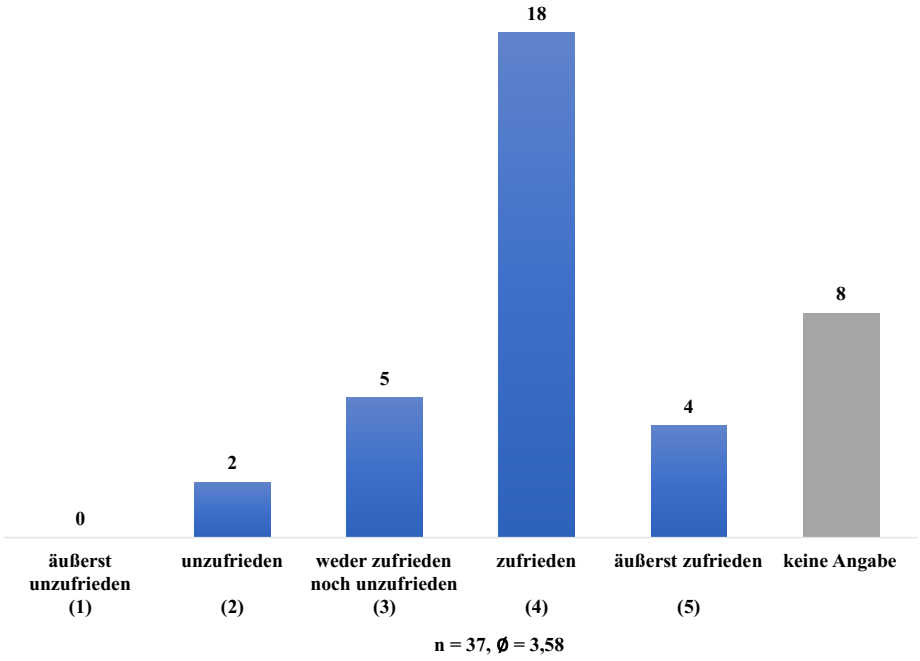

Abb. 4-28: Wie zufrieden sind Organisationen mit der Nutzung von TIS-Platforms?

5 Schlussbemerkungen

5.1 Zusammenfassung

Im Rahmen dieser Studie wurde untersucht, wie verbreitet Threat Intelligence Sharing Platforms in Deutschland, Österreich und der Schweiz sind und wie diese in Unternehmen, Behörden und Universitäten genutzt werden. Die Online-Befragung wurde von Juli bis August 2022 durchgeführt und an 380 Organisationen im DACH-Raum versendet. Personen aus 69 Organisationen haben den Fragebogen beantwortet, 63 davon vollständig und sechs nahezu vollständig. Die Untersuchung ergab unter anderem folgende Ergebnisse: Mehr als die Hälfte der befragten Organisationen im DACH-Raum setzt Threat Intelligence Sharing Platforms ein. 84,2 Prozent der börsennotierten Unternehmen verwenden die Plattformen und damit signifikant mehr als Behörden (48,3 Prozent) und Universitäten (33,3 Prozent). Im Ländervergleich setzen die schweizerischen Organisationen am häufigsten Threat Intelligence Sharing Platforms ein (71,4 Prozent), gefolgt von deutschen (53,7 Prozent) und österreichischen (37,5 Prozent) Organisationen. 78 Prozent der antwortenden Organisationen stammen aus Deutschland, weshalb die Ergebnisse für Österreich und die Schweiz eher eine Tendenz für die Verbreitung der Plattformen in diesen Ländern anzeigen. Fast jede

dritte Organisation setzt Threat Intelligence Platforms seit über vier Jahren ein. Des Weiteren hat es in den letzten vier Jahren einen kontinuierlichen Anstieg des Einsatzes gegeben. Von den Organisationen, die bisher keine dieser Plattformen einsetzen, planen etwa die Hälfte den Einsatz innerhalb der nächsten fünf Jahre. Somit ist davon auszugehen, dass der Einsatz von Threat Intelligence Sharing Platforms nochmal deutlich weiter zunehmen wird. Je wichtiger der Stellenwert der IT-Sicherheit für die Organisationen ist und je mehr Personen im Bereich der IT-Sicherheit beschäftigt sind, desto häufiger setzen diese Threat Intelligence Sharing Platforms ein. Vier von fünf Organisationen, die ein CERT, SOC oder CSIRT betreiben, setzen die Plattformen ein. Die häufigsten Gründe, warum Organisationen Threat Intelligence Sharing Platforms nicht einsetzen, sind der Mangel an Personal und dass sie ihre Prioritäten bei anderen Technologien sehen. Von den Organisationen, die Threat Intelligence Sharing Platforms einsetzen, nutzen nahezu zwei Drittel MISP. Diese Plattform ist mit Abstand marktführend unter den Teilnehmern diese Studie. Bei der Auswahl von Threat Intelligence Sharing Platforms sind den Organisationen eine hohe Verbreitung der Plattform (zum Beispiel unter Partnern), niedrige Lizenzkosten, ein großer Funktionsumfang sowie der Umfang der angebotenen Bedrohungsinformationen am wichtigsten. Fast jede zweite Organisation, die Threat Intelligence Sharing Platforms einsetzt, nutzt mehrere Plattformen gleichzeitig. Organisationen nutzen eher externe als interne Threat Intelligence Sharing Platforms und teilen Threat Intelligence eher mit externen als mit internen Stellen. Threat Intelligence Sharing Platforms werden für die Sammlung, Vorverarbeitung, Analyse und den Austausch von Threat Intelligence regelmäßig genutzt, für die Bewertung und Feedback von Threat Intelligence werden die Plattformen weniger genutzt. Mehr als zwei Drittel der Organisationen verbinden oder integrieren Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen, dabei werden SIEM-Systeme von 51,4 Prozent der Organisationen genannt. Am häufigsten nutzen die Organisationen Threat Intelligence Sharing Platforms zur Unterstützung der Aufgabenbereiche Incident Management, Threat Hunting und Malware-Analyse.

5.2 Kritische Würdigung

Bisher gab es keine vergleichbare Untersuchung im deutschsprachigen Raum, die die Verbreitung und Nutzung von Threat Intelligence Sharing Platforms untersucht hat. Diese Arbeit konnte viele offene Fragen beantworten und es wurde ein breites Spektrum an Organisationen befragt. Allerdings ist die Aussagekraft der Ergebnisse eher für deutsche

Organisationen gegeben, da aus Österreich und der Schweiz nur relativ wenige Antworten vorliegen. Kleine und mittlere Unternehmen werden in dieser Studie nicht betrachtet, die Aussagekraft ist auf börsennotierte Unternehmen beschränkt. Weiterhin konnte bei den börsennotierten Unternehmen nicht festgestellt werden, welche Branche führend beim Einsatz von Threat Intelligence Sharing Platforms ist, da fast alle der befragten Konzerne diese Plattformen einsetzen. Zudem wurden Unterschiede in der Nutzung von Threat Intelligence Sharing Platforms zwischen Unternehmen, Behörden und Universitäten nicht untersucht.

5.3 Ausblick

Zukünftig könnte man die Befragung wiederholen, um Entwicklungen der Verbreitung von Threat Intelligence Sharing Platforms oder Änderungen bei der Nutzung der Plattformen festzustellen. Dazu wäre es möglich, den Fragebogen zu erweitern beziehungsweise an die zukünftigen technischen Gegebenheiten anzupassen. Durch diese Untersuchung wurde unter anderem bestätigt, dass einige Organisationen im DACH-Raum mehrere Threat Intelligence Sharing Platforms gleichzeitig nutzen. Eine Forschungsfrage für zukünftige Untersuchungen ist, ob diese Plattformen für verschiedene Zwecke verwendet werden. Außerdem könnte eine spezifische Befragung kleiner und mittlerer Unternehmen durchgeführt werden, da diese vermutlich seltener Threat Intelligence Sharing Platforms nutzen. Für die Wiederholung und Ausweitung der Studie wäre das BSI zukünftig ein möglicher Kooperationspartner. Die Allianz für Cyber-Sicherheit, die vom BSI geleitet wird, umfasst mehr als 7.400 Organisationen, die bereits zu verschiedenen Themen der IT-Sicherheit befragt wurden.

Literaturverzeichnis

[ABLe2019] Albakri, A.; Boiten, E.; Lemos, R. de: Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. In: Naldi, M.; Italiano, G. F.; Rannenberg, K.; Medina, M.; Bourka, A. (Hrsg.): Privacy Technologies and Policy. Springer, Cham, 2019, S. 28–41.

[Alie2023] AlienVault: The World's First Truly Open Threat Intelligence Community. Abruf am 12.12.2023, https://otx.alienvault.com/.

[Asso2011] Association for Information Systems (AIS): Association for Information Systems (AIS). Abruf am 12.12.2023, https://aisnet.org/page/SeniorScholarBasket.

[AWS2023] AWS Marketplace: Anomali. Abruf am 12.12.2023, https://aws.amazon.com/marketplace/pp/prodview-unjq3gvyoflti.

[Bake2022] Baker, K.: What is Cyber Threat Intelligence? Abruf am 12.12.2023, https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/.

[BBJK2022] Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A.; Kutka, E.: Overcoming information-sharing challenges in cyber defence exercises. In: Journal of Cybersecurity. 8(1), 2022, S. 1–9.

[BFSL+2020] Bauer, S.; Fischer, D.; Sauerwein, C.; Latzel, S.; Stelzer, D.; Breu, R.: Towards an evaluation framework for threat intelligence sharing platforms. In: Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020, S. 1947–1956.

[BGED+2020] Bouwman, X.; Griffioen, H.; Egbers, J.; Doerr, C.; Klievink, B.; van Eeten, M.: A different cup of TI? The added value of commercial threat intelligence: Proceedings of the 29th USENIX Security Symposium. USENIX Association, Berkeley, CA, 2020.

[BGSe2015] Brown, S.; Gommers, J.; Serrano, O.: From Cyber Security Information Sharing to Threat Management. In: Ray, I.; Sander, T.; Yung, M. (Hrsg.): Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. Denver, Colorado, USA, S. 43–49.

[BrLe2019] Brown, R.; Lee, R. M.: The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey. Abruf am 12.12.2023, https://www.sans.org/white-papers/38790/.

[BrLe2021] Brown, R.; Lee, R. M.: 2021 SANS Cyber Threat Intelligence (CTI) Survey. Abruf am 12.12.2023, https://www.sans.org/white-papers/40080/.

[BrSt2022] Brown, R.; Stirparo, P.: SANS 2022 Cyber Threat Intelligence Survey. Abruf am 12.12.2023, https://www.sans.org/white-papers/sans-2022-cyber-threat-intelligence-survey/.

[BrSu2010] Brunner, E.; Suter, M.: Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz MELANI. Abruf am 12.12.2023, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Evaluation-MELANI-2010.pdf.

[Bund2022a] Bundesministerium für Finanzen: Behörden. Abruf am 12.12.2023, https://www.oesterreich.gv.at/at.gv.brz.portalframe/oegvat/orgsuche/portlet?

[Bund2022b] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben: Adressen der Bundesverwaltung. Abruf am 12.12.2023, https://x500.bund.de/.

[Bund2022c] Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport: Geschäftseinteilung. Abruf am 12.12.2023, https://www.bmkoes.gv.at/dam/jcr:9de63d79-fb53-4184-a63c-df6c6be739c0/Geschäftseinteilung_zum_1._Juli_2022.pdf.

[Bund2022d] Bundeskanzlei: Departemente. Abruf am 12.12.2023, https://www.admin.ch/gov/de/start/departemente.html.

[Bund2022e] Bundesverwaltungsamt: Behörden. Abruf am 12.12.2023, https://www.service.bund.de/Content/DE/Behoerden/Suche/Formular.html.

[Bund2022f] Bundesministerium für Bildung, Wissenschaft und Forschung: Liste Universitäten. Abruf am 12.12.2023, https://www.bmbwf.gv.at/Themen/HS-Uni/Hochschulsystem/Universit%C3%A4ten/Liste-Universit%C3%A4ten.html.

[Bund2022g] Bundesministerium für Finanzen: Personen und Organisationen der österreichischen Bundesverwaltung. Abruf am 12.12.2023, https://www.oesterreich.gv.at/ldap#/suche.

[Bund2022h] Bundesministerium des Innern und für Heimat: Bundesinnenministerin stellt ihre Cybersicherheitsagenda vor. Abruf am 12.12.2023, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html.

[Bund2023] Bundesamt für Sicherheit in der Informationstechnik: Allianz für Cyber-Sicherheit. Abruf am 12.12.2023, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Allianz-fuer-Cyber-Sicherheit/Wer-sind-wir/wer-sind-wir_node.html.

[Byte2022] Byteplant: E-Mail-Validierung. Abruf am 12.12.2023, https://www.email-validator.net/de/.

[CCSL2021] Collins, J.; Contu, R.; Schneider, M.; Lawson, C.: Market Guide for Security Threat Intelligence Products and Services. Abruf am 12.12.2023, https://go.cyware.com/market-guide-for-security-threat-intelligence.

[ChRu2015] Chismon, D.; Ruks, M.: Threat Intelligence: Collecting, Analysing, Evaluating. Abruf am 12.12.2023, https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf.

[Comp2022] Compliance Essentials: Geldbußen für DSGVO-Verstöße. Abruf am 12.12.2023, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/.

[DaSe2013] Dandurand, L.; Serrano, O. S.: Towards improved cyber security information sharing. In: 2013 5th International Conference on Cyber Conflict (CyCon). IEEE, Piscataway, NJ, 2013, S. 1–16.

[DFN-2022a] DFN-CERT Services: Deutscher CERT-Verbund. Abruf am 12.12.2023, https://www.cert-verbund.de/.

[DFN-2022b] DFN-CERT Services: Trusted Introducer – Team Database. Abruf am 12.12.2023, https://www.trusted-introducer.org/contact.html.

[DöBo2016] Döring, N.; Bortz, J.: Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften. Springer, Berlin, Heidelberg, 2016.

[Euro2022] Europäische Kommission: Cyber Resilience Act. Abruf am 12.12.2023, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[Foru2022] Forum of Incident Response and Security Teams (FIRST): FIRST Teams. Abruf am 12.12.2023, https://www.first.org/members/teams/.

[FSWS2023] Fischer, D.; Sauerwein, C.; Werchan, M.; Stelzer, D.: An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany, Austria and Switzerland. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. Benevento, S. 1–7.

[FWS2023] Fischer, D.; Werchan, M.; Sauerwein, C.: Tauschringe für Bedrohungsdaten. In: <kes>: Status quo der Nutzung von Threat-Intelligence-Sharing-Platforms im DACH-Raum. DATAKONTEXT, Frechen, April 2023, S. 10–15.

[Gart2013] Gartner: Definition: Threat Intelligence. Abruf am 12.12.2023, https://www.gartner.com/en/documents/2487216.

[GDGM2018] Gschwandtner, M.; Demetz, L.; Gander, M.; Maier, R.: Integrating Threat Intelligence to Enhance an Organization's Information Security Management. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. Hamburg, S. 1–8.

[GFMä2019] Garousi, V.; Felderer, M.; Mäntylä, M. V.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. In: Information and Software Technology. 106(2019), 2019, S. 101–121.

[Hoch2022] Hochschulrektorenkonferenz: Mitgliedshochschulen. Abruf am 12.12.2023, https://www.hrk.de/mitglieder/mitgliedshochschulen/universitaeten/.

[IBM2023] IBM: Was ist Threat Hunting? Abruf am 12.12.2023, https://www.ibm.com/de-de/topics/threat-hunting.

[Klee2015] Klees, N.: Meckenheimer steuern IT der Bundeswehr. Abruf am 12.12.2023, https://ga.de/news/wirtschaft/regional/meckenheimer-steuern-it-der-bundeswehr_aid-42614921.

[Koep2017] Koepke, P.: Cybersecurity information sharing incentives and barriers. Abruf am 12.12.2023, https://cams.mit.edu/wp-content/uploads/2017-13.pdf.

[KRSt2016] Kromrey, H.; Roose, J.; Strübing, J.: Empirische Sozialforschung: Modelle und Methoden der standardisierten Datenerhebung und Datenauswertung mit Annotationen aus qualitativ-interpretativer Perspektive. UVK; UTB, Konstanz, München, Stuttgart, 2016.

[LBCo2019] Lawson, C.; Benson, R.; Contu, R.: Market Guide for Security Threat Intelligence Products and Services. Abruf am 12.12.2023, https://www.gartner.com/en/documents/3902168.

[Lee2020] Lee, R. M.: 2020 SANS Cyber Threat Intelligence (CTI) Survey. Abruf am 12.12.2023, https://www.sans.org/white-papers/39395/.

[Link2022] LinkedIn: Willkommen in deiner beruflichen Community. Abruf am 12.12.2023, https://de.linkedin.com/.

[LLCC+2020] Lawson, C.; LaPorte, B.; Contu, R.; Collins, J.; Schneider, M.: Market Guide for Security Threat Intelligence Products and Services. Abruf am 12.12.2023, https://www.gartner.com/en/documents/3988089.

[Matt2022] Matthews, T.: The Complete Guide to CSIRT Organization: How to Build an Incident Response Team. Abruf am 12.12.2023, https://www.exabeam.com/incident-response/csirt/.

[MCOG2020] Melo e Silva, A. de; Costa Gondim, J. J.; Oliveira Albuquerque, R. de; García Villalba, L. J.: A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. In: Future Internet. 12(6), 2020, S. 108.

[MISP2022] MISP: Features of MISP, the open source threat sharing platform. Abruf am 12.12.2023, https://www.misp-project.org/features/.

[Moyl2021] Moyle, E.: CERT vs. CSIRT vs. SOC: What's the difference? Abruf am 12.12.2023, https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference.

[MuLe2015] Murdoch, S.; Leaver, N.: Anonymity vs. Trust in Cyber-Security Collaboration. In: Ray, I.; Sander, T.; Yung, M. (Hrsg.): Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. Denver, Colorado, USA, S. 27–29.

[Pone2019] Ponemon Institute: The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies. Abruf am 12.12.2023, https://stratejm.com/wp-content/uploads/2019/08/2019_Ponemon_Institute-Value_of_Threat_Intelligence_Research_Report_from_Anomali.pdf.

[Pone2022] Ponemon Institute: Why We Are Unique. Abruf am 12.12.2023, https://www.ponemon.org/about/.

[Quac2022] Quacquarelli Symonds: QS World University Rankings 2023: Top global universities. Abruf am 12.12.2023, https://www.topuniversities.com/university-rankings/world-university-rankings/2023.

[Qual2022] Qualtrics: Webseite. Abruf am 12.12.2023, https://www.qualtrics.com/de/.

[Raja2019] Rajamäki, J.: European network of Cybersecurity centres and competence Hub for innovation and Operations. Abruf am 12.12.2023,

https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8e7ae90&appId=PPGMS.

[SFRR+2021] Sauerwein, C.; Fischer, D.; Rubsamen, M.; Rosenberger, G.; Stelzer, D.; Breu, R.: From threat data to actionable intelligence: an exploratory analysis of the intelligence cycle implementation in cyber threat intelligence sharing platforms. In: ARES 2021: The 16th International Conference on Availability, Reliability and Security, New York, 2021, S. 1–9.

[Shac2015] Shackleford, D.: Who's Using Cyberthreat Intelligence and How? Abruf am 12.12.2023, https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf.

[Shac2016] Shackleford, D.: The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing. Abruf am 12.12.2023, https://information.rapid7.com/sans-state-of-cti.html.

[Shac2017] Shackleford, D.: Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey. Abruf am 12.12.2023, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/CRN360/20170314_Survey_CTI-2017_LookingGlass.pdf.

[Shac2018] Shackleford, D.: CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey. Abruf am 12.12.2023, https://www.domaintools.com/wp-content/uploads/SANS_CTI_Survey_2018.pdf.

[SHEl2018] Schnell, R.; Hill, P. B.; Esser, E.: Methoden der empirischen Sozialforschung. De Gruyter Oldenbourg, Berlin, Boston, 2018.

[Søre2022] Sørensen, E.: Das neue Schweizer Bundesgesetz über den Datenschutz. Abruf am 12.12.2023, https://www.activemind.de/magazin/schweiz-datenschutz/.

[SSFi2016] Skopik, F.; Settanni, G.; Fiedler, R.: A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security

information sharing. In: Computers & Security. 60(2016), 2016, S. 154–176.

[SSMB2017] Sauerwein, C.; Sillaber, C.; Mussmann, A.; Breu, R.: Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: Leimeister, J. M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), S. 837–851.

[Staa2022] Staatssekretariat für Bildung, Forschung und Innovation SBFI: Universitäre Hochschulen und Hochschulinstitutionen. Abruf am 12.12.2023, https://www.sbfi.admin.ch/sbfi/de/home/hs/hochschulen/kantonale-hochschulen/universitaere-hochschulen-und-hochschulinstitutionen.html.

[StLe2021] Stojkovski, B.; Lenzini, G.: A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Rhodos, S. 324–330.

[SWIT2023] SWITCH: Switch CERT. Abruf am 12.12.2023, https://www.switch.ch/de/cert.

[Thre2019] ThreatConnect: Building a Threat Intelligence Program. Abruf am 12.12.2023, https://threatconnect.com/wp-content/uploads/ThreatConnect-Building-a-Threat-Intelligence-Program.pdf.

[Thre2022] ThreatConnect: ThreatConnect the Company. Abruf am 12.12.2023, https://threatconnect.com/company/.

[ToRa2018] Tounsi, W.; Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. In: Computers & Security. 72(2018), 2018, S. 212–233.

[Toun2019] Tounsi, W.: What is Cyber Threat Intelligence and How is it Evolving? In: Tounsi, W. (Hrsg.): Cyber-vigilance and digital trust. John Wiley & Sons Inc; ISTE Ltd, Hoboken, NJ, London, UK, 2019, S. 1–49.

[Tren2020] Trend Micro: Indicators of compromise. Abruf am 12.12.2023, https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise.

[Verb2015] Verband der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaft e.V. (VHB): Verband der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaft e.V. (VHB). Abruf am 12.12.2023, https://vhbonline.org/fileadmin/user_upload/JQ3_WI.pdf.

[vPEJ2016] van de Kamp, T.; Peter, A.; Everts, M. H.; Jonker, W.: Private Sharing of IOCs and Sightings. In: Katzenbeisser, S.; Weippl, E.; Blass, E.-O.; Kerschbaum, F. (Hrsg.): Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Wien, S. 35–38.

[WDWI2016] Wagner, C.; Dulaunoy, A.; Wagener, G.; Iklody, A.: MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In: Katzenbeisser, S.; Weippl, E.; Blass, E.-O.; Kerschbaum, F. (Hrsg.): Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Wien, S. 49–56.

[WeWa2002] Webster, J.; Watson, R. T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. In: MIS Quarterly. 26(2), 2002, S. xiii–xxiii.

[Wigm2021] Wigmore, I.: threat intelligence feed (TI feed). Abruf am 12.12.2023, https://www.techtarget.com/whatis/definition/threat-intelligence-feed.

[WMPA2019] Wagner, T. D.; Mahbub, K.; Palomar, E.; Abdallah, A. E.: Cyber threat intelligence sharing: Survey and research directions. In: Computers & Security. 87(2019), 2019, S. 1–27.

[Wohl2014] Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Shepperd, M.; Hall, T.; Myrtveit, I. (Hrsg.): Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE'14). London, S. 1–10.

[WPMA2018] Wagner, T. D.; Palomar, E.; Mahbub, K.; Abdallah, A. E.: A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. In: Security and Communication Networks. 2018(2018), 2018, S. 1–11.

[YaKa2019] Yamin, M. M.; Katt, B.: A Survey of Automated Information Exchange Mechanisms Among CERTs. In: Bleimann, U.; Burkhardt, D.; Humm, B.; Loew, R.; Regier, S.; Stengel, I.; Walsh, P. (Hrsg.): Proceedings of the 5th Collaborative European Research Conference, Darmstadt, 2019, S. 311–322.

[ZiSi2019] Zibak, A.; Simpson, A.: Cyber Threat Information Sharing. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. Canterbury, CA, United Kingdom, S. 1–9.

[ZSSi2021] Zibak, A.; Sauerwein, C.; Simpson, A.: A success model for cyber threat intelligence management platforms. In: Computers & Security. 111(2021), 2021, S. 1–19.

[ZSSi2022] Zibak, A.; Sauerwein, C.; Simpson, A. C.: Threat Intelligence Quality Dimensions for Research and Practice. In: Digital Threats: Research and Practice. 3(4), 2022, S. 1–22.

Anhang 1: Forschungsfragen

Fragen zur Verbreitung von Threat Intelligence Sharing Platforms:

- Welche Organisationen setzen Threat Intelligence Sharing Platforms ein und welche nicht? Was charakterisiert diese Organisationen?
- Gibt es den Markt dominierende Threat Intelligence Sharing Platforms?
- Welche Kriterien sind für die Auswahl einer Threat Intelligence Sharing Platform wichtig?
- Was sind Gründe, warum Organisationen auf den Einsatz von Threat Intelligence Sharing Platforms verzichten?

Fragen zur Art und Weise der Nutzung von Threat Intelligence Sharing Platforms:

- Welche Funktionen von Threat Intelligence Sharing Platforms nutzen die Organisationen und wie intensiv nutzen sie diese Funktionen?
- Welche Aufgabenbereiche werden durch die Nutzung von Threat Intelligence Sharing Platforms unterstützt?
- Werden Threat Intelligence Sharing Platforms mit anderen organisationsinternen IT-Sicherheitssystemen verbunden beziehungsweise mit diesen integriert oder werden die Plattformen als Insellösungen betrieben?
- Betreiben Organisationen Threat Intelligence Sharing Platforms häufiger selbst oder nutzen sie organisationsexterne Plattformen?
- Werden Bedrohungsinformationen mithilfe von Threat Intelligence Sharing Platforms eher mit organisationsinternen oder organisationsexternen Stakeholdern geteilt?

Anhang 2: Initiale Suche der Literaturanalyse

Datenbank	Suchterm[43]	Suchort	Ergebnisse
ACM Digital Library	Title:((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)) OR) OR Abstract:((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)) OR) OR Keyword:((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)))	Standardsuche: Titel, Abstract oder Keywords	17
AIS eLibrary	title:(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)) OR abstract:(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)) OR subject:(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))	Standardsuche: Titel, Abstract oder Subject	1
EBSCOhost	TI ((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))) OR AB ((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))) OR SU ((("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis)))	Business Source Premier, Communication & Mass Media Complete, The Nation Archive (DFG), eBook Collection (EBSCOhost), Library, Information Science & Technology Abstracts: Titel, Abstract, Subject Terms	10
IEEE Xplore	(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))	Standardsuche	61
Taylor & Francis Online	(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))	Standardsuche	160
Wiley Online Library	(("threat data" OR "threat information" OR "threat intelligence" OR "threat knowledge") AND (sharing OR exchange) AND (platform OR service OR tool OR system) AND (market OR study OR survey OR overview OR analysis))	Standardsuche	308
Summe			557

[43] Für alle Datenbanken wurde nach der Eingabe des Suchterms auf den Zeitraum ab 2018 gefiltert.

Anhang 3: Rückwärtssuche nach der Snowballing-Methode

Ausgangsquellen	Berücksichtigte Beiträge
[BGED+2020]	[LBCo2019] [BrLe2019] [Pone2019]
[BBJK2022]	[ABLe2019] [BGSe2015] [Koep2017] [MuLe2015] [Raja2019] [StLe2021] [vPEJ2016] [WDWI2016]
[SFRR+2021]	[DaSe2013] [MCOG2020] [GDGM2018] [SSMB2017] [Shac2015] [SSFi2016] [ToRa2018] [WMPA2019]
[ZSSi2021]	[ZiSi2019]
[BrSt2022]	/
[Thre2019]	/
Summe	20

Anhang 4: Konzeptmatrix

Verbreitung und Nutzung von TIS-Platforms	Konzepte				
	Verbreitung von TI-Produkten [44]	Use-Cases für TI [45]	Hemmnisse für den TI-Austausch [46]	Erwähnte TIS-Platform(s)	Methoden
[BGED+2020]	X	X	/	OTX	Empirische Untersuchung
[BBJK2022]	/	/	X	MISP	Fallstudie
[BrSt2022]	X	X	X	keine	Anwenderbefragung (über 200 Personen, weltweit, hauptsächlich USA)
[CCSL2021]	X	X	/	Analyst1, EclecticIQ, Falcon X, Flashpoint, IntSights, MISP, QI-ANXIN, Threat-Book, ThreatConnect, ThreatQ, ThreatStream, X-Force Exchange, ZeroFox	keine explizite (Anbieterübersicht, Marktanalyse)
[Pone2019]	X	X	X	keine	Anwenderbefragung (1.098 Personen, USA und GB)
[SFRR+2021]	X	X	/	CRITs, CIF, Falcon X, MISP, OTX, ThreatConnect, ThreatStream, ThreatQ, X-Force Exchange	Literaturanalyse, Fallstudie
[Thre2019]	/	X	X	keine, aber Durchführung der Befragung von ThreatConnect	Anwenderbefragung (351 Personen, USA)
[WDWI2016]	X	/	/	MISP	Fallstudie
[WMPA2019]	X	X	X	CTX/Soltra Edge, Falcon X, MISP, OTX, ThreatConnect, ThreatExchange, ThreatStream, ThreatQ, X-Force Exchange	Literaturanalyse
[ZiSi2019]	/	X	X	keine	Befragung (67 Personen, GB)
[ZSSi2021]	X	/	/	keine	Befragung (152 Personen, GB)

[44] Dies können Informationen zur Art der Organisationen, die TI-Produkte einsetzen, führenden Branchen oder Nutzerzahlen einzelner Plattformen sein. Zu den Threat-Intelligence-Produkten zählen auch Threat Intelligence Sharing Platforms, allerdings werden diese teils am Rande erwähnt, weshalb das Konzept weiter gefasst wurde.

[45] Beschreibt, wofür Threat Intelligence beziehungsweise Threat Intelligence Sharing Platforms genutzt werden oder welche Aufgabengebiete die Plattformen in den Organisationen unterstützen.

[46] Gründe, die gegen den Austausch von Threat Intelligence beziehungsweise gegen den Einsatz von Threat Intelligence Sharing Platforms sprechen.

Anhang 5: Liste der befragten Organisationen

Unternehmen (DAX, MDAX, ATX, SMI)		
Adidas	Bechtle	Vantage Towers
Airbus	Befesa	Varta
Allianz	Cancom	Wacker Chemie
BASF	Carl Zeiss Meditec	Andritz
Bayer	Commerzbank	AT&S
Beiersdorf	CTS Eventim	BAWAG Group
BMW	Delivery Hero	CA Immo
Brenntag	Deutsche Lufthansa	Do & Co
Continental	Deutsche Wohnen	Erste Group
Covestro	Dürr	EVN AG
Daimler Truck	Encavis	Immofinanz
Deutsche Bank	Evonik Industries	Lenzing AG
Deutsche Börse	Evotec	Mayr-Melnhof
Deutsche Post	Fraport	OMV
Deutsche Telekom	Freenet	Österreichische Post
E.ON	Fuchs Petrolub	Raiffeisen Bank International
Fresenius	GEA Group	S IMMO
Fresenius Medical Care	Gerresheimer	Schoeller-Bleckmann Oilfield
Hannover Rück	Hugo Boss	Uniqa Insurance Group
HeidelbergCement	Jungheinrich	Verbund
HelloFresh	K+S	Vienna Insurance Group
Henkel	Kion Group	Voestalpine
Infineon	Knorr-Bremse	Wienerberger
Linde plc	Lanxess	ABB
Mercedes-Benz Group	LEG Immobilien	Alcon
Merck	Nemetschek	Credit Suisse Group
MTU Aero Engines	ProSiebenSat.1 Media	Geberit
Münchener Rück	Rational	Givaudan
Porsche SE	Rheinmetall	Holcim
Puma	RTL Group	Logitech
Qiagen	Scout24	Lonza Group
RWE	Siemens Energy	Nestlé
SAP	Siltronic	Novartis
Sartorius	Sixt	Partners Group Holding
Siemens	Software	Richemont
Siemens Healthineers	Ströer	Roche Holding
Symrise	TAG Immobilien	SGS
Volkswagen	Talanx	Sika
Vonovia	TeamViewer	Swiss Life
Zalando	Telefónica Deutschland	Swiss Re
Aixtron	Thyssenkrupp	Swisscom
Aroundtown	Uniper	UBS
Aurubis	United Internet	Zurich Insurance Group

Universitäten (Deutschland)	
Bauhaus-Universität Weimar	Universität Erlangen-Nürnberg
Europa-Universität Flensburg	Universität Frankfurt am Main
Europa-Universität Frankfurt (Oder)	Universität Freiburg im Breisgau
FernUniversität in Hagen	Universität für Verwaltungswissen-schaften Speyer
Freie Universität Berlin	Universität Gießen
HafenCity Universität Hamburg	Universität Göttingen
Humboldt-Universität Berlin	Universität Greifswald
Jacobs University Bremen	Universität Halle-Wittenberg
Katholische Universität Eichstätt-Ingolstadt	Universität Hamburg
KIT Karlsruhe	Universität Hannover
Leuphana Universität Lüneburg	Universität Heidelberg
Ludwig-Maximilians-Universität München	Universität Hildesheim
Medizinische Hochschule Hannover	Universität Hohenheim
Sporthochschule Köln	Universität Jena
Technische Hochschule Aachen	Universität Kassel
Technische Universität Bergakademie Freiberg	Universität Koblenz-Landau
Technische Universität Berlin	Universität Konstanz
Technische Universität Braunschweig	Universität Leipzig
Technische Universität Chemnitz	Universität Magdeburg
Technische Universität Clausthal	Universität Mainz
Technische Universität Cottbus-Senftenberg	Universität Mannheim
Technische Universität Darmstadt	Universität Marburg
Technische Universität Dortmund	Universität Münster
Technische Universität Dresden	Universität Oldenburg
Technische Universität Hamburg	Universität Osnabrück
Technische Universität Ilmenau	Universität Paderborn
Technische Universität Kaiserslautern	Universität Passau
Technische Universität München	Universität Potsdam
Tierärztliche Hochschule Hannover	Universität Regensburg
Universität Augsburg	Universität Rostock
Universität Bamberg	Universität Siegen
Universität Bayreuth	Universität Stuttgart
Universität Bielefeld	Universität Trier
Universität Bochum	Universität Tübingen
Universität Bonn	Universität Ulm
Universität Bremen	Universität Vechta
Universität der Bundeswehr Hamburg	Universität Witten/Herdecke
Universität der Bundeswehr München	Universität Wuppertal
Universität des Saarlandes	Universität Würzburg
Universität Duisburg-Essen	Universität zu Kiel
Universität Düsseldorf	Universität zu Köln
Universität Erfurt	Universität zu Lübeck

Universitäten (Österreich)
Akademie der bildendenden Künste Wien
Johannes Kepler Universität Linz
Medizinische Universität Graz
Medizinische Universität Innsbruck
Medizinische Universität Wien
Montanuniversität Leoben
Technische Universität Graz
Technische Universität Wien
Universität für angewandte Kunst Wien
Universität für Bodenkultur Wien
Universität für künstlerische und industrielle Gestaltung Linz
Universität für Musik und darstellende Kunst Graz
Universität für Musik und darstellende Kunst Wien
Universität für Weiterbildung Krems
Universität Graz
Universität Innsbruck
Universität Klagenfurt
Universität Mozarteum Salzburg
Universität Salzburg
Universität Wien
Veterinärmedizinische Universität Wien
Wirtschaftsuniversität Wien

Universitäten (Schweiz)
Eidgenössische Technische Hochschule Zürich
FernUni Schweiz
Hochschulinstitut für internationale Studien und Entwicklung
Università della Svizzera Italiana
Universität Basel
Universität Bern
Universität Freiburg
Universität Genf
Universität Luzern
Universität St. Gallen
Universität Zürich
Université de Lausanne
Université de Neuchâtel
SWITCH-CERT

Behörden (Deutschland)
Auswärtiges Amt
Beauftragte der Bundesregierung für Kultur und Medien
Beschaffungsamt des BMI
Bundesagentur für Arbeit
Bundesamt für Auswärtige Angelegenheiten
Bundesamt für Bauwesen und Raumordnung
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Bundesamt für die Sicherheit der nuklearen Entsorgung
Bundesamt für Familie und zivilgesellschaftliche Aufgaben
Bundesamt für Güterverkehr
Bundesamt für Justiz
Bundesamt für Kartographie und Geodäsie
Bundesamt für Migration und Flüchtlinge
Bundesamt für Naturschutz
Bundesamt für Seeschifffahrt und Hydrographie
Bundesamt für Sicherheit in der Informationstechnik
Bundesamt für Soziale Sicherung
Bundesamt für Strahlenschutz
Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
Bundesamt für Wirtschaft und Ausfuhrkontrolle
Bundesamt für zentrale Dienste und offene Vermögensfragen
Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
Bundesanstalt für Geowissenschaften und Rohstoffe
Bundesanstalt für Gewässerkunde
Bundesanstalt für Immobilienaufgaben
Bundesanstalt für Landwirtschaft und Ernährung
Bundesanstalt für Materialforschung und -prüfung
Bundesanstalt für Straßenwesen
Bundesanstalt für Verwaltungsdienstleistungen
Bundesanstalt für Wasserbau
Bundesarchiv
Bundesaufsichtsamt für Flugsicherung
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Bundeseisenbahnvermögen
Bundesinstitut für Arzneimittel und Medizinprodukte
Bundesinstitut für Berufsbildung
Bundesinstitut für Bevölkerungsforschung
Bundesinstitut für Risikobewertung
Bundeskanzleramt
Bundeskartellamt
Bundeskriminalamt
Bundesministerium der Finanzen
Bundesministerium der Justiz
Bundesministerium der Verteidigung
Bundesministerium des Innern und für Heimat
Bundesministerium für Arbeit und Soziales
Bundesministerium für Bildung und Forschung

Bundesministerium für Digitales und Verkehr
Bundesministerium für Ernährung und Landwirtschaft
Bundesministerium für Familie, Senioren, Frauen und Jugend
Bundesministerium für Gesundheit
Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
Bundesministerium für Wirtschaft und Klimaschutz
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
Bundesnetzagentur
Bundespolizei
Bundespräsidialamt
Bundespresseamt
Bundesrechnungshof
Bundessortenamt
Bundesstelle für Eisenbahnunfalluntersuchung
Bundesstelle für Flugunfalluntersuchung
Bundesverwaltungsamt
Bundeswehr
Bundeszentralamt für Steuern
Bundeszentrale für gesundheitliche Aufklärung
Bundeszentrale für Kinder- und Jugendmedienschutz
Bundeszollverwaltung
BWI GmbH
Dataport GmbH
Deutsche Bundesbank
Deutsche Patent- und Markenamt
Deutsche Rentenversicherung
Deutscher Wetterdienst
Eisenbahn-Bundesamt
Fernstraßen-Bundesamt
Friedrich-Loeffler-Institut (Bundesforschungsinstitut für Tiergesundheit)
Informationstechnikzentrum Bund
IT-Dienstleistungszentrum Berlin (ITDZ Berlin)
IT.NRW
Johann Heinrich von Thünen-Institut
Julius Kühn-Institut (Bundesforschungsinstitut für Kulturpflanzen)
Kraftfahrt-Bundesamt
Luftfahrt-Bundesamt
Max Rubner-Institut (Bundesforschungsinstitut für Ernährung und Lebensmittel)
Paul-Ehrlich-Institut
Physikalisch-Technische Bundesanstalt
Robert Koch-Institut
Statistisches Bundesamt
Umweltbundesamt
Wasserstraßen- und Schifffahrtsverwaltung des Bundes
Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Behörden (Österreich)
Bundeskanzleramt
Bundesministerium für Arbeit
Bundesministerium für Bildung, Wissenschaft und Forschung
Bundesministerium für Digitalisierung und Wirtschaftsstandort
Bundesministerium für europäische und internationale Angelegenheiten
Bundesministerium für Finanzen
Bundesministerium für Inneres
Bundesministerium für Justiz
Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium für Landesverteidigung
Bundesministerium für Landwirtschaft, Regionen und Tourismus
Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
Bundesrechenzentrum GmbH
IKT-Sicherheit der Stadt Wien
Präsidentschaftskanzlei

Behörden (Schweiz)
Bundesamt für Bevölkerungsschutz
Bundesamt für Energie
Bundesamt für Gesundheit
Bundesamt für Informatik und Telekommunikation
Bundesamt für Kommunikation
Bundesamt für Kultur
Bundesamt für Lebensmittelsicherheit und Veterinärwesen
Bundesamt für Meteorologie und Klimatologie
Bundesamt für Polizei
Bundesamt für Rüstung armasuisse
Bundesamt für Sozialversicherungen
Bundesamt für Statistik
Bundeskanzlei
Eidgenössisches Departement des Innern
Eidgenössisches Departement für auswärtige Angelegenheiten
Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
Eidgenössisches Finanzdepartement
Eidgenössisches Justiz- und Polizeidepartement
GovCERT.ch
Informatik Service Center ISC-EJPD
Nationales Zentrum für Cybersicherheit
Schweizerisches Bundesarchiv

Anhang 6: Fragebogen[47]

1 Angaben zur Organisation

F1: In welcher Art von Organisation sind Sie tätig?

- o Unternehmen → weiter mit Frage 2
- o Behörde → weiter mit Frage 3
- o Universität → weiter mit Frage 3
- o Sonstige: _____ → weiter mit Frage 3
- o keine Angabe → weiter mit Frage 3

F2: In welcher Branche ist Ihr Unternehmen tätig?

- o Finanzen
- o Maschinenbau, Verkehr, Logistik
- o Technologie
- o Chemie, Pharma, Bio- und Medizintechnik
- o Handel und Konsum
- o Energie und Rohstoffe
- o Sonstige: _____
- o keine Angabe

F3: In welchem Land befindet sich der Hauptsitz Ihrer Organisation?

- o Deutschland
- o Österreich
- o Schweiz
- o Sonstige: _____
- o keine Angabe

F4: Wie viele Personen sind in Ihrer Organisation tätig?

- o ≤ 500
- o 501 – 1.000
- o 1.001 – 5.000
- o 5.001 – 15.000
- o 15.001 – 50.000
- o 50.001 – 100.000
- o > 100.000
- o keine Angabe

F5: Was ist Ihre Rolle innerhalb der Organisation?

- o CEO / Direktor:in / Präsident:in
- o Chief Information Officer (CIO) / IT-Leiter:in
- o Chief Information Security Officer (CISO)
- o IT-Sicherheitsbeauftragte:r (ISB)

[47] Legende: Bei Fragen mit Rechtecken als Auswahlmöglichkeit sind mehrere Antworten zulässig, bei Fragen mit Kreisen ist nur eine Antwort möglich.

- o Abteilungs- / Referatsleitung
- o IT-Systemadministrator:in
- o Analyst:in im SOC / CERT / CSIRT
- o Sonstige: _____
- o keine Angabe

F6: Wie viele Jahre Berufserfahrung haben Sie im Bereich IT-Sicherheit?

- o < 2 Jahre
- o 2 – 5 Jahre
- o 6 – 10 Jahre
- o > 10 Jahre
- o keine Angabe

F7: Welche Zertifizierungen und Qualifikationen haben Sie im Bereich IT-Sicherheit?

Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
Certified Ethical Hacker (CEH)
Cisco Certified Network Professional (CCNP)
Certified Information Systems Auditor (CISA)
Sonstige: _____
keine Angabe

F8: Verfügt Ihre Organisation über eine oder mehrere der folgenden Organisationseinheiten?

Computer Emergency Readiness Team (CERT)
Computer Security Incident Response Team (CSIRT)
Security Operations Center (SOC)
Abteilung für IT-Sicherheit (abgesehen von CERT, CSIRT und SOC)
keine Angabe

F9: Wie viele Personen sind in Ihrer Organisation insgesamt im Bereich IT-Sicherheit (CERT, CSIRT, SOC etc.) beschäftigt?

- o < 10
- o 10 – 50
- o 51 – 100
- o > 100
- o keine Angabe

F10: Welchen Stellenwert hat IT-Sicherheit in Ihrer Organisation?

- o unwichtig
- o nicht sehr wichtig
- o wichtig
- o sehr wichtig
- o äußerst wichtig
- o keine Angabe

2 Einsatz von Threat Intelligence Sharing Platforms

F11: Setzt Ihre Organisation für den Austausch von Informationen über IT-Bedrohungen eine oder mehrere Threat Intelligence Sharing Platforms ein?

- o Ja → weiter mit Frage 17
- o Nein → weiter mit Frage 12

F12: Planen Sie in den nächsten fünf Jahren den Einsatz einer Threat Intelligence Sharing Platform?

- o Ja, bereits in diesem oder im nächsten Jahr. → weiter mit Frage 13
- o Ja, allerdings erst in 3-5 Jahren. → weiter mit Frage 13
- o Nein → weiter mit Frage 16

F13: Welche Threat Intelligence Sharing Platform(s) planen Sie einzusetzen?

CrowdStrike Falcon X
IBM X-Force Exchange
Malware Information Sharing Platform (MISP)
Open Threat Exchange (OTX)
ThreatConnect
ThreatQ
ThreatStream
andere Threat Intelligence Sharing Platform(s): _____
noch keine (Vor-)Auswahl getroffen
keine Angabe

F14: Welche der folgenden Kriterien sind für die Auswahl einer Threat Intelligence Sharing Platform wichtig?

Funktionsumfang
Umfang der angebotenen Bedrohungsinformationen
Lizenzkosten
Betriebsaufwand
Bekanntheit der Plattform
hohe Verbreitung der Plattform (zum Beispiel unter Partnern)
Benutzerfreundlichkeit (Usability)
weitere Kriterien: _____
keine Angabe

F15: Welche der folgenden Funktionen von Threat Intelligence Sharing Platforms planen Sie zu nutzen?

	Stimme überhaupt nicht zu	Stimme nicht zu	Stimme weder zu noch lehne ich ab	Stimme zu	Stimme voll und ganz zu	keine Angabe
Sammlung von TI	◯	◯	◯	◯	◯	◯
Vorverarbeitung von TI	◯	◯	◯	◯	◯	◯
Analyse von Threat Intelligence	◯	◯	◯	◯	◯	◯
Austausch/Verbreitung von TI	◯	◯	◯	◯	◯	◯
Bewertung und Feedback von TI	◯	◯	◯	◯	◯	◯

Ende der Umfrage.

F16: Was sind Gründe dafür, dass auf den Einsatz einer Threat Intelligence Sharing Platform verzichtet wird?

Mangel an Personal für den Betrieb und die Nutzung der Plattform
mangelnde Finanzierung
zu große Herausforderung im Hinblick auf Datenschutz und Compliance
Interoperabilitätsprobleme
nicht als prioritär betrachtet
bereits eingesetzte IT-Sicherheitssysteme (zum Beispiel Firewall, SIEM etc.) genügen
weitere Gründe: _____
keine Angabe

Ende der Umfrage.

F17: Seit wann nutzt Ihre Organisation Threat Intelligence Sharing Platforms?

- o < 2 Jahre
- o 2 – 4 Jahre
- o > 4 Jahre
- o keine Angabe

F18: Welche Threat Intelligence Sharing Platform(s) setzt Ihre Organisation ein?

CrowdStrike Falcon X
IBM X-Force Exchange
Malware Information Sharing Platform (MISP)
Open Threat Exchange (OTX)
ThreatConnect
ThreatQ
ThreatStream
andere Threat Intelligence Sharing Platform(s): _____
keine Angabe

F19: Welche der Kriterien waren für die Auswahl einer Threat Intelligence Sharing Platform wichtig?

Funktionsumfang
Umfang der angebotenen Bedrohungsinformationen
Lizenzkosten
Betriebsaufwand
Bekanntheit der Plattform
hohe Verbreitung der Plattform (zum Beispiel unter Partnern)
Benutzerfreundlichkeit (Usability)
weitere Kriterien: _____
keine Angabe

F20: Werden Threat Intelligence Sharing Platforms selbst betrieben oder organisationsexterne Plattformen genutzt?

Betrieb einer eigenen (organisationsinternen) Plattform
Nutzung einer organisationsexternen Plattform
Sonstige: _____
keine Angabe

3 Art und Weise der Nutzung von Threat Intelligence Sharing Platforms

F21: Wie häufig werden die folgenden Funktionen von Threat Intelligence Sharing Platforms in Ihrer Organisation genutzt?

	überhaupt nicht	unregelmäßig, anlassbezogen	monatlich	wöchentlich	täglich	keine Angabe
Sammlung von TI	○	○	○	○	○	○
Vorverarbeitung von TI	○	○	○	○	○	○
Analyse von Threat Intelligence	○	○	○	○	○	○
Austausch/Verbreitung von TI	○	○	○	○	○	○
Bewertung und Feedback von TI	○	○	○	○	○	○

Wenn Austausch/Verbreitung von TI ≠ „überhaupt nicht“ → weiter mit Frage 22
Wenn Austausch/Verbreitung von TI = „überhaupt nicht“ → weiter mit Frage 23

F22: Mit wem werden in Ihrer Organisation Bedrohungsinformationen (Threat Intelligence) mit Hilfe von Threat Intelligence Sharing Platforms geteilt?

mit organisationsinternen Stellen → weiter mit Frage 24
mit organisationsexternen Partnern/Stellen → weiter mit Frage 24
keine Angabe → weiter mit Frage 24

F23: Was sind Gründe, warum Ihre Organisation auf das Teilen von Threat Intelligence verzichtet?

mangelnde Qualität der Threat Intelligence
Angst vor Reputationsverlust
zu große Herausforderung im Hinblick auf Datenschutz und Compliance
weitere Gründe: _____
keine Angabe

F24: Sind Threat Intelligence Sharing Platforms in Ihrer Organisation mit anderen IT-Sicherheitssystemen verbunden beziehungsweise mit diesen integriert?

nicht mit diesen verbunden beziehungsweise integriert
Firewall / Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
Security Information and Event Management (SIEM)
Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR)
Vulnerability Management System
mit weiteren IT-Sicherheitssystemen: _____
keine Angabe

F25: Welche Aufgabenbereiche werden in Ihrer Organisation durch Threat Intelligence Sharing Platforms unterstützt?

Incident Management
Risikomanagement
Schwachstellenmanagement
Training des Sicherheitsbewusstseins
Threat Hunting
Betrugserkennung
Malware-Analyse
weitere Aufgabenbereiche: _____
keine Angabe

F26: Wie zufrieden ist Ihre Organisation mit der Nutzung von Threat Intelligence Sharing Platforms?

- o äußerst unzufrieden
- o unzufrieden
- o weder zufrieden noch unzufrieden
- o zufrieden
- o äußerst zufrieden
- o keine Angabe

Vielen Dank für Ihre Antworten!

Falls Sie über die Ergebnisse der Studie direkt benachrichtigt werden möchten, können Sie hier eine E-Mail-Adresse als Kontaktmöglichkeit angeben.