St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Entwicklung einer Methode zur Bewertung von Cyber Threat Intelligence Landscapes

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Murat Aksakalli, BSc
1910619822

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Simon Tjoa

St. Pölten,
08.08.2021

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St. Pölten,
08.08.2021

(Unterschrift Autor/Autorin)

Danksagung

Ich möchte mich an dieser Stelle bei allen Personen bedanken, die mich bei der Erstellung dieser Arbeit mit allen Kräften unterstützt und motiviert haben.

Ich möchte mich besonders bei meinem Betreuer Herrn FH-Prof. Mag. Dr. Simon Tjoa dafür bedanken, dass Sie sich im letzten Jahr immer wieder die Zeit genommen haben, den Fortschritt meiner Arbeit regelmäßig zu begutachten und Verbesserungsvorschläge zu äußern.

Schließlich möchte ich mich bei meiner Familie und Freundin, die die gesamte Zeit hinter mir gestanden und mich unterstützt haben, bedanken.

Zusammenfassung

Neue technologische Innovationen und fortschreitende Digitalisierung kreieren neue und sich ständig verändernde Bedrohungslandschaften. Diese Bedrohungen sind nicht statisch und verändern sich mit schnellem Tempo Jahr für Jahr. Unternehmen und Regierungsstellen versuchen, ihre Cyberlandschaft auf die schnellen Veränderungen und neuen Bedrohungen so gut wie möglich anzupassen. Cyber Threat Intelligence (CTI) Landscapes helfen ihnen dabei, einen Überblick über die aktuellen Trends der Angreifenden zu erhalten. Für die Leserschaft ist ein Bewusstsein über die neuesten Angriffsmethoden oder Werkzeuge essenziell, um die nächsten Schwerpunkte in der Verteidigung ihrer Cyberlandschaft zu setzen. Daher ist es umso wichtiger, dass die Cyber Threat Intelligence Landscapes auf die Lesenden zugeschnitten sind und ihnen bei der Planung einer Cybersicherheits-Strategie helfen.

Das Ziel der vorliegenden Diplomarbeit ist es, eine Methode zu entwickeln, um Cyber Threat Intelligence Landscapes zu bewerten und zu evaluieren. Diese in der Arbeit gewonnenen Erkenntnisse sollen Verfassenden von Cybersicherheits-Strategien die wichtigsten Aspekte von CTI Landscapes darlegen und die wesentlichen Unterschiede der aktuellen Berichte aufzeigen.

Zuerst werden aktuelle CTI Landscapes und die Literatur selektiert und analysiert, um einen Überblick zu erhalten. Dadurch entsteht auch eine Übersicht der verschiedenen Kategorien der Berichte. Danach wird für die Bewertung der Berichte eine Methode zur Analyse entwickelt. Am Ende finden ein Vergleich und eine Evaluation statt. Die Evaluation legt dabei den Fokus auf den Inhalt und Mehrwert für die Leserschaft aus Sicht eines Unternehmens.

Die Bewertungsmethode verwendet die gewählten Kriterien, um eine Bewertung und Einstufung von aktuellen CTI Landscapes durchzuführen. Mithilfe dieser Diplomarbeit kann nachgewiesen werden, dass mit der entwickelnden Methode aktuell nur der Bericht der ENISA alle Kriterien zugunsten einer problemlosen Verwendung in einer Cybersicherheits-Strategie erfüllt.

Abstract

New technological innovations and advancing digitalization are creating new and dynamic threat landscapes. These threats are not static and change at a rapid pace every year. Enterprises and government agencies are trying to adapt their cyber landscape to the rapid changes and new cyber threats as best they can. Cyber Threat Intelligence (CTI) Landscapes help them get an overview of current trends by attackers. For readers, an awareness of the latest attack methods or tools is essential in order to set the next priorities in defending their cyber landscape. Therefore, it is even more important that the Cyber Threat Intelligence Landscapes are tailored to the reader and assist them in developing a cybersecurity strategy.

The goal of this thesis is to develop a methodology to assess and evaluate Cyber Threat Intelligence Landscapes. These findings obtained in the thesis will present cybersecurity strategy authors with the most important aspects of CTI Landscapes and aid them in identifying the key gaps from current reports.

Current CTI Landscapes and literature are selected and reviewed to provide an overview. This will reveal the different categories of the reports. Then, a method of analysis will be developed for evaluating the reports. Finally, a comparison and an evaluation will be made. The evaluation will focus on the content and added value for the reader from a company's point of view.

The evaluation methodology uses the chosen criteria to perform an assessment and ranking of current CTI Landscapes. With the help of this thesis, it can be proven that with the developing method currently only the report of ENISA fulfils all criteria in favour of a proper use in a cybersecurity strategy.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced Persistent Threat
BKA	Bundeskanzleramt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSOC	Bundes Security Operations Centers
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CISA	Infrastructure Security Agency
CISO	Chief Information Security Officer
CTI	Cyber Threat Intelligence
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung
ENISA	The European Network and Information Security Agency
IMF	International Monetary Fund
ICS	Industrial Control Systems
IoC	Indicators of Compromise
IoT	Internet of Things
ISMS	Information Security Management System
KRITIS	Betreiber Kritischer Infrastrukturen
LGPD	Brazilian General Data Protection Law
MELANI	Melde- und Analysestelle Informationssicherung
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OSINT	Open Source Intelligence
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
RaaS	Ransomware-as-a-service
SIEM	Security Information and Event Management
SOC	Security Operations Centre
STIX	Structured Threat Information eXpression
TTP	Tactics, Techniques, and Procedures
VPN	Virtuellen Privaten Netzwerke
WEF	Weltwirtschaftsforum

1. Einleitung

In der modernen Welt der Cybersicherheit versuchen Angreifende und Verteidigende ständig, sich gegenseitig zu übertreffen - sei es durch neue und ausgefallene Techniken von angreifenden Personen oder durch proaktive Vorbereitungen der verteidigenden Partei. Chief Information Security Officers (CISO) spielen eine leitende Rolle bei der Umsetzung proaktiver Maßnahmen in Unternehmen. Sie sind nicht nur für die Einhaltung von Compliance Vorgaben verantwortlich, sondern auch für die Maßnahmen, welche das Unternehmen vor den neuen Techniken der Angreifer schützt.

Bei der Cybersicherheit geht es nicht nur um die verwendeten Technologien, sondern auch um die Geschäftsinformationen. Der Schutz von Unternehmensinformationen stellt eine große Herausforderung dar. Im Zusammenhang mit der Cybersicherheits-Strategie gibt es einige wichtige Diskussionen über den Einsatz und die Anwendung in Unternehmen. [1]

Eine Basis für die strategische Ausrichtung der Maßnahmen sind oft die Cyber Threat Intelligence (CTI) Landscapes. Diese ausführlichen Berichte über die aktuellen Cyber-Bedrohungen können von verschiedenen Organisationen stammen, welche wiederum unterschiedliche Quellen, Fokuspunkte oder Perspektiven nutzen. Diese aufgezählten Faktoren haben bei einer falschen Umsetzung das Potenzial, den Mehrwert der Berichte für die Leserschaft zu senken und CISO bei der Planung der strategischen Ausrichtung zu beeinträchtigen.

Eine Herausforderung ist zum Beispiel die Priorisierung von Bedrohungen. In einer kürzlich veröffentlichten Studie [2] wurde die Priorisierung von Fachpersonen detaillierter untersucht. Dabei wurde festgestellt, dass Sachverständige Schwierigkeiten haben, Empfehlungen zu priorisieren. Beispielsweise finden sie, dass 118 von den untersuchten Empfehlungen zu den "Top 5" gehören, die der Anwendende beachten sollte. Dadurch bleibt es den Endanwendern selbst überlassen, Prioritäten zu setzen. Das macht CTI Landscapes für CISO besonders interessant, da die Priorisierung ein wichtiges Element der Landscapes ist und dieser somit bei der Erstellung einer Cybersicherheits-Strategie für das Unternehmen hilfreich sind.

Ein weiteres wichtiges Element von CTI Landscapes ist die Integrität und Transparenz der Quellen. Des- oder Falschinformationen über Bedrohungen sind in der Lage, sich über den digitalen Raum hinaus negativ auszuwirken – besonders, wenn die Informationen aus ungeprüften Open Source Intelligence (OSINT) Quellen bezogen werden. Caramancion [3] plädiert darauf, dass die Verbreitung von Desinformation als Cyberbedrohung anerkannt werden sollte. Speziell, wenn künstliche Intelligenz dafür verwendet wird, sieht der Autor in der Zukunft eine große Herausforderung, um die Integrität der Daten und Informationen in der Cyberlandschaft des Unternehmens aufrechtzuerhalten.

Cyber-Angriffe beschränken sich heutzutage nicht nur auf das Defacement von Websites, sondern zielen auch auf bestimmte Organisationen oder Branchen ab, um die Infrastruktur zu zerstören, geistiges Eigentum zu stehlen oder die Wirtschaft aus politischen Gründen zu beeinträchtigen. [4, 5] Daher ist es wichtig, den nicht-technischen Aspekt von Cybersicherheit zu verstehen, um die öffentliche und private Infrastruktur zu schützen. Zum Beispiel überschreitet Cyberterrorismus nationale Grenzen, weshalb ein effektives Modell durch eine globale und multidisziplinäre Perspektive benötigt wird. [6]

Dass diese erweiterte Perspektive wichtig für Cybersicherheit ist, war beim 51. Jahrestreffen vom Weltwirtschaftsforum (WEF) 2021 ersichtlich. Die Pandemie hat systemische Veränderungen beschleunigt, die bereits vor ihrem Beginn erkennbar waren. Die sogenannte Davos Agenda von WEF hat das Ziel, globaler Führungspersönlichkeiten zu mobilisieren, um die Prinzipien, Politiken und Partnerschaften zu gestalten. Zusätzlich streicht die Davos Agenda von WEF das Centre for Cybersecurity hevor. [7]

Ein wichtiger Beitrag des WEF und dessen Centre of Cybersecurity ist der Global Risks Report 2021. Dieser rät mit dem Blick auf das kommende Jahr, Cybersicherheit weiterhin als strategisches Geschäftsthema zu betrachten und mehr Partnerschaften zwischen Branchen, Wirtschaftsführern, Regulierungsbehörden und politischen Entscheidungsträgern aufzubauen. Wie jede andere strategische gesellschaftliche Herausforderung kann auch die Cybersicherheit nicht in Silos gelöst werden. [8] Dies zeigt nicht nur die aktuelle Relevanz der neuen Bedrohungslandschaften der Cybersicherheit, sondern

unterstreicht auch, wie essenziell für CTI Landscapes diese Ausblicke und Empfehlungen von internationalen Organisationen sind. Die CTI Landscapes helfen, Trends vorherzusagen und der lesenden Person auf die neue Lage der Bedrohungen aufmerksam zu machen.

Besonders nach einer raschen Digitalisierung ist eine post-pandemische Perspektive wichtig für Unternehmen. Eine 451Research Umfrage [9] gibt an, dass für die meisten Unternehmen Informationssicherheit das wichtigste technologische Ziel aufgrund der Pandemie wurde. Mit dieser raschen Entwicklung müssen auch CTI Landscapes mithalten können.

Die Priorisierung, Integrität sowie Transparenz der Quellen, die erweiterte Perspektive, aktuelle Relevanz und der Ausblick in zukünftige Trends sind sehr nützliche Elemente eines guten CTI Landscapes die CISO helfen, CTI im Unternehmen zu implementieren und eine Cybersicherheits-Strategie zu erstellen. Zusätzlich hilft es dem Unternehmen, Risiken zu kalkulieren und sicher zu stellen, dass das Sicherheitsteam über eine große Anzahl von Cyber-Bedrohungen informiert ist, einschließlich der verwendeten Methoden, Schwachstellen, Ziele und Cyber-Angreifenden in den verschiedenen Branchen.

Daher hat diese Diplomarbeit das Ziel, eine Methode zu entwickeln, um die Elemente eines CTI Landscapes zu analysieren und zu evaluieren. Diese Methode soll danach bei aktuellen Landscapes anzuwenden sein, um einerseits neue Anforderungen für zukünftige Landscapes zu definieren und andererseits herauszufinden, welche Landscapes neue Erkenntnisse oder einen bestimmten Mehrwert für Cybersicherheits-Strategien schaffen.

Dazu werden in der Diplomarbeit folgende Forschungsfragen analysiert und beantwortet:

- Mit welcher Methode kann man CTI Landscapes analysieren und evaluieren?
- Welche Kriterien eines CTI Landscapes haben einen hohen Stellenwert bei der Erstellung einer Cybersicherheits-Strategie?
- Welche Anforderungen kann man mit der Methode aus aktuellen CTI Landscapes gewinnen?

Die Arbeit ist wie folgt strukturiert:

- Kapitel 1: In der Einleitung wird die Relevanz des Themas unterstrichen sowie der Aufbau dieser Arbeit beschrieben. Des Weiteren wird auf den wissenschaftlichen Beitrag eingegangen, den diese Arbeit liefert.
- Kapitel 2: Im zweiten Abschnitt werden die verschiedenen Begrifflichkeiten beschrieben, welche für das Verständnis der weiteren Kapitel benötigt werden. Zusätzlich wird die Auswahlmethode der CTI Landscapes beschrieben.
- Kapitel 3: Um die Forschungsfragen zu beantworten, bildet der dritte Teil der Diplomarbeit eine literarische Analyse, in der der aktuelle Stand der Technik erfasst wird.
- Kapitel 4: Im vierten Kapitel wird die Methode entwickelt, um CTI Landscapes evaluieren und analysieren zu können. Der Schwerpunkt liegt darauf, sich auf bestimmte Faktoren festzulegen, die besonders wichtig für die Erstellung einer Cybersicherheits-Strategie sind.
- Kapitel 5: Im fünften Kapitel liegt der Fokus auf aktuelle CTI Landscapes, die von verschiedenen Regierungsstellen oder Cybersicherheits-Unternehmen veröffentlicht wurden. Dabei wird die Analyse der Landscapes durchgeführt.
- Kapitel 6: Dieser Abschnitt führt mithilfe der Methode von Kapitel 4 eine Evaluation mit den CTI Landscapes aus Kapitel 5 durch. Ein wichtiges Element wird sein, Überschneidungen oder Differenzen ausfindig zu machen.
- Kapitel 7: Im siebten Kapitel wird die Methode und deren Ergebnisse diskutiert und interpretiert. Es wird beschrieben, inwieweit die Methode in der Lage ist, CTI Landscapes zu analysieren und zusätzlich, wo

Grenzen und Probleme des verwendeten Ansatzes liegen. Am Ende werden Anknüpfungspunkte für weiterführende Arbeiten und zukünftige Forschungen erstellt.

- Kapitel 8: Das letzte Kapitel liefert die Zusammenfassung der Arbeit. Es werden die wichtigsten Erkenntnisse und Fakten dargestellt. Am Ende wird eine Handlungsempfehlung beschrieben und konkrete Maßnahmen für CTI Landscapes vorgestellt.

Der Austausch von Bedrohungsdaten in unbearbeiteter Form oder von CTI Landscapes in bearbeiteter Form ist zu einem wichtigen Bestandteil der kooperativen und kollaborativen Cybersicherheit geworden. In den letzten Jahren ist die Zahl der Quellen, die solche Daten veröffentlichen, gewachsen. Sie reicht von Regierungsstellen, welche teilweise durch gesetzliche Änderungen angetrieben worden sind, bis hin zu Privatunternehmen, die Informationen über Schwachstellen anbieten, um Organisationen und Einzelpersonen zu helfen, Risiken besser zu verstehen.

Der wissenschaftliche Beitrag dieser Arbeit liegt in dem Gesamtpaket, das von der Kategorisierung bis zur methodischen Analyse der CTI Landscapes reicht. In dieser Arbeit werden verschiedene Merkmale zur Klassifikation definiert und mit Hilfe einer Methode die Anforderungen für zukünftige CTI Landscapes erkannt.

2. Background

Dieses Kapitel gibt einen Überblick über die wichtigsten Modelle und erklärt relevante Begriffe in Bezug auf Cybersicherheitsmanagement und Schwachstellenmanagement.

Das Internet ist zu einem der wichtigsten Wirtschafts- und Handelsräume für den Staat, die Wirtschaft und die Gesellschaft geworden. Es bringt große Chancen, aber auch Risiken mit sich. Jedoch kann das Internet von staatlichen und nicht staatlichen Akteuren missbraucht werden. Die IT-Systeme sind nicht das Ziel, sie sind lediglich das Mittel zum Zweck. Die Angreifenden nutzen zur Erreichung ihrer Ziele Methoden wie Cybercrime, Cyberspionage oder Cybersabotage, um einen finanziellen, politischen, wirtschaftlichen oder militärischen Vorsprung zu erlangen. Vor diesem Hintergrund wird auch klar, dass die Cybersicherheit hauptsächlich eine Management-Verantwortung darstellt. [10]

ISMS

Die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen Geschäftsprozesse sind Grundlage für einen reibungslosen und sicheren Geschäftsbetrieb und erfordern unmittelbar, dass alle Informationssysteme vor dem Zugriff durch Dritte geschützt werden. Für Unternehmen und Regierungen gleichermaßen ist es unerlässlich, dass ihre Prozesse und Systeme unter allen relevanten Umständen abgeschirmt werden. Das gesamte Unternehmen und seine Liefer- und Logistikketten müssen berücksichtigt werden, da ein Cyberangriff auf eine kleinere, jedoch wichtige Lieferfirma große Auswirkungen auf das gesamte Unternehmen haben und zu unvorhergesehenen Effekten führen kann. [10]

Mit einem Information Security Management System (ISMS) wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen jeder Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein. [11]

Der Prozess, die beste Entscheidung zu treffen, hängt stark von den Qualitätsindikatoren der Organisation ab. Eine der Anforderungen der CISO ist es, eine bessere Sicherheitseinrichtung der Organisationsstrategie mit Hilfe eines Sicherheitsmanagements zu spezifizieren. Die besonderen Merkmale von Cybersicherheit erlauben es nicht, eine statische und vordefinierte Methode zur Bewertung des Sicherheitsstatus der Organisation zu verwenden. Die quantitative Darstellung der Cybersicherheit in einer Organisation ist mit vielen variablen Parametern verbunden, die als Input eines Frameworks empfangen und verarbeitet werden müssen. [12] Einen Einfluss auf diese Parameter haben Informationen aus CTI Landscapes.

Das Österreichische Informationssicherheitshandbuch [13] beschreibt das ISMS-Prozessmodell auf Basis des PDCA-Life-Cycle-Modells. Dieses Modell besteht aus vier Hauptbestandteilen: Plan, Do, Check und Act. Im ersten Teil des Zyklus werden relevante Sicherheitsziele und -strategien ermittelt und eine Informationssicherheits-Policy mit spezifisch geeigneten Sicherheitsmaßnahmen erstellt. Im zweiten Teil wird der Betrieb und die Umsetzung des ISMS definiert. Im dritten Teil wird die Wirksamkeit des ISMS und der definierten Sicherheitsmaßnahmen überwacht und überprüft. Im letzten Teil wird die Instandhaltung und laufende Verbesserung des ISMS durch erkannte Fehler, Schwachstellen und veränderte Umfeldbedingungen definiert. Threat Intelligence hat dabei im letzten Teil des Zyklus einen großen Einfluss. [14]

Für den Aufbau eines ISMS wird der PDCA-Zyklus (Plan - Do - Check - Act) verwendet. Das auf ISMS-Prozesse angewandte PDCA-Zyklus wird folgendermaßen erläutert [15]:

- Plan: In dieser Phase findet die Planung und Gestaltung des ISMS statt.
- Do: In dieser Phase findet die Implementierung und der Betrieb der Policy, Kontrollen, Prozesse und Strategie des ISMS statt.
- Check: In dieser Phase findet die Überwachung von der Umsetzung des ISMS statt, inklusiver Bewertungen und Prüfungen.
- Act: In der letzten Phase ist die Verbesserung, Entwicklung und Instandhaltung vom ISMS.

Cyber Threat Intelligence

Als Threat Intelligence ist evidenzbasiertes Wissen, einschließlich Kontext, Mechanismen, Indikatoren, Implikationen und umsetzbarer Ratschläge, über eine Bedrohung zu sammeln. Diese Informationen werden als Entscheidungsgrundlage für eine passende Reaktion auf Bedrohungen oder Gefahren verwendet. Bedrohungsinformationen, die von Sicherheitsteams gemeldet und ausgetauscht werden, sind überwältigend und erschweren die Aufnahme und Korrelation mit bereits vorhandenem Wissen. Daher gehen Anbieter von Bedrohungsdaten zunehmend dazu über, diesen Prozess zu automatisieren, um die Bedrohungsanalyse zu einer praktikablen Aufgabe zu machen. [16]

STIX (Structured Threat Information eXpression) ist eine standardisierte Sprache, die von MITRE in gemeinschaftlicher Arbeit entwickelt wurde, um strukturierte Informationen über Cyber-Bedrohungen darzustellen. Sie wurde so entwickelt, dass sie gemeinsam genutzt, gespeichert und anderweitig in einer konsistenten Weise verwendet werden kann, die die Automatisierung und die von Menschen unterstützte Analyse erleichtert. [17]

STIX ermöglichen den Transport von Bedrohungsinformationen zwischen IT-Sicherheits- und Intelligence-Technologien. Mithilfe von STIX ist ein Unternehmen in der Lage die IT-Sicherheitsbemühungen neu auszurichten und eine Basis von Echtzeit-Informationsaustausch zwischen Regierung, kommerziellen Anbietern, gemeinnützigen Organisationen und Industriepartnern aufzubauen. Was für die eine Organisation reaktiv ist, ist für die andere proaktiv. [17]

STIX 2.1 Objekte kategorisieren jede Information mit spezifischen Attributen, die ausgefüllt werden müssen. Die Verkettung mehrerer Objekte durch Beziehungen ermöglicht einfache oder komplexe Darstellungen von CTI. [17]

Domain Objects		
Object	**Name**	**Description**
	Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways Threat Agents attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
	Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence.

	Grouping	Explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle.
	Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Infrastructure	Represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.).
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
	Location	Represents a geographic location.
	Malware	A type of TTP that represents malicious code.
	Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
	Note	Conveys informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
	Observed Data	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
	Opinion	An assessment of the correctness of the information in a STIX Object produced by a different entity.
	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
	Threat Actor	Actual individuals, groups, or organizations believed to be operating with malicious intent.
	Tool	Legitimate software that can be used by Threat Agents to perform attacks.

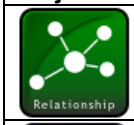
	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Relationship Objects		
Object	**Name**	**Description**
	Relationship	Used to link together two SDOs or SCOs in order to describe how they are related to each other.
	Sighting	Denotes the belief that something in CTI (e.g., an indicator, malware, tool, threat actor, etc.) was seen.

Tabelle 1 - Beschreibung STIX 2.1 [17]

Beschreibung der Tabelle: Die erste Spalte zeigt eine Grafik des Objects, um es später in der Visualisierung zu nutzen. Die zweite und dritte Spalte benennen und beschreiben die Domain Objects beziehungsweise Relation Objects.

Um einen Fall mit STIX zu visualisieren, werden die angebotenen Attribute genutzt. Zum Beispiel können die Objects Vulnerability, Campaign, Threat Actor und Indicator verwendet werden, um die Beziehung zwischen Threat Agents und Schwachstellen darzustellen. In der folgenden Abbildung wird dieses Beispiel mit STIX 2 Objects und Pfeilobjekten dargestellt. [17]

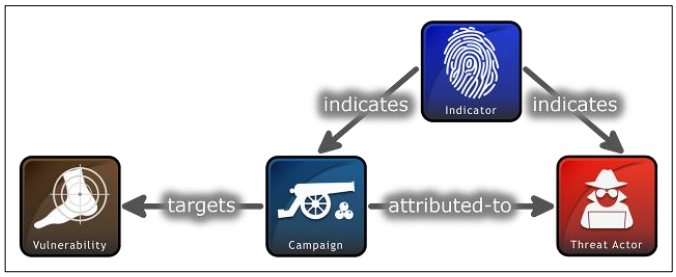


Abbildung 1 - STIX 2 Relationship Beispiel [17]

OpenIOC ist eine weitere Methode, die ein Standardformat und Begriffe für die Beschreibung der Objekte bietet. Der häufigste Anwendungsfall ist das Aufspüren von bekannter Malware, entweder durch die Suche nach Attributen der Binärdatei selbst. Mithilfe von OpenIOC kann ein Unternehmen Informationen von böswilligen Aktivitäten wie Metadaten im Zusammenhang mit der Installation von Hintertüren, der Ausführung von Tools oder der Bereitstellung von Dateien für den Diebstahl verfolgen. [18]

Eine IOC besteht aus drei Hauptbestandteilen: Die Definition, IOC-Metadaten und Referenzen. IOC-Metadaten beschreiben Informationen wie den Autor des IOC (jsmith@domain.tld), den Namen des IOC (Evil.exe (BACKDOOR)) und eine kurze Beschreibung wie "Diese Variante der Open-Source-Backdoor Poison Ivy wurde so konfiguriert, dass sie ein Beacon an 10.127.10.128 sendet und sich als "Microsoft 1atent time services" registriert. Innerhalb des IOC sind Informationen wie der Name einer Untersuchung oder Fallnummer zu finden. Ein häufiger Verwendungszweck für Referenzen ist die Zuordnung einer IOC zu einer bestimmten Bedrohungsgruppe. Innerhalb der Definition werden die Indikatoren aufgelistet oder zu Ausdrücken kombiniert, die aus zwei Begriffen und einer Form von boolescher Logik bestehen. Ein Beispiel für die Definition von OpenIOC ist die folgende Abbildung: [18]

```
OR
    Service Name contains "MS latent time services"
    Service DLL contains "evil.exe"
    AND
        File Name is "bad.exe"
        File Size is "4096 TO 10240"
```

Abbildung 2 – OpenIOC Definition Beispiel [18]

Der traditionelle Ansatz zur Risikobehandlung von Security Schwachstellen ist ein risikobasierter Ansatz. Die drei Grundsätze des traditionellen Ansatzes sind Erkennung, Reaktion und Schutz. Dabei liegt der Fokus auf der Schwachstelle des Risikos. Die Erkennung dient dazu, herauszufinden, ob jemand versucht, die Schutzmechanismen zu überwinden. Danach kommt die Reaktion, um schnelle Schadensbegrenzung durchzuführen, Ausfallzeiten zu minimieren und Systeme oder Daten wiederherzustellen.

Der letzte Grundsatz ist der Schutz, um Systeme oder Daten mit geeigneten Kontrollen abzusichern. Dabei haben Threat Agents wenig oder keine Gewichtung und in der Praxis liegt der Fokus zu wenig auf den Schutz. Der Data Breach Report [19] von IBM zeigt auf, dass der Lifecycle eines Data Breachs im Jahr 2019 durchschnittlich 279 Tage gedauert hat.

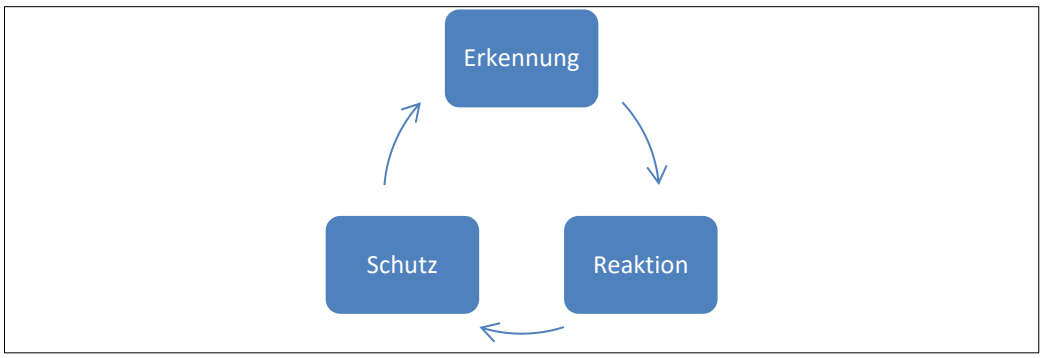


Abbildung 3 - Traditionelle Ansatz zur Risikobehandlung von Security Schwachstellen

Das Ziel von CTI ist es nun, den Grundsätzen ein proaktives Element hinzuzufügen, um vorbeugende Maßnahmen gegen potenzielle Angreifer zu ergreifen und Methoden zu identifizieren. Die CTI-gesteuerte Erkennung von Bedrohungen ist von Natur aus proaktiver, vorausschauender und dynamischer als traditionelle Risikomanagement-Aktivitäten, die tendenziell statisch, starr und eher reaktiv sind, obwohl die zwei Ausrichtungen komplementär sind. [20]

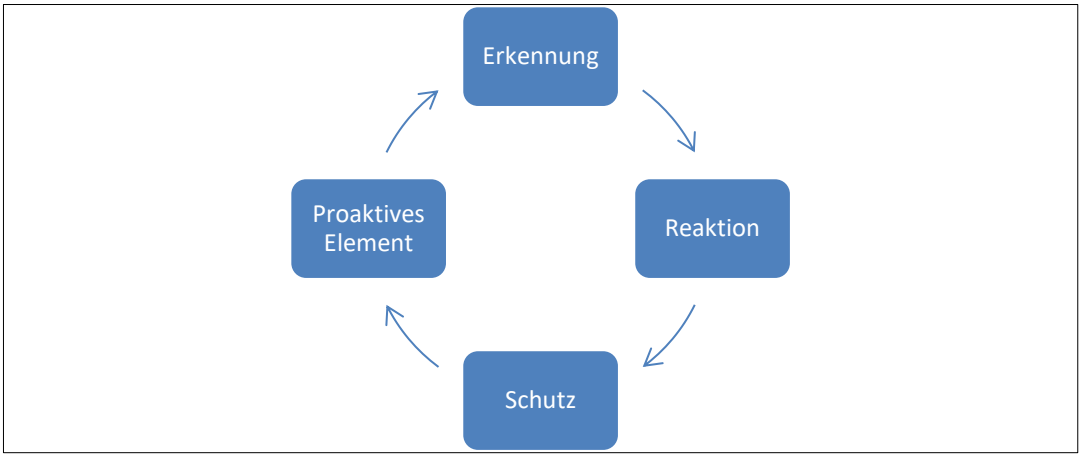


Abbildung 4 - Risikobehandlung von Security Schwachstellen mit einem proaktiven Element

Zur Identifikation von Bedrohungen werden Daten aus unterschiedlichen Quellen aufgearbeitet und anschließend der Kontext zu Indicators of Compromise (IoCs) und Tactics, Techniques, and Procedures (TTPs) von Threat Agents hergestellt. IoCs werden als forensische Fragmente ausgetauscht, um Sicherheitsexperten zu helfen, Cyber-Bedrohungen schnell zu identifizieren und darauf zu reagieren. [21]

Tactical Threat Intelligence zeigen auf, wie das Unternehmen angegriffen werden könnte. Sie helfen dabei, bestehende Sicherheitsprozesse zu verbessern und die Reaktion auf Vorfälle zu beschleunigen. Dabei ist die Motivation der Angreifenden und die Schwachstellen, welche die Angreifenden ins Visier nehmen, essenziell. Obwohl Tactical Threat Intelligence die einfachste Art von Threat Intelligence ist und von Unternehmen meist automatisiert wird, haben die IoCs eine kurze Lebensdauer. Dies kann bei der Analyse zu false-positive Ergebnissen führen, weshalb es sich nicht um einen langfristigen Sicherheitsplan für ein Unternehmen handelt. Die Berichte, die von Tactical Threat Intelligence erstellt werden, haben eine technisch-orientierte Zielgruppe. [22]

Operational Threat Intelligence liefert Informationen über die angreifende Partei. Mit Operational Threat Intelligence können Unternehmen vorhersagen, wer der Attackierende ist, welche Motivation dieser hat und wie er seinen Angriff plant, einschließlich seiner TTPs. Operational Threat Intelligence überschneidet sich in vielen Bereichen mit Tactical Threat Intelligence, jedoch ist dieses stärker automatisiert, während für eine effektive Operational Threat Intelligence eine menschliche Analyse erforderlich ist. Operational Threat Intelligence wird vor allem in Cybersecurity-Disziplinen wie dem Schwachstellenmanagement, der Abwehr von Zwischenfällen und der Überwachung von Bedrohungen eingesetzt. [22]

Strategic Threat Intelligence bietet einen breiten Überblick über die Bedrohungslandschaft, zum Beispiel mithilfe eines CTI Landscapes. Sie ist als Entscheidungsgrundlage für Führungskräfte und andere Entscheidungsträger in einem Unternehmen gedacht - daher ist der Inhalt in der Regel weniger technisch und wird in Form von Berichten oder Briefings präsentiert. [22] Gute strategische Informationen sollten Einblicke in Bereiche wie die mit bestimmten Vorgehensweisen verbundenen Risiken, allgemeine Muster in den Taktiken und Zielen von Bedrohungsakteuren sowie geopolitische Ereignisse und Trends bieten. Häufige Quellen für Strategic Threat Intelligence sind Regierungsstellen oder Cybersicherheits-

Unternehmen. Obwohl Strategic Threat Intelligence nicht technisch ist, erfordert die Erarbeitung eine gründliche Recherche in riesigen Datenmengen.

In [23] werden einige der Hauptunterschiede zwischen strategischen und taktischen Cyber-Bedrohungsinformationen mithilfe einer Tabelle dargestellt.

	Tactic CTI	**Strategic CTI**
Info. Source	Honey pots, incident reports, logs	Analysis based on substantial amount of tactic info.
Shared Attack Source	IP address, domains	Hosting networks, botnets
Action	Firewall blocking	Eliminate botnets, improve hosting policy

Tabelle 2 - Tactic vs. Strategic Threat Information [23]

Schwachstellen

Threat Intelligence hilft, die Schwachstellen zu identifizieren, die ein tatsächliches Risiko für das Unternehmen darstellen. Diese Feststellung ist dabei mehr als eine Punkteskala, welche den Schweregrad der Schwachstelle beschreibt, sondern kombiniert interne Schwachstellen-Scandaten, externe Daten und den Kontext über die TTPs von Threat Agents. [22]

Eine Sicherheitslücke entsteht durch die potenzielle Ausnutzung von Software, zum Beispiel durch unberechtigten Zugriff. Dieses böswillige Verhalten oder der betrügerische Zugriff kann sich als Einschleusen von Viren, Trojanern, Malware usw. in den ursprünglichen Code äußern. In seinem Buch [24] definiert der Autor Pfleeger eine Schwachstelle als einen Fehler, der einer Anwendung innewohnt und von einem Angreifer missbraucht werden kann.

Das STIX 2 Object [17] „Schwachstelle“ wird hauptsächlich verwendet, um auf externe Definitionen von Schwachstellen zu verweisen oder um 0-Day-Schwachstellen zu beschreiben, für die es noch keine Definition gibt. Zusätzlich stellt es dar, wie es als Teil einer böswilligen Cyber-Aktivität anvisiert und ausgenutzt werden kann.

Threat Agents

Die häufigsten Angreifer im Zusammenhang mit Cyberangriffen sind als Script Kiddies, Hacktivisten, Insider-Bedrohungen, organisierte Kriminalität und Advanced Persistent Threats bekannt. [25] Die Analyse der Threat Agents hilft den Verteidigenden oft, nach bestimmten Spuren zu suchen und zu versuchen, die nächste gegnerische Aktion zu antizipieren.

Laut STIX [17] sind Threat Agents tatsächliche Personen, Gruppen oder Organisationen, von denen angenommen wird, dass sie mit böswilligen Absichten operieren. Ein Threat-Actor ist klar vom STIX 2 Object „Intrusion Set“ zu unterscheiden, jedoch sind Intrusion Sets im Laufe der Zeit in der Lage, Gruppen oder Organisationen zu unterstützen oder mit ihnen verbunden zu sein. Threat Agents können durch ihre Motive, Fähigkeiten, Ziele, ihren Entwicklungsstand, frühere Aktivitäten, Ressourcen und ihre Rolle in der Organisation charakterisiert werden. [17]

Laut der Definition von National Institute of Standards and Technology (NIST) ist ein Threat Actor eine Einzelperson oder eine Gruppe, die eine Bedrohung darstellt. [26] OSINT und Social Engineering sind typische Methoden von Threat Agents, um sich Informationen über Schwachstellen zu beschaffen.

OSINT

OSINT ist ein Verfahren, das durch die Verarbeitung von Informationen, wie z. B. der Analyse und Auswertung, aussagekräftige Informationen sammelt. Es wurde in einer Vielzahl von Bereichen eingesetzt, darunter in den Gebieten Mensch, Wirtschaft, Gesellschaft, Verkehr, Kommunikation, Militär, Politik, Wissenschaft und Technologie. [27] Während des OSINT-Verfahrens werden hauptsächlich öffentliche Informationen verwendet. Zu diesen Quellen gehören traditionelle Medien wie Zeitungen und Zeitschriften sowie digitale Medien wie das Internet und Datenbanken. [28]

MITRE ATT&CK

MITRE ATT&CK ist eine weltweit zugängliche Wissensbasis über Taktiken und Techniken von Angreifenden, die auf realen Beobachtungen basieren. Die ATT&CK-Wissensbasis wird als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden im privaten Sektor, in der Regierung und in der Gemeinschaft der Cybersicherheitsprodukte und -dienste verwendet. Die Informationen von MITRE ATT&CK können auch verwendet werden, um das Verhalten der Threat Agents zu kategorisieren. [29]

MITRE unterteilt ihr Framework in drei verschiedene Matrizen: Enterprise, Mobile und Industrial Control Systems (ICS). Im Kern dokumentiert das ATT&CK Framework bekanntes feindliches Verhalten und ist nicht dazu gedacht, eine Checkliste von Punkten zu erstellen. Die Grundlage der ATT&CK Matrizen ist die Sammlung von Techniken und Untertechniken, die Aktionen von Angreifenden darstellen. Weiters kann die Beziehung zwischen Taktiken, Techniken und Untertechniken in der ATT&CK-Matrix veranschaulicht werden. Zum Beispiel gibt es unter der Taktik "Persistenz" eine Reihe von Techniken wie "Hijack Execution Flow", "Pre-OS Boot" und "Scheduled Task/Job". Jede von ihnen ist eine einzelne Technik, die Angreifende verwenden können, um „Persistenz“ zu erreichen. Die folgende Abbildung stellt die ATT&CK Enterprise Matrix als Grafik da. [30]

Abbildung 5 - Vollständige Darstellung der ATT&CK Enterprise Matrix [30]

ATT&CK organisiert mithilfe der Matrix kurz und bündig die Taktiken und Techniken des Gegners und bietet eine einheitliche Formulierung, die in allen Sicherheitsdisziplinen verwendet wird. Diese Eigenschaften machen es zu einem nützlichen Konzept für diejenigen, die sich gegen Attackierende verteidigen müssen, indem sie deren Verhalten besser verstehen. Obwohl der Fokus von ATT&CK darauf liegt, wie Angreifende Computernetzwerke kompromittieren und darin operieren, kann die Methode auch auf andere Bereiche angewendet werden. [30]

Zusammenfassend lässt sich sagen, dass die simpelste Nutzung von ATT&CK die Identifizierung einiger Verhaltensweisen von bestimmten Angreifenden ist, um die Verteidigenden des Unternehmensnetzwerkes darüber zu informieren. Die Verteidigung erfährt durch die Bedrohungsanalyse, wie die Angreifenden zu erkennen sind. Zusätzlich bietet ATT&CK eine Reihe von Informationen, die für die Analyse des gesamten Lebenszyklus eines Cyberangriffs nützlich sind, einschließlich des Aufspürens eines Angriffsziels, der Angriffsvektoren, des tatsächlichen Eindringens und dem Verhalten nach einem Angriff. [30]

Risikomanagement

Wenn Unternehmen online arbeiten, sind sie einem Risiko ausgesetzt. Cyber-Bedrohungen können jederzeit zuschlagen und sich auf Organisationen jeder Größe auswirken. Obwohl die Anschaffungskosten für fortschrittliche Cybersicherheit überwältigend erscheinen können, sind die Auswirkungen eines Cyberangriffs weitaus gravierender. Es droht nicht nur ein finanzieller Schaden durch den Ausfall von Diensten oder Abhilfemaßnahmen, sondern auch ein Reputationsschaden. [31]

Risiko kann als eine Funktion von drei Faktoren gesehen werden: Bedrohung, Schwachstellen und Konsequenz. Eine Risikobewertung ist ein Prozess, der versucht, Risiken zu identifizieren, zu analysieren

und zu verstehen. Im Idealfall beinhaltet eine Risikobewertung die Beurteilung von Bedrohungen, Schwachstellen und Folgen, die nachstehend erörtert werden. [31]

Entscheidungen über Risikoziele sind Geschäftsentscheidungen und werden daher auf der höchsten Ebene des Versorgungsunternehmens getroffen, wie zum Beispiel durch den Vorstand oder die Geschäftsführung. Das Risikomanagement der Cybersicherheit berührt jeden Aspekt einer Organisation und ist abhängig von Richtlinien und Verfahren. Die organisatorische Sicherheitsrichtlinie fasst den Ansatz des Unternehmens für das Risikomanagement zusammen. Dazu gehören klar identifizierte Rollen und Verantwortlichkeiten, die eine Sicherung für Risiken in der gesamten Organisation schaffen. [32]

Das Risikomanagement muss die sich verändernde Bedrohungslandschaft berücksichtigen, wie sie von der CTI beschrieben wird. Die meisten Unternehmen sind für diese Informationen auf externe Quellen angewiesen, die Details über neue Bedrohungen, Schwachstellen und Cyberangriffstools enthalten. [32]

In einer Partnerschaft zwischen der US-Agentur für internationale Entwicklung und dem National Renewable Energy Laboratory sowie der Resilient Energy Platform wurden Cybersecurity Bausteine definiert und eine Grafik erstellt, um für den Stromsektor den Zusammenhang zwischen CTI und Risikomanagement visuell darzustellen. Viele Unternehmen haben Schwierigkeiten damit, ein Cybersicherheitsprogramm zu erstellen, das zum Schutz ihrer Anlagen vor Angriffen erforderlich ist. Für diese Organisationen wurde der Baustein-Ansatz erschaffen. In der folgenden Abbildung stellt die Grafik die Bausteine im Zusammenhang miteinander dar. [32]

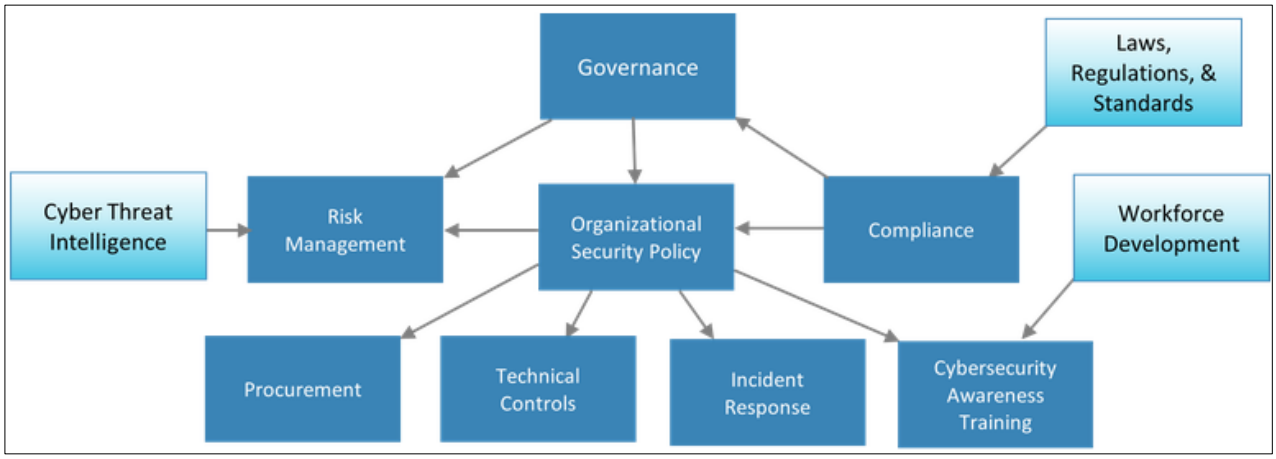


Abbildung 6 - Cybersecurity Building Blocks im Stromsektor [32]

Ziel der Einführung eines IT-Risikomanagements ist, ein angemessener Schutz für alle Informationen zu erreichen. Dabei muss der ganzheitliche Ansatz des IT-Grundschutzes wie zum Beispiel organisatorische, personelle, infrastrukturelle und technische Sicherheitsmaßnahmen und Standards umgesetzt werden. Ein ISMS bringt die Möglichkeiten die IT-Sicherheit zu erhöhen und eine Basis für die strategische Ausrichtung der Maßnahmen zu schaffen. Hilfreich dabei sind die Berichte von aktuellen CTI Landscapes die einen Überblick über die Bedrohungslandschaft bieten. Welche Bedeutung und Herausforderungen CTI Landscapes haben, wird im nächsten Kapitel analysiert.

3. Literaturübersicht

Das Ziel dieser Literaturrecherche ist es, verwandte Arbeiten sowie die Bedeutung und Probleme von CTI Landscapes, etwas näher zu betrachten beziehungsweise darauf aufmerksam zu machen, dass die Probleme bereits in der Literatur erkannt wurden. Außerdem soll die Literaturrecherche weiterführende Informationen rund um das Thema Cyber Threats und CTI Landscapes bieten.

In diesem Kapitel wird auch beschrieben mit welcher Methode die CTI Landscapes ausgewählt worden sind. Mithilfe eines Flussdiagramms werden die verschiedenen Phasen einer systematischen Überprüfung dargestellt. Zusätzlich werden die identifizierten, eingeschlossenen und ausgeschlossenen Gründe für die Ausschlüsse dargestellt.

3.1. Auswahl der CTI Landscapes

Die Suchstrategie der CTI Landscapes besteht aus Inclusion und Exclusion Kritierien. Da keine Datenbank mit CTI Landscapes existiert, wird mithilfe von Google gesucht. Die verschiedenen Phasen der systematischen Suche werden mithilfe eines Flussdiagramms dargestellt. Die Analyse der CTI Landscapes findet in Kapitel 5 statt.

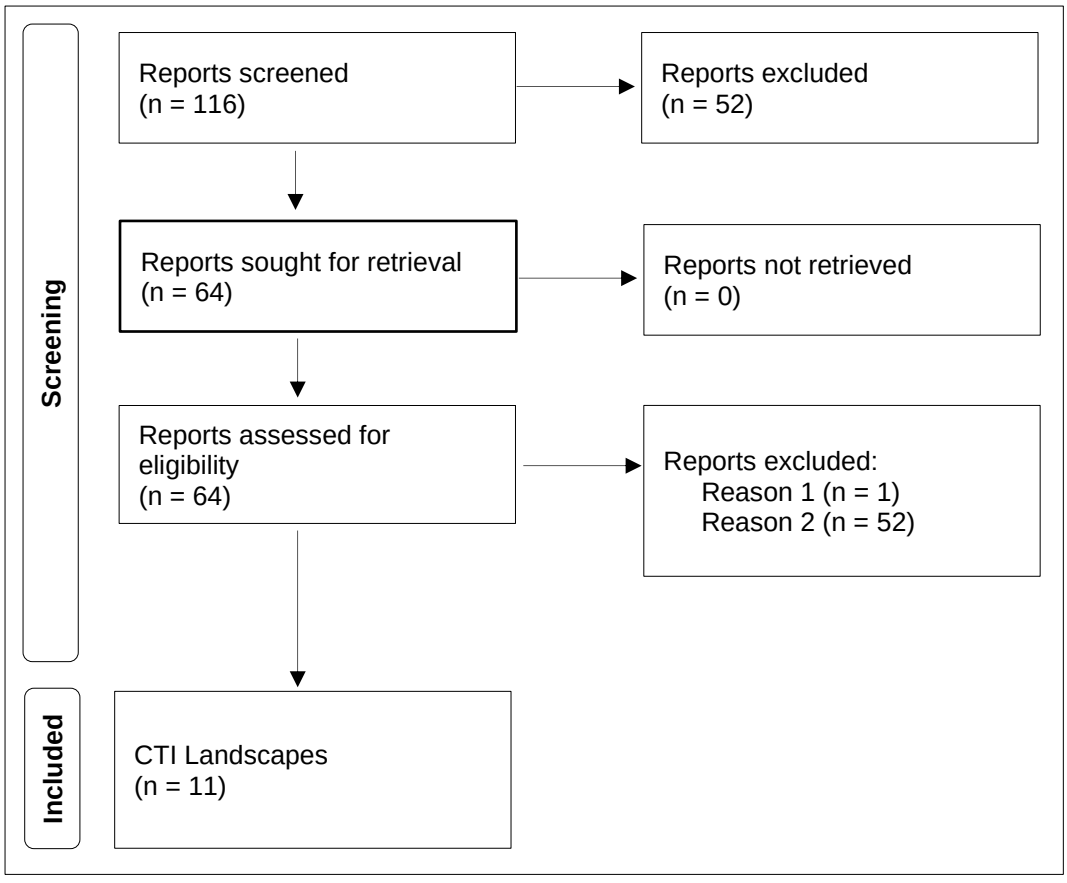


Abbildung 7 - CTI Landscapes Flussdiagramm

Beschreibung des Diagramms:

Das Flussdiagramm stellt die verschiedenen Phasen einer systematischen Überprüfung dar. Auf der ersten Ebene werden die Reports identifiziert und auf Standardkriterien gefiltert. Die Reports werden im Anhang 1 aufgelistet. Auf der zweiten Ebene werden die Reports gelistet, die nicht erfasst werden konnten. Auf der dritten Ebene sind Reports zu finden, die aus bestimmten Gründen nicht inkludiert werden.

Kriterien

Da regelmäßig CTI Landscapes veröffentlicht werden [33, 34, 35, 36], wurde Anfang 2021 mithilfe bestimmter Kriterien eine Auswahl an bestimmten CTI Landscapes getroffen. Als CTI Landscape gelten Studien oder Erhebungen von Bedrohungslandschaften im Cyber-Sektor. Mithilfe von Google wurde mit Suchbegriffen, wie „CTI Landscape“, „Threat Report“ und „Cybersecurity Survey“ die erste Auswahl getroffen.

Um unspezifische und kleine CTI Landscapes im Vorhinein auszuschließen, wurde eine Mindestanzahl von 20 Seiten gesetzt. Ausgenommen davon sind kleinere Berichte, die aufgrund ihrer Zielgruppe vereinfacht worden sind - zum Beispiel falls zu einem CTI Landscape zusätzlich ein Executive Summary veröffentlicht wurde. Hinzukommend werden CTI Landscapes aus Mitteleuropa in englischer oder deutscher Sprache bevorzugt, zum Beispiel falls Cybersicherheits-Unternehmen mehrere CTI Landscapes in mehreren Ländern anbieten.

Gründe

Der erste Grund für die Exklusion von einem CTI Landscape ist, der überwältigende Fokus auf Gesetze und Regierungsinitiativen. Eine Empfehlung oder Handlungsempfehlung ist schwer möglich, wenn nur die regulativen Aspekte analysiert werden.

Ein weiterer großer Grund für die Ausscheidung von CTI Landscapes sind Berichte die nur auf bestimmte Branchen, Trends oder Vorfälle spezialisiert sind. Der Vergleich von sehr allgemeinen und sehr spezifischen Berichten ist sehr schwierig und selten sinnvoll - besonders wenn sich der Bericht nur auf bestimmte Trends, wie zum Beispiel KI oder Cloud Technologien, fokussiert.

Im Anhang 1 sind alle exkludierten Berichte aufgelistet.

Kategorien

In dieser Arbeit werden die ausgewählten CTI Landscapes in zwei verschiedene Kategorien aufgeteilt – Regierungsstellen und Cybersicherheits-Unternehmen. Regierungsstellen sind dabei Bericht, die von öffentlich finanzierten Stellen stammen, während Cybersicherheits-Unternehmen Berichte aus der Privatwirtschaft beinhaltet. Diese Kategorien wurden erstellt, um stark unterschiedlichen Ziele im Vorhinein vorzubeugen.

3.2. Untersuchung von Cyber Threat Intelligence Landscapes

In [37] untersuchten die Forschenden 11 CTI und 14 Malware Analyseportale auf ihre Inhalte. Der Fokus der Arbeit lag auf der Frage, ob die Analyseportale Informationen von Online Hacker Foren verwenden. Obwohl viele bestehende CTI- und Malware-Portale darauf abzielen, Cyber-Bedrohungen einzudämmen, stützen sie sich häufig auf aktuelle Angriffsdaten und werden als zu reaktiv kritisiert. Im Bericht [38] von SANS gaben nur 20% der von SANS befragten Unternehmen an, dass sie die Integration herstellerbasierter Dark Web Intelligence in ihre CTI-Plattform in Betracht gezogen haben. In der Arbeit [39] möchten die Forschenden mithilfe von Machine Learning einen Überblick über die Hackerforen gewinnen und die Informationen aus den Foren verarbeiten. Die Herausforderung, die sich stellt, lautet, auf manuelle Analysen zu verzichten und keine nutzlosen oder redundanten Informationen zu verarbeiten. [39]

Im aktuellen Bericht [40] von SANS verwenden 38,90% der befragten Unternehmen verschlossene oder Dark Web Informationen. Der Bericht enthält weitere aktuelle Informationen über den Stand von CTI. Weiteres berichtet das Dokument über die steigende Automatisierung in dem Bereich und die wachsende Anzahl der kleinen Organisationen die CTI verwenden. Zusätzlich erkennt SANS, dass im Jahr 2020 die

CTI-Analysten mehr Informationen aus staatlichen Sicherheits- und Medienberichten in ihre Analysen einbezogen haben.

SANS berichtet, dass die CTI Community weitergewachsen und gereift ist. Eine Rekordzahl von Organisationen gab an, dass die Methoden und Prozesse zur Messung der Wirksamkeit von CTI-Systemen eingeführt wurden. Diese Verbesserungen zeigen weiterhin die Widerstandsfähigkeit des Bereichs und den Wert der CTI als Ressource für Klarheit und Priorisierung bei komplexen Herausforderungen. [40]

3.3. Bedeutung von Cyber Threat Intelligence Landscapes

Die Fähigkeit von Angreifern, Informations- und Kommunikationssysteme zu untergraben, zu stören und zu deaktivieren, ist eine Bedrohung für viele Branchen weltweit und erfordert zusätzliche Aufmerksamkeit. Für Cyber Threats gibt es viele Definitionen. Als technische Definition ist das Cyber Threat eine mögliche Angriffsfläche, die eine Schwachstelle schafft. Diese Bedrohung kann dann ausgenutzt werden, um Sicherheitssysteme zu umgehen und somit Schaden zu verursachen. [41]

Die Zunahme von Angriffen und steigenden Verlusten haben das Cyber-Risiko von einer Angelegenheit der IT-Abteilungen zu einem zentralen Risikomanagement-Thema für alle Institute weltweit und zu einem Risiko für die systemweite Stabilität von Unternehmen oder Regierungsstellen gemacht.

In [42] analysieren Accenture und das Ponemon Institute die Kosten von Internetkriminalität. Die Studie kombiniert Untersuchungen aus 11 Ländern und 16 Branchen. Dafür wurden 2647 Führungskräfte aus 355 Unternehmen befragt und auf die Erfahrung und Expertise der Accenture-Sicherheitsexperten zurückgegriffen, um die wirtschaftlichen Auswirkungen von Cyberattacken zu untersuchen. Die Studie gibt an, dass der Einfluss von Cyber Threat mit neuen Techniken [43] [44] oder Technologien [45] auf Organisationen, Branchen und Gesellschaft erheblich sind. Neben der wachsenden Zahl von Sicherheitsverletzungen stiegen für jedes Unternehmen im Jahr 2017 die Gesamtkosten der Cyberkriminalität von 11,7 Millionen US-Dollar auf einen neuen Höchststand von 13,0 Millionen US-Dollar - ein Anstieg von 12 Prozent.

Angreifer haben eine universelle Reichweite. Ihre Ziele sind große und kleine Institutionen, reiche und weniger wohlhabende Länder gleichermaßen. Die COVID-19-Krise hat das Bewusstsein dafür geschärft, wie wichtig der Schutz digitaler Systeme und der Konnektivität ist, um die Kontinuität der wirtschaftlichen und finanziellen Aktivitäten zu gewährleisten. Dass der finanzielle Sektor Cyber Threat als größeres Risiko anerkennt, ist im Diskussionsbericht vom International Monetary Fund (IMF) [46] ersichtlich.

Der Diskussionsbericht [46] zitiert dabei ein speziell auf die Banken und Finanzsektor spezifisches CTI Landscape von Insights [47], welcher angibt, dass Banken und Finanzdienstleister im vergangenen Jahr das Ziel von 25,7 Prozent aller Malware-Angriffe waren. Die Prozentzahl übersteigt jedes Ergebnis der anderen 27 vom CTI Landscape untersuchten Branchen. Dadurch wird verdeutlicht welche Bedeutung branchenspezifische CTI Landscapes in ihrem Umfeld haben und dass diese maßgeblich für weitere Diskussionen sind.

Zusätzlich geht der Bericht [46] auf Cyber Threats ein, die immer raffinierter werden und sich in der Regel über mehrere Länder strecken, was die Untersuchung und Verfolgung erschwert. Cyberangriffe sind industrialisiert worden und viele Vorgänge sind international aufgeteilt. Es gibt Märkte für Hacking-Dienste, Börsen für Schwachstellen, spezialisierte Betreiber und Outsourcing-Dienstleister. Angreifer zeigen dabei ein hohes Maß an Flexibilität. [48]

Angreifer haben einen breiten Zugang zu Technologie, die es ihnen ermöglicht, grenzüberschreitend zu operieren und aus Profitgründen oder einfach nur zur Störung anzugreifen. Jegliche Informationen über Cyber Threats, wie zum Beispiel Ziele, Techniken oder weitere Details werden CTI genannt. Eine ausführliche Definition von CTI wird auch von Gartner [49] geliefert.

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard". [49]

Um eine erfolgreiche Cybersicherheits-Strategie zu etablieren, hat die Cybersecurity-Community damit begonnen, CTI auszutauschen, um Organisationen bei der Verteidigung vor sich ständig ändernden sowie neu auftretenden Cyber Threats zu unterstützen. CTI ist eine strukturierte Art und Weise, Wissen über Cyber Threats und Schwachstellen darzustellen, nachdem relevante Informationen gesammelt, aggregiert, bewertet, untersucht oder mit Unterstützung geeigneter Analyseverfahren angereichert wurden. [50] Ein besserer Informationsaustausch von CTI verbessert die Abschreckung und Reaktionsfähigkeit gegen Angriffe. Dennoch gibt es nach wie vor ernsthafte Hindernisse, die oft aus Sicherheitsbedenken und komplexen Angriffen entstehen.

Raffinierte Angreifer nutzen fortschrittliche Methoden wie zum Beispiel polymorphe und zusammengesetzte Angriffe, die so personalisiert sind, dass sie signaturbasierten Tools unbekannt erscheinen und dennoch authentisch genug sind, um Spam-Filter zu umgehen. Daher können sie den Angriff nicht als eine koordinierte Abfolge von Angriffen betrachten und analysieren. [51] Eine umfassende Klassifizierung der Bedrohungslandschaft wurde Anfang 2017 von European Network and Information Security Agency (ENISA) vorgenommen, indem erstmalig auch aktuelle Informationen über den CTI präsentiert worden ist.

3.4. Probleme von Cyber Threat Intelligence Landscapes

In diesem Kapitel wird eine Literaturrecherche durchgeführt, um festzustellen, welche allgemeinen Probleme Cyber Threat Intelligence Landscapes haben.

3.4.1. Ineffektive Priorisierung

In der Studie [2] wurde die Qualität der Sicherheitsberatung evaluiert. Dabei wurde zuerst eine Klassifizierung von 374 Sicherheitshinweisen erstellt. Die Klassifizierung hat dabei einen Einblick in den Umfang und die Menge der von Benutzern erhaltenen Ratschläge vermittelt. Die Klassifizierung soll ein Hilfsmittel für Forscher sein, welche Sicherheits- und Datenschutzverhalten analysieren, um die Verbesserung von Sicherheitsratschlägen voranzutreiben. Bei der Analyse von Sicherheitsratschlägen wurde besonders viel Wert auf die Nachvollziehbarkeit, Handlungsfähigkeit und Wirksamkeit gelegt.

Ein wesentliches Problem, dass die Experten der Studie erfasst haben, ist die Priorisierung von Ratschlägen von Sicherheitsexperten. Von den 41 professionellen Sicherheitsexperten, die in dieser Studie befragt wurden, bewerteten nicht nur 89 % der Ratschläge als zutreffend, sondern gaben auch an, dass 118 Ratschläge zu den Top 5 gehören, die sie den Benutzern empfehlen würden.

Die Experten warnen, dass sich die Situation zwangsläufig verschlimmern wird, wenn die Erteilung von Ratschlägen sich nicht verbessert. Da immer wieder neue Angriffe auftauchen, werden wahrscheinlich weiterhin neue, reaktive Ratschläge herausgegeben, ohne alte Ratschläge zu verwerfen oder die Prioritäten neu zu bewerten. Dabei wird auf die Forschungsarbeit [52] „Unfalsifiability of security claims" verwiesen, indem eine inhärente Asymmetrie in der Computersicherheit analysiert wird: Dinge können durch Beobachtung für unsicher erklärt werden, aber nicht umgekehrt. Es gibt keine Beobachtung, die es uns erlaubt, ein beliebiges System oder eine beliebige Technik für sicher zu erklären.

Die Experten empfehlen ein klares Bekenntnis der Sicherheitsberater zur Minimalität und Praktikabilität. Die empirische Identifizierung von einfachen und umsetzbaren Ratschlägen, um den maximalen Schutz des Benutzers zu gewährleisten. In dieser Arbeit wird versucht, den Ratschlag der Experten für CTI Landscapes zu berücksichtigen, um Priorisierungen effektiv durchführen zu können.

Wie wichtig eine effektive Priorisierung ist, erkennt man durch die Studie [42] von Accenture und das Ponemon Institute. Die Studie schlussfolgert, dass durch die effektive Priorisierung von Schutztechnologien und in dem Sinne auch Bedrohungen, Unternehmen die Folgen von Cyberkriminalität reduzieren und

zukünftige wirtschaftliche Vorteile bringen können, da ein höheres Maß an Vertrauen zu mehr Geschäften mit Kunden führt.

Müller Krzysztof beschreibt aus einer praktischen Sicht, weshalb der richtige Fokus wichtig ist.

> *„Fokus auf die gefährlichsten Bedrohungen ist viel wichtiger als der Versuch alle möglichen Gefahren zu analysieren und Gegenmaßnahmen zu ergreifen. Für die Vorbeugung aller möglichen Gefahren reichen in der Regel die Ressourcen des Unternehmens nicht aus.“ [53]*

3.4.2. Integrität und Transparenz der Quellen

Des- und Falschinformationen sind im Internet weit verbreitet und bedrohen die Integrität der Quellen für CTI Landscapes. In den nächsten Abschnitten wird analysiert, wie der aktuelle Stand der Forschung zum Erhalt der Integrität und Transparenz von Informationen ist.

Für Politiker sind Des- und Falschinformationen ein großes Thema, da ausländische Regierungen soziale Medien nutzen, um die Politik von bestimmten Ländern zu beeinflussen, indem sie Propaganda betreiben, kontroverse Standpunkte vertreten und Desinformationen verbreiten. [54, 55]

In einer ähnlichen Arbeit [3] wird die Verbreitung von Desinformation in Bezug auf ungeprüfte OSINT-Quellen analysiert. Der Autor weist auf die hartnäckige Verbreitung von Desinformationen hin, insbesondere in sozialen Netzwerken, diese stellen derzeit einer der größten Bedrohungen für Benutzer dar.

Die Social Media Plattformen reagieren darauf, indem sie an Desinformationsinhalte Warnungen anhängen. Dass Warnungen nicht ausreichen, haben Sicherheitsforscher schon vor Jahrzehnten aufgezeigt. In einer Studie [56] aus dem Jahre 2006 wurden Toolbars von Browsern, inklusive Security-Toolbars, um ihre Effektivität überprüft. Alle Toolbars konnten den Benutzer nicht vor einem Phishing Angriff beschützen. Die Versuche scheiterten an den Benutzern, die es nicht geschafft haben, verdächtige Anzeichen oder Indikatoren zu interpretieren. Eine weitere ältere Studie [57] aus 2008 hat den Fachkundigen aufgezeigt, dass 87% der Studienteilnehmenden einem Phishing Link gefolgt sind und dabei die passiven Warnhinweise ignoriert haben.

Auch für den Finanzsektor können Des- und Falschinformationen entscheidend sein. Für den Finanzsektor ist der besorgniserregendste Aspekt solcher Angriffe die Untergrabung des Vertrauens. Vertrauensbeziehungen zwischen den beteiligten Akteuren sind unerlässlich, um CTI zu teilen. Eine ähnliche Arbeit [58] hat sich darauf fokussiert, 30 Bedrohungsdaten-Anbieter und -Plattformen zu analysieren. Dabei wurden die Methoden zur Vertrauenserstellung, wie zum Beispiel Vetting analysiert. Das Ergebnis der Studie ist eine Vertrauens-Taxonomie mit realistischen Fallstudien.

In [59] haben die Autoren die Notwendigkeit einer Bewertung der Informationsqualität speziell für Big Data im Kontext der Intelligence-Community aufgezeigt. Ihre Lösung ist die Einführung einer Reihe von Metriken zur Bestimmung der Qualität der Quelle sowie eines Ansatzes zur Validierung dieser Quelle. Dabei wurde ein Set von Parametern (Umfang, Wartung, False-Positives, Verifizierbarkeit, Intelligence, Interoperabilität, Konformität, Aktualität, Vollständigkeit, Ähnlichkeit) verwendet.

Die Autoren der Arbeit [60], beschreiben einen anderen Ansatz, welcher Metriken und Indikatoren identifiziert, die spezifisch für die Domäne sind. Der Ansatz beruht darauf die Methodik in fünf Bewertungskriterien strukturiert zu haben: Syntaxgenauigkeit, Vollständigkeit, Aktualität, Situationsgenauigkeit, Konsistenz und Relevanz. Dieser Ansatz wurde speziell für den Kontext des

Situationsbewusstseins in Notfällen entwickelt. Das Ziel ist es, den Empfang kritischer Informationen durch Notfallteams zu verbessern, indem die Quellen anhand der oben genannten Kriterien bewertet werden.

3.4.3. Starker Kontrast der Perspektiven

Die Perspektive eines CTI Landscapes kann sich je nach Zielgruppe des Berichts stark ändern. Ein Beispiel ist der CTI Landscape von Intsights [47], welcher sich auf den Finanzsektor spezialisiert hat. Internationale Organisation wie der WEF [7] und IMF [46] erkennen dadurch, wie wichtig die erweiterte Perspektive für Cybersecurity ist. Dass eine zu unspezifische oder zu allgemeine Perspektive langfristig keine Lösung bietet, um über die aktuelle Landschaft der Bedrohung zu berichten, hat man durch die Entscheidung von ENISA gemerkt, welche zu mehreren spezifischeren Berichten gewechselt haben. Ziel war ein benutzerfreundlicheres Format, das den Bedürfnissen der Empfänger entspricht, um ihre Bereitschaft zu verbessern und die Reaktion besser auszurichten. [61]

Intsights fällt durch zahlreiche spezifische CTI Landscapes auf. Um zu verstehen, welchen Einfluss verschiedene Perspektiven haben, werden aktuelle Berichte von den verschiedenen Sektoren verglichen. Zum Beispiel im aktuellen Bericht [62] zum Banken- und Finanzdienstleistungssektor. Banken und Finanzinstitute schützen unglaublich sensible Daten von Nutzern und Mitarbeitern gleichermaßen, und Datenschutzverletzungen können sowohl in Bezug auf geleakte Daten als auch auf die anfallenden finanziellen Strafen kostspielig sein. Der Bericht gibt an, dass Cyberkriminelle ständig neue Wege entwickeln, um selbst die umfangreichsten Sicherheitssysteme zu infiltrieren. Aufgrund der großen Menge an Kreditkarteninformationen in Online-Foren empfiehlt Intsights auf die proaktive Identifizierung und Validierung von Bedrohungen zu setzen.

In einem weiteren Bericht [63] wird die Bedrohungslandschaft der Telekommunikationsindustrie analysiert. Die Telekommunikationsbranche sieht sich aufgrund der raschen Digitalisierung einem Ansturm von Cyberangriffen gegenüber. Laut des Berichts sichern Telekommunikationsunternehmen äußerst wertvolle Bestände an sensiblen Kundendaten und Zwei-Faktor-Authentifizierungssystemen. Dies erhöht den Druck der Sicherheitsteams von dem Sektor, Cyber-Bedrohungen proaktiv zu erkennen und zu vereiteln, bevor sie sich zu Angriffen entwickeln. Aufgrund der Menge an historischen Angriffen auf Mitarbeiter und Hinweise auf Bestechungsangebote in Online-Foren, empfiehlt Intsights Telekommunikationsanbietern, in Insider-Threat Programme zu investieren.

Noch spezifischer wird Intsights mit einem Bericht [64] für Automobilhersteller und -händler. Auch hier sehen die Autoren einen Ansturm von Cyberangriffen, da die Angreifer von Automobilhersteller den Betrieb der Autos stören und sensible Daten oder geistiges Eigentum stehlen. Der Bericht schätzt den Schaden durch Angriffe auf Mitarbeiter oder interne Systeme größer ein als durch das Hacken von Autosoftware. Für die Automobilhersteller sieht Intsights die größte Gefahr durch Supply-Chain-Attacks und Ransomware-Angriffe, um die Informationen zu stehlen oder die Produktion zu hindern.

Intsights zeigt auf, welche Hinweise sie aus Hacker-Foren gesammelt haben, in denen Informationen und Userdaten von Finanzdienstleistern, Telekommunikationsanbietern oder Autohändlern verkauft werden. Weiters zählen sie die Datenpannen von den jeweiligen Sektoren auf. Am Ende werden Ergebnisse und Empfehlungen zusammengefasst. Die Empfehlungen sind dabei sehr spezifisch und unterscheiden sich stark, dadurch ist erkennbar, dass die Perspektive des Berichts einen starken Einfluss auf die Ergebnisse hat.

Die stetig wandelnde Bedrohungslandschaft gilt auch für die einzelnen Branchen und Sektoren, unterstrichen wird das, zum Beispiel durch neue Gesetzesentwürfe, die dem Staat erlauben Telekommunikationsanbieter anzugreifen [65] oder durch erstmalige Einsätze von neuen Technologien im öffentlichen Sektor. Letzteres bezieht sich auf eine Voting-App mit Blockchain Technologie, die bei einer US-Wahl zum Einsatz kam. In der Forschungsarbeit [66] wurden Schwachstellen untersucht, die trotz neuer Blockchain Technologien nicht beseitigt werden konnten.

In einer weiteren wissenschaftlichen Arbeit [67] wird das CTI Landscape vom Energiesektor in Finnland untersucht und weitere Probleme von verschiedenen Perspektiven beschrieben. Dort stellen die Autoren fest, dass in der Regel weitgehend Einigkeit bei der Berichterstattung über die technischen Details eines Security Incident herrscht, jedoch variiert die Interpretation von Akteur, Motivation oder Bedeutung je nach

analysierender Organisation und Einzelpersonen. In der Regel ist die Interpretation von offizieller Seite eher konservativ und Pressematerial oder sozialen Medien nähern sich in einigen Fällen Vermutungen an. [67]

Genau beschreiben die Autoren, dass bei einem bestimmten Fall Vodafone und das National Cyber Security Centre den Angriff auf einen staatlich gesponserten Akteur zurückführen, jedoch wird nicht weiter auf diese Einschätzung eingegangen. Zusätzlich zu den gezielten Cyber-Kampagnen sind die Akteure im Energiesektor auch mit konventionelleren Arten von Cyber-Angriffen konfrontiert. Diese werden in der Regel weder von Sicherheitsunternehmen analysiert noch in großem Umfang gemeldet. [67]

Cybersicherheits-Unternehmen veröffentlichen dagegen nur White Papers von größeren Veranstaltungen, und die Autoren geben an, dass es schwierig ist, Informationen über den Energiesektor herauszufiltern. Laut Arbeit bleiben dadurch nur Medienberichte, die oft ihre Quellen nicht angeben und nicht auf die technischen Details eingehen. [67]

3.4.4. Barrieren beim Teilen von Informationen

In der Studie [68] beschreiben die Autoren, wie aufgrund des steigenden Risikos, Geschädigte eines Angriffes zu werden, die gemeinsame Nutzung und Verbreitung von CTI-Informationen zunimmt, dabei ist die Motivation der Threat Agents und ihre Fähigkeiten entscheidend. Es hilft Organisationen, sich besser zu verteidigen und das Risiko der Bedrohungen einzuschätzen. Die Ergebnisse der Studie stellen dar, dass der Austausch von Gefahrenmeldungen mit Tausenden von Intrusion-Detection-Systemen in Echtzeit aufgrund des entstehenden Aufwands und des fehlenden Vertrauens zwischen den Netzwerken unpraktisch ist.

Die Freigabe von CTI-Informationen hat jedoch bestimmte Konsequenzen, die Organisationen zögern lassen, diese zu teilen. Die Hindernisse können sein: (1) Die Wahrscheinlichkeit der unerwünschten Offenlegung von Informationen, wenn sie mit nicht vertrauenswürdigen Organisationen oder Öffentlichkeit geteilt werden, (2) CTI-Informationen können vertrauenswürdige Informationen enthalten, z. B. persönliche, organisatorische, finanzielle und Cybersicherheitsinformationen [69]. Daher ist die Bewertung des Risikos der gemeinsamen Nutzung von kritischen CTI-Informationen, wie z. B. bestehende Schwachstellen, eine Herausforderung, insbesondere angesichts der sich weiterentwickelnden Cyber-Bedrohungslandschaft und der ausgefeilten Cyber-Angriffe für verschiedene Geschäftsbereiche. [70]

In einer Studie, indem 67 Cybersicherheitsexperten zum Thema Vorteile und Hindernisse des Informationsaustauschs befragt worden sind, wurde festgestellt, dass 41% der Befragten das Risiko der Verletzung des Datenschutzes und der Kartellgesetze als eine große Sorge beschreiben und dass dies den Austausch von Bedrohungsdaten behindern könnte. Etwa ein Viertel der Befragten stimmte nachdrücklich zu, dass uneinheitliche rechtliche Rahmenbedingungen den internationalen Austausch von Informationen über Bedrohungen erschweren. [71]

Da der Informationsaustausch stark von lokalen und gesetzlichen Anforderungen abhängt, sind ebenfalls die rechtlichen und politischen Aspekte zu beachten. Das Fehlen von allgemeinen Sicherheitsvereinbarungen kann das Teilen von CTI hindern. In [72] beschreiben die wissenschaftlich Publizierenden, welche Auswirkungen die DSGVO auf die gemeinsame Nutzung von CTI haben kann. Zusätzlich wird ein Modell zur Bewertung der rechtlichen Anforderungen zur Entscheidungsfindung bei der gemeinsamen Nutzung von CTI gegeben.

Nicht nur die DSGVO stellt eine rechtliche Basis für den Austausch von CTI zur Verfügung, sondern in gewissem Maß auch die EU-NIS-Richtlinie [73]. Speziell für Organisationen, die Teil kritischer nationaler Infrastrukturen sind. Sie verlangt von allen EU-Mitgliedsstaaten die Einrichtung nationaler Computer Security Incident Response Teams (CSIRT) als zentrale Anlaufstelle für die Meldung von Cyber-Vorfällen, die kritische Infrastrukturen und wesentliche Dienste betreffen. Dies wird von der ENISA unterstützt, die die

CSIRT durch die Bereitstellung von Tools und Methoden zur Unterstützung der Netz- und Informationssicherheit verbessert. [72]

Trotz der zunehmenden Reife der CTI-Techniken und der CTI-Nutzung gibt es immer noch Lücken, behauptet ENISA im Bericht [74]. Insbesondere in Bezug auf die verschiedenen Anwendungsfälle, wie zum Beispiel die sektorale CTI und die CTI-Arten (operativ, taktisch, strategisch). ENISA stellt fest, dass CTI-Elemente wie zum Beispiel TTPs, die in verschiedenen internationalen bewährten Verfahren und Rahmenbedingungen wie ATT&CK, enthalten sind, weiterentwickelt werden müssen. Das Wesentliche der erforderten Weiterentwicklung ist, dass die bewährten Verfahren Informationen aus einem breiteren Spektrum von Angriffen einbeziehen. Besonders dringlich sind die CTI-Elemente verschiedener Sektoren sowie Infrastrukturen und Angebote für die Bereitstellung von Diensten. [74]

ENISA listet die Zeitspanne zwischen dem Vorfall, Erstellung der CTI und der Einpflegung dieser Informationen mit Open-Source-Tools, als Haupthindernis für die Verbreitung umsetzbarer CTI für verschiedene Plattformen und Infrastrukturen. Die beteiligten Parteien benötigen engere Koordination und Zusammenarbeit. Der Aufbau von Vertrauen zwischen den teilnehmenden Unternehmen ist wesentlich für CTI. CTI wird in einigen breiten Kategorien angeboten, je nach den Anforderungen der Benutzer. Die drei Typen der Anforderungen sind operativ, taktisch und strategisch. Bestehende kommerzielle Angebote, deren Basis aus Erfassung, Wartung, Analyse und Verbreitung von CTI oder CTI-Feeds bestehen, unterstützen einige dieser CTI-Typen. Es gibt jedoch keinen einheitlichen Ansatz. Bestehende Angebote konzentrieren sich auf operative und taktische CTI, während strategische CTI meist unabhängig angeboten werden. [74]

Eine weitere Barriere ist das Nutzen von CTI auf einer strategischen Ebene. Auf der strategischen Ebene sind die Vorstände von Organisationen mit Aufgaben wie Entscheidungsfindung, Investitionen in die Cybersicherheit und Interessenausgleich verantwortlich. Auf operativer Ebene ermitteln die Vorstände zukünftige und langfristige Risiken durch Risikobewertungen und Analysen der Geschäftskontinuität. Im Rahmen eines Risikobewertungsprozesses stehen die kritischen Vermögenswerte im Mittelpunkt. Es ist wichtig, die Bedrohungen, denen diese Anlagen ausgesetzt sind, die Schwachstellen sowie die Wahrscheinlichkeit eines Angriffs oder einer Kompromittierung zu ermitteln. Einige Attribute der CTI auf technischer Ebene, wie zum Beispiel IoCs und TTPs, können verwendet werden, um Vorstände zu informieren. [75]

In [75] beschäftigt sich damit, mithilfe des Cyber Security Decision Making Informed by Threat Intelligence Framework, die CTI auf technischer Ebene in eine Sprache übersetzt, die die strategische Ebene verstehen kann, so dass der Vorstand sie für die Entscheidungsfindung im Bereich der Cybersicherheit nutzen können. Der Vorstand, die mit umsetzbaren CTI ausgestattet sind, um besser informierte Entscheidungen zu treffen.

Welche Auswirkungen es haben kann, wenn CTI nicht ordnungsgemäß in die strategische Ebene einfließt, damit die Vorstände fundierte Entscheidungen treffen können, wird in [76] beschrieben. Dabei wurde festgestellt, dass strategische Nutzung von CTI das Risiko von wertvollen Vermögenswerten der Organisation erheblich verringern und die Zuverlässigkeit erhöhen kann. Die Arbeit beschreibt wie strategische CTI in einem Unternehmen implementiert und genutzt werden kann, um die Cyber-Verteidigung zu verbessern und eine proaktivere und anpassungsfähigere Sicherheitsposition zu schaffen. Zusätzlich wird aufgezeigt, wie sich die wichtigsten CTI Inhalte mit bestehenden Standards für das Cybersecurity-Risikomanagement verbinden lassen. [76]

4. Methodik

Mithilfe der im letzten Kapitel durchgeführten Literaturrecherche wird in diesem Kapitel eine Methode entwickelt, um CTI Landscapes zu analysieren und zu evaluieren. Wie in den Studien [2, 42] beschrieben ist die ineffektive Priorisierung ein großes Problem für Experten. Bei der Erstellung einer Cybersicherheits-Strategie ist daher die Einbindung von möglichst vielen CTI Landscapes unzweckmäßig. Um die Auswahl der CTI Landscapes so effektiv wie möglich zu gestalten, wird eine Bewertungsmethode entwickelt, um die vorhandenen CTI Landscapes miteinander zu vergleichen. Diese Methode wird darauf abzielen, die Bewertung und Platzierung von mehreren CTI Landscapes zu ermöglichen.

4.1. Methodologie und Quellenanalyse

Wie in der Arbeit [3] beschrieben ist die Verbreitung ungeprüfter Quellen zu verhindern. Daher ist es für CTI Landscapes essenziell mit der Methodologie transparent zu sein. Um eine Überprüfung der Quellen zu ermöglichen, muss die Auflistung vollständig sein.

Die Beschreibung der Methodologie ist wichtig, da der Leser Kenntnis von den methodologischen Grundlagen benötigt. Beim Schreiben einer Cybersicherheits-Strategie ist es essenziell, dass der Autor Informationen über die Objektivität, Reliabilität und Validität seiner Quellen hat.

- M1: Wird die Methodologie beschrieben?
- M2: Werden die Quellen gelistet?

4.2. Zielgruppe

In der wissenschaftlichen Arbeit [67] wurde aufgezeigt, wie wichtig die Zielgruppen und Perspektiven sind sowie die Ergebnisse sich dementsprechend unterscheiden können. Daher ist es für CTI Landscapes wesentlich, die Zielgruppe zu definieren und die Informationen auf die Sektoren oder Branchen aufzuteilen.

Manche Cyber Bedrohungen gelten für alle Sektoren, jedoch muss der Autor einer Cybersicherheits-Strategie über die sektorspezifischen Risiken informiert sein. Da Bedrohungen sich weiter auf spezifische Zielgruppen oder Sektoren spezialisieren [36], werden die Information über die aktuelle Bedrohungslage des eigenen Sektors immer wichtiger.

- Z1: Wird explizit eine Zielgruppe definiert?
- Z2: Ist eine Aufteilung von Sektoren vorhanden?

4.3. Threat Agents

Threat Agents sind ein wesentlicher Teil der Bedrohungslandschaft. Um Dynamik und Modus Operandi von Angriffen zu verstehen, ist es essenziell die Verhaltensweisen und Motivationsfaktoren der Angreifenden zu verstehen. Daher werden Informationen über Threat Agents in die Bewertungstabelle mit eingebunden.

Um die Bedrohung von menschlichen Threat Agents vollständig zu verstehen, muss man die menschlichen Antriebe verstehen. Dieses Verständnis ermöglicht Verteidigenden maßgeschneiderte Kontrollen zu entwickeln oder die Cybersicherheits-Strategie anzupassen, da die Motivation die Intensität und die Ausdauer eines Angriffs bestimmen kann. Zum Beispiel hat ein ideologisch motivierter Threat Agent wahrscheinlich die Geduld, um langfristige Ziele zu erreichen und jahrelang im Stillen zu arbeiten, während

ein Cybervandale schnell das Interesse verliert und weiterzieht. Daher hat Intels Security and Privacy Office den Parameter “Motivation” neu in ihre Bedrohungs-Taxonomie hinzugefügt. [77]

- T1: Wird über Threat Agents berichtet?
- T2: Werden über die Motivationsfaktoren berichtet?

4.4. Angriffsvektor

Ein weiterer wesentlicher Teil der Bedrohungslandschaft sind die Angriffsvektoren. Mithilfe von Statistiken oder Rangfolgen ist eine einfache Darstellung der Bedrohungslandschaft möglich. Daher werden Informationen über Angriffsvektoren in die Bewertungstabelle mit eingebunden.

- A1: Wird über Angriffsvektoren berichtet?
- A2: Werden Statistiken zu den beliebtesten Angriffsvektoren beschrieben?

4.5. Prognosen

Um gegen zukünftige Herausforderungen gewappnet zu sein, sind die Prognosen oder Trendanalysen ein wichtiges Element von CTI Landscapes. Besonders aufgrund der wachsenden Komplexität von Bedrohungen ist es wichtig die Möglichkeit zu haben, die Bedrohungslage von neuen Technologien zu berücksichtigen.

Die Angriffsvektoren sind wesentlich bei der Erstellung einer Cybersicherheits-Strategie. Je mehr Angriffsvektoren berücksichtigt werden, desto mehr Risiken können abgemildert werden. Da eine vollständige Cybersicherheit nicht zu erreichen ist, wird nicht empfohlen, sich nur auf einzelne Risiken oder Bedrohungen zu fokussieren.

- P1: Wird eine Prognose ODER Trendanalyse durchgeführt?
- P2: Wird die Bedrohungslage von neuen Technologien beschrieben?

4.6. Empfehlungen

Bei der Erstellung einer Cybersicherheits-Strategie geben die Empfehlungen von CTI Landscapes Orientierung. Die Entscheidungsprozesse werden verkürzt und das Risiko einer bedrohlichen Fehlentscheidung sinkt. Jedoch ist nicht nur die technischen Empfehlungen für die Cybersicherheits-Strategie relevant, sondern auch die organisatorischen Empfehlungen. Cyber Sicherheit entsteht nicht nur durch den Schutz der technischen Aspekte, sondern durch eine multidisziplinäre Perspektive. [6]

- E1: Werden Empfehlungen gegeben?
- E2: Werden technische UND organisatorische Empfehlungen gegeben?

4.7. Vorlage der Bewertungstabelle

In diesem Kapitel wird die Vorlage zur Bewertung vorgestellt, dafür wird eine Bewertungstabelle mit Ja/Nein-Fragen erstellt. Je mehr Fragen mit „Ja“ beantwortet werden, desto höher wird das CTI Landscape eingeordnet. Im Kapitel 6 werden die Fragen mit dem im Kapitel 5 ausgewählten CTI Landscapes beantwortet.

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
CTI Landscape 1													
CTI Landscape 2													
...													

Tabelle 3 - Eigene Darstellung der Mustertabelle

Beschreibung der Tabelle:

Jedes CTI Landscape ist eine Zeile. Die sechs wesentlichen Aspekte werden in jeder Spalte abgebildet. Die Aspekte sind in den zwei jeweiligen Fragen unterteilt. Die Fragen dieses Kapitels sind abgekürzt dargestellt. Die Antwortmöglichkeiten der Fragen sind „Ja“ oder „Nein“. Am Ende wird die Anzahl der „Ja“ Antworten zusammengezählt.

5. Cyber Threat Intelligence Landscapes

In diesem Kapitel wird die Auswahlmethode der CTI Landscapes beschrieben. Danach werden die CTI Landscapes kategorisiert, um am Ende die Struktur sowie Inhalte der Berichte zu analysieren. Um eine methodische Bewertung zu ermöglichen, wird die Struktur der CTI Landscapes und sechs grundlegende Aspekte analysiert. Die sechs Aspekte sind abgeleitet von den Fragen aus Kapitel 4 und stellen folgende grundlegende Fragen:

- Wird die Methodologie und Quellen angegeben?
- Welche Zielgruppe haben die Berichte definiert?
- Werden über Threat Agents berichtet?
- Werden über Angriffsvektoren berichtet?
- Werden Prognosen gestellt?
- Werden Empfehlungen geäußert?

5.1. Regierungsstellen

ENISA veröffentlich weitaus den umfangreichsten und größten CTI Landscape [33]. Im deutschsprachigen Raum folgen danach „Die Lage der IT-Sicherheit in Deutschland“ [34], „Melani“ [78] von der Schweiz, „Bericht Cybersicherheit“ [79] vom Bundeskanzleramt (BKA) in Österreich und „Jahresbericht Internet-Sicherheit“ [80] von CERT.at und GovCERT Austria. Zusätzlich veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus Deutschland gemeinsam mit dem Agence nationale de la sécurité des systèmes d’information (ANSSI) aus Frankreich den „Franco-German common situational picture“ [81], welcher jedoch wegen dem großen politischen Anteil nicht analysiert wird.

5.1.1. ENISA

Die ENISA ist die zentrale europäische Einrichtung mit dem Ziel, die Zusammenarbeit der verschiedenen europäischen Institutionen und Mitgliedsstaaten zu verbessern, indem sie den Austausch von Bedrohungen, Methoden und Ergebnissen im Bereich der Netz- und Informationssicherheit fördert und Doppelarbeit vermeidet. [33]

Seit 2012 veröffentlicht die ENISA jährlich CTI Landscapes, welche einen Überblick über Bedrohungen sowie über aktuelle und sich abzeichnende Trends liefert. Sie basiert auf öffentlich verfügbaren Daten und bietet eine unabhängige Sicht auf beobachtete Bedrohungen, Bedrohungsagenten und Bedrohungstrends. Dabei wird das Angebot von Exzellenznetzwerken der IT-Security-Branche, Standardisierungsgremien und anderen unabhängigen Instituten analysiert und erweitert. [33]

ENISA - Struktur

Im Jahr 2020 wechselte ENISA die Struktur von einem großen Bericht zu mehreren Berichten [61], welche sich durch die Art des Inhalts und der Zielgruppe unterscheiden. Dabei unterscheidet ENISA technische und spezifische Berichte von generischen und strategischen Berichten. Erstmalig differenziert ENISA auch die Zielgruppe der Berichte, die für strategisches Management und Führungskräfte oder speziell für die CTI Community sind.

Der erste Bericht [33] „The Year In Review“ bietet einen allgemeinen Überblick über die Bedrohungslandschaft und umreißt die wichtigsten Themen, auf die in allen anderen ENISA Berichten Bezug genommen wird. Außerdem enthält es die ENISA-Liste der 15 größten Cyber Threats, Schlussfolgerungen und Empfehlungen. Der Inhalt ist generisch und nicht-technisch, daher ist es für jeden

geeignet. Für ein besseres Verständnis, wie das CTI Landscape aufgebaut ist, empfiehlt ENISA, zuerst diesen Bericht zu lesen.

ENISA - Methodologie und Quellen

Die Berichte basieren auf öffentlich verfügbaren Quellen. Dabei spezialisiert sich der Bericht auf keinen Sektor, keine Technologie oder keinen Kontext. Der Bericht [33] versucht, branchen- und herstellerunabhängig zu sein. Die Quellen sind

- aus verschiedenen Sicherheitsforschungen,
- Sicherheitsblogs,
- Medienartikeln,
- Expertenmeinungen,
- Geheimdienstberichten,
- Vorfallsanalysen,
- Mitglieder der EU CTI Community
- und Sicherheitsforschungsberichten.

ENISA versichert dabei, die offenen Quellen gründlich zu recherchieren. Ziel ist es, eine Top-15-Bedrohungsliste zu definieren und Annahmen über die Trends und zukünftige Herausforderungen im Bereich Cybersicherheit zu treffen. [33]

ENISA verwendet hauptsächlich eigene Quellen. Bei Berichten über vergangene Hackingangriffe weist ENISA auf renommierte Nachrichtenseiten, wie zum Beispiel cnbc.com oder cnet.com. Weiters beziehen die Berichte auch aus Quellen von ähnlichen europäischen Agenturen wie dem Europäischen Zentrum für die Förderung der Berufsbildung oder East StratCom Task Force und branchenbekannten Instituten wie SANS. Auch Quellen von Unternehmen wie intel471.com, verizon.com und bitdefender.com, werden verwendet, besonders, wenn die Berichte Statistiken behandeln. [33]

ENISA - Zielgruppe

Der Bericht ist zum Teil strategisch und zum Teil technisch, mit Informationen, die sowohl für technische als auch für nicht-technische Leser relevant sind. Dabei stellt der Bericht eine Tabelle mit den jeweiligen Zielgruppen auf. [33]

	Inhalt	Zielgruppe
The Year in Review [33]	Generisch	Alle
CTI Overview [82]	Spezifisch	CTI Community Mitglieder und Anwender
Sectoral and Thematic Threat Analysis [83]	Strategisch	Experten für strategisches Management, Politikern und Entscheidungsträgern, Risiko Analysten, Cybersicherheitsmanager und Führungskräfte
Main Incidents in the EU and Worldwide [84]	Strategisch	Experten für strategisches Management, Politikern und Entscheidungsträgern, Risiko Analysten, Risikomanager und Führungskräfte
Research Topics [85]	Strategisch	Experten für strategisches Management, Politikern und Entscheidungsträgern, Risiko analysten, Risikomanager und Führungskräfte
Emerging Trends [86]	Strategisch	Experten für strategisches Management, Politikern und Entscheidungsträgern, Risiko analysten, Risikomanager und Führungskräfte
List Of Top 15 Threats [87]	Technisch	Informationssicherheits-Manager (ISM), Verantwortliche für Informationssicherheit (CISO), Cybersicherheitsspezialisten und CTI Analysten

Tabelle 4 - ENISA Zielgruppe [33]

ENISA - Threat Agents

Im Bericht [84] fokussiert sich ENISA auf die Threat Agents, um Verhaltensweisen zu klassifizieren, die Dynamik und den Modus Operandi bestimmter Angreifer zu verstehen. Dabei listet ENISA die aktivsten Threat Agents auf, die ihnen bekannt sind. Ein weiterer wesentlicher Punkt dabei ist auch die Motivation der Threat Agents. Da liefert ENISA die größten Motivationsfaktoren für die Angreifer auf. Spionage, Störung, Vergeltung, politische und finanzielle Faktoren sind dabei die beliebtesten Motive.

ENISA - Angriffsvektor

Die Angriffsvektoren vom Bericht [87] werden als Top-15-Bedrohungsliste angezeigt, dabei wird die Entwicklung der Bedrohung im Vergleich zum Vorjahr gestellt, um einen Trend darzustellen.

Platzierung	Bedrohungen	Trend
1	Malware [88]	~
2	Web-based Attacks [89]	~
3	Phishing [90]	↑
4	Web application attacks [91]	~
5	Spam [92]	↓
6	Denial of service [93]	↓
7	Identity theft [94]	↑
8	Data breaches [95]	~
9	Insider threat [96]	↑
10	Botnets [97]	↓
11	Physical manipulation, damage, theft and loss [98]	~
12	Information leakage [99]	↑
13	Ransomware [100]	↑
14	Cyberespionage [101]	↓
15	Crytojacking [102]	↓

Tabelle 5 - ENISA Angriffsvektoren [87]

Beschreibung der Tabelle:

Die Tabelle listet die größten 15 Bedrohungen auf. Der Trend gibt an, ob die Bedrohung im Vergleich zum ENISA Bericht 2018 [103] in der Platzierung gleichgeblieben, gestiegen oder gesunken ist. „↓“ steht dafür, dass die Bedrohung gesunken ist. „↑“ steht dafür, dass die Bedrohung gestiegen ist. „~“ steht dafür, dass die Bedrohung gleichgeblieben ist.

Der Bericht [87] von ENISA hat für jeden Angriffsvektor wieder einen spezifischen Bericht veröffentlicht. In den spezifischen Berichten wird noch detaillierter die jeweilige Bedrohung analysiert. Zum Beispiel steht im Malware Bericht [88], dass Malware eine häufige Art von Cyberangriffen in Form von bösartiger Software ist. Zu der Malware-Familie gehören Kryptominers, Viren, Ransomware, Würmer und Spyware. ENISA gibt an, dass 46,5% aller Malware in E-Mail-Nachrichten im Dateityp '.docx' gefunden [104] und 67% der Malware über verschlüsselte Verbindungen übertragen werden. [105] Dabei verweist ENISA auf öffentlich zugänglichen Quellen.

Im Bericht [83] werden die beliebtesten Bedrohungen der jeweiligen Sektoren aufgelistet. Somit werden die Schutzanforderungen und Prioritäten aufgezeigt.

ENISA - Prognosen

Zusätzlich wird im Bericht [83] die Bedrohungslage und neue Herausforderungen von neuen Technologien beschrieben. Kontextualisierte Cyber-Bedrohungsdaten für Sektoren ist ein wichtiges Instrument zur Vorbereitung auf Rückschlüsse auf zu erwartende Cyberangriffe innerhalb eines bestimmten Sektors. Die Sektoren sind Einzelpersonen, mehrere Industrien, öffentliche Verwaltung, Finanzwesen, Gesundheitswesen, Bildung, IT, digitale Dienstleistungen, Unterhaltung und Produktion. Zu den neuen Technologien gehört 5G, Internet of Things (IoT) und Smart Cars.

Im Bericht [86] werden die größten Herausforderungen und Trends aufgelistet, ohne dabei auf einen speziellen Sektor einzugehen. ENISA gibt an, dass in der nächsten Dekade die Cybersecurity-Risiken aufgrund der wachsenden Komplexität der Bedrohungslandschaft, der wachsenden Komplexität und der Vergrößerung der Angriffsfläche werden. Ein weiterer Aspekt ist die Komplexität und Raffinesse der TTPs, die von Gegenspielern für ihre Angriffe verwendet werden.

ENISA - Empfehlungen

In den Berichten [33, 82] unterteilt ENISA die Empfehlungen auf drei verschiedene Zielgruppen – für Entscheidungsträger, Unternehmen und Wissenschaftler. Die Empfehlung für Entscheidungsträger ist eine CTI Kooperation und Koordination zu etablieren. Zusätzlich wird eine risikobasierte Herangehensweise empfohlen, um die Cybersecurity Bereitschaft zu verbessern. ENISA empfiehlt auch CTI in die Security Management Prozesse einzubinden, um rechtzeitig zur Identifizierung, Erkennung und Prävention von Bedrohungen beizutragen.

Für Unternehmen wird die Nutzung von Test-Labs oder Cyber-Ranges empfohlen, um Mitarbeiter zu trainieren oder Angriffe zu simulieren. ENISA empfiehlt langfristig OpenCTI [106] zu verwenden. OpenCTI ist eine Open-Source-Plattform, welche es Unternehmen ermöglicht, ihr Wissen über Cyber-Bedrohungen zu speichern, zu organisieren, zu visualisieren und zu teilen.

Für die Forschung und pädagogische Einrichtungen empfiehlt ENISA weiterhin die finanzielle Förderung und Entwicklung von der EU. Zusätzlich wird eine multidisziplinäre Cybersecurity Forschung mit sozialen, verhaltenswissenschaftlichen und wirtschaftlichen Disziplinen empfohlen. Im Bericht [85] wird empfohlen neue CTI Forschung im Bereich von Automatisierung und return-on-investing durchzuführen. Zum Beispiel automatisierte Werkzeuge zur Verwaltung von CTIs und neue Methoden oder Werkzeuge, um mithilfe von KPIs die Effektivität der Investitionen zu messen.

In den spezifischen Berichten von den Angriffsvektoren werden detaillierte Informationen zur Prävention von den jeweiligen Angriffsvektoren empfohlen. Zum Beispiel gibt ENISA im Bericht über Malware [88] an, dass folgende Herangehensweise gegen fire-less Angriffe von Malware durchgeführt werden sollte [107]:

- Analyse und Messung der vom Angreifer durchgeführten Aktionen
- Identifizierung der verwendeten Techniken
- Überwachung von Aktivitäten in PowerShell oder anderen Scripting-Engines
- Zugriff auf aggregierte Bedrohungsdaten
- Kontrolle über den Zustand des Zielsystems
- Anhalten fremder Prozesse
- Prozesse, die Teil des Angriffs sind, beseitigen
- Isolierung infizierter Geräte

Zusätzlich zu den spezifischen Empfehlungen gegen eine bestimmte Art von Malware liefert ENISA auch allgemeine Empfehlungen gegen Malware. Diese Empfehlungen sind eine Mischung aus eigenen Quellen und öffentlich verfügbaren Quellen. Zum Beispiel empfiehlt ENISA den Zugriff auf PowerShell-Funktionen zu deaktivieren oder zu reduzieren und verweist dabei auf eine NIST Publikation [108]. Ein Beispiel für eine Empfehlung ohne Verweis auf eine andere Quelle ist, dass ENISA empfiehlt, E-Mail-Filter oder Spam-Filter für die Entfernung von bösartigen E-Mails und ausführbaren Anhängen zu implementieren.

ENISA - Besonderheiten

Die erste große Besonderheit ist, wie erwähnt, die große Aufteilung auf mehrere Berichte und auf ihre Zielgruppen. Eine Besonderheit des Berichtes [84] ist, dass auf die COVID-19 Situation eingegangen und die dadurch veränderte Bedrohungslandschaft zum Thema gemacht wird. Dabei wird erläutert, welche Bedrohungen besonders durch die Pandemie profitieren. Für die Analyse wurden die kritischsten Bedrohungen während dieses Zeitraums bewertet.

5.1.2. BSI

Das BSI ist die Cyber-Sicherheitsbehörde von Deutschland. Ihre Aufgabe ist es, Deutschland digital sicher zu machen. Der Bericht [34] zur Lage der IT-Sicherheit in Deutschland im Jahr 2020 macht deutlich, welche Aufgaben und Herausforderungen im Bereich Cybersicherheit vorhanden sind.

BSI - Struktur

Der BSI fasst alle Inhalte in einem Bericht zusammen. Dabei wird die Bedrohungslandschaft auf die Angriffsvektoren unterteilt. Danach folgen zielgruppenspezifische Erkenntnisse und Lösungen, die in verschiedenen Kategorien wie Gesellschaft, Wirtschaft/Kritische Infrastruktur, Staat/Verwaltung, Internationales und sonstige Entwicklungen in der IT-Sicherheit aufgelistet werden. [34]

BSI - Methodologie und Quellen

Das BSI gibt an, konstant die Bedrohungslandschaft zu beobachten. Der vorliegende Bericht bezieht sich auf den Zeitraum vom 1. Juni 2019 bis 31. Mai 2020 und greift auch Ereignisse danach auf. Das BSI wertet die Rohdaten des Instituts AV-Test GmbH [109] aus. AV-Test ist ein unabhängiges Forschungsinstitut für IT-Sicherheit in Deutschland und gibt an, einer der größten Sammlungen digitaler Schädlinge weltweit zu besitzen. Das BSI erhebt und sammelt somit umfangreiche Daten, welche von hauseigenen Experten unterschiedlicher Fachgebiete analysiert werden. Zusätzlich hat das BSI selbst auch Online-Befragungen

durchgeführt. In der zweiten Hälfte des Berichts beschreibt der BSI eigene Methoden zur Erstellung der Bedrohungslandschaft für die jeweiligen Zielgruppen. [34]

BSI - Zielgruppe

Die zweite Hälfte des Berichts „Zielgruppenspezifische Erkenntnisse und Lösungen“ fokussiert sich auf unterschiedlichen Herausforderungen und Bedrohungen jeweiliger Zielgruppen. Dabei machen von den Seitenzahlen die Zielgruppen Gesellschaft und Wirtschaft den größten Teil aus. [34]

Für die Fokusgruppe Gesellschaft legt das BSI auf den gesamtgesellschaftlichen Dialog. Dieser Dialog basiert auf einem partizipativ ausgerichteten MultiStakeholder-Ansatz, welcher die Bereiche Wissenschaft, Wirtschaft, Staat, Kultur und Medien sowie organisierte Zivilgesellschaft umfasst. Dieses Modell ist im Grunde eine jährlich stattfindende Denkwerkstatt, in der die Stakeholder Vorschläge einbringen können, um die Inhalte über eine agile Arbeitsweise in den nächsten neun Monaten zu bearbeiten. Dabei sind Schwerpunkte entstanden, wie zum Beispiel Smart Homes, Wearables, IoT oder elektronische Gesundheitskarte. Die Schwerpunkte beschreiben die Projekte und Zusammenarbeit mit dem BSI. [34]

Zusätzlich setzt das BSI auf die Plattform bsi-fuer-buerger.de [110], um die Bürger auf Cyber-Security Themen zu sensibilisieren. Auf dieser Plattform werden komplexe Angriffe und Cybersicherheitsthemen mithilfe von Checklisten, informativen Grafiken, interaktive Quizze, einfachen Erklärvideos oder Podcasts verständlich aufgearbeitet. [34]

Für die Fokusgruppe Wirtschaft prüft das BSI, inwieweit ein ausreichender Schutz für die Betreiber Kritischer Infrastrukturen (KRITIS) vorhanden ist. Dabei beschreibt der BSI, welche Maßnahmen in den jeweiligen Sektoren der KRITIS noch Probleme verursachen. Zum Beispiel hat der Transportsektor weiterhin Probleme, technische und organisatorische Maßnahmen vollständig über ein ganzheitlichen Managementprozess, wie etwa ein ISMS, zu etablieren. Zusätzlich werden die Meldezahlen der jeweiligen Sektoren der KRITIS und eine Risikomatrix für KRITIS-Betreiber veröffentlicht. Weiters wird über die weiteren Aufgaben und Projekte des BSIs in der Fokusgruppe Wirtschaft berichtet. Zum Beispiel die Zertifizierungen nach Common Criteria oder Kataloge mit Sicherheitsanforderungen für diverse Projekte. [34]

Für die Fokusgruppe Staat und Verwaltung hat das BSI direkte Informationen, da es Teil des Nationalen Cyber-Abwehrzentrums und Betreiber des Bundes Security Operations Centers (BSOC) sowie des CERT Bund ist. Sonst berichtet das BSI über weitere Projekte, Aufgaben und Erfolge in der Fokusgruppe. [34]

BSI - Threat Agents

Die Motive und Herangehensweise von Threat Agents werden im Kapitel „Advanced Persistent Threats“ beschrieben. BSI sieht im Berichtszeitraum den Trend, dass Angreifer sich immer mehr auf bestimmte Zielgruppen fokussieren. [34]

BSI - Angriffsvektor

Der Bericht [34] vom BSI unterteilt die Bedrohungslandschaft in folgende Angriffsvektoren:

- Schadprogramme
- Diebstahl und Missbrauch von Identitätsdaten
- Schwachstellen
- Advanced Persistent Threats
- Distributed Denial of Service
- Angriffe im Kontext Kryptografie
- Hybride Bedrohungen
- Gefährdung der Cyber-Sicherheit durch die COVID-19-Pandemie

In den jeweiligen Kategorien beschreibt das BSI die auffälligsten Angriffsvektoren sehr ausführlich. Dabei werden reale Angriffe in Sachverhalten dargestellt und dementsprechend Bewertungen oder Maßnahmen empfohlen. [34]

BSI - Prognosen

Analysen zu Trends werden nur im Berichtszeitraum dargestellt, jedoch keine konkreten Prognosen. Zum Beispiel sieht der BSI am Ende des Berichts die schnell voranschreitende Digitalisierung als großes Problem für die Zukunft. Eine detaillierte Analyse zur veränderten Bedrohungslandschaft aufgrund der Digitalisierung ist nicht vorhanden. [34]

Die Bedrohungen von neuen Technologien, wie 5G, Künstliche Intelligenz, intelligente Verkehrssysteme und elektronische Registerkassen, werden in eigenen Unterkapiteln behandelt sowie Maßnahmen und Projekte dazu beschrieben. [34]

BSI - Empfehlungen

Um Empfehlungen oder Bewertungen abzugeben, untersucht das BSI in jedem Kapitel den dazu passenden Sachverhalt. Dabei ist die Initiative von Behörden oder Unternehmen, mit dem BSI zusammenzuarbeiten, wichtig, um besser Erfahrungen aus dem Sachverhalt zu gewinnen. Die Empfehlungen leitet das BSI aus realen Angriffen und Sachverhalten aus. Zum Beispiel leitet das BSI aus zwei verschiedenen Ransomware-Angriffen zwei verschiedene Empfehlungen ab, in diesem Fall fehlende Backups und fehlendes Notfallmanagement. Obwohl der Angriffsvektor gleich ist, wurde vom BSI je Sachverhalt und Defizit eine andere Empfehlung ausgesprochen. [34]

BSI - Besonderheiten

Da der BSI die Aufgabe hat, Deutschland digital sicher zu machen, erhält das BSI in Deutschland direkt Informationen von staatlichen und privatwirtschaftlichen Quellen und dessen Zusammenarbeit. [34]

5.1.3. MELANI

Der Halbjahresbericht 2020/1 [78] der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cybervorfällen der ersten Jahreshälfte 2020 in der Schweiz und international. Im aktuellen Bericht wird als Schwerpunktthema die Corona-Pandemie beleuchtet, die als Lockmittel für zahlreiche Cyberangriffe gedient hat. Der Bericht wurde im Oktober 2020 veröffentlicht.

MELANI - Struktur

Der Bericht der MELANI fängt mit einem Schwerpunktthema an. In diesem Fall ist die Corona-Pandemie der Schwerpunkt. Danach folgt die Bedrohungslandschaft, die nach Angriffsvektoren aufgeteilt wird. Am Ende folgen eigene Kapitel zu Forschung, Ausblick und publizierten MELANI Produkten. [78]

MELANI - Methodologie und Quellen

Da der Schwerpunkt ein aktuelles Ereignis behandelt, werden Quellen von Nachrichtenmeldungen und Blogs von großen Sicherheitsunternehmen verwendet, wie zum Beispiel cybercrimepolice.ch [111], das von der Kantonspolizei Zürich verfasst wird. [78]

Für die Bedrohungslandschaft verwendet MELANI Quellen vom Schweizer National Cyber Security Centre (NCSC). Das NCSC ist in der schweizerischen Eidgenossenschaft das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Zusätzlich werden auch Informationen vom Swiss Government Computer Emergency Response Team [112] verwendet. Als Quellen werden nicht nur eigene Informationen verwendet, sondern auch von renommierten Nachrichtenseiten, wie zdnet.com, heise.de, bleepingcomputer.com, itnews.com, washingtonpost.com, wsj.com, abc.net oder bloomberg.com, und lokalen Nachrichtenseiten, wie srf.ch, rts.ch oder swissinfo.ch. Für detaillierte Analysen werden die Blogs direkt von Sicherheitssoftwareanbietern, wie trendmicro.com, kaspersky.com, proofpoint.com, crowdstrike.com, fireeye.com, barracuda.com, bitdefender.com oder vom eigenem GovCert verwendet. Für Statistiken werden eigene Quellen von NCSC, Schweizer Nachrichtendienst des Bundes oder GovCert und internationalen Organisationen, wie der amerikanischen Cybersecurity and Infrastructure Security Agency (CISA), Verteidigungsministerium der Vereinigten Staaten, National Security Agency National Security der USA oder Ministerium für auswärtige Angelegenheiten in Israel verwendet. [78]

MELANI - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. Die Bedrohungslandschaft für den Industriesektor ist vorhanden. Zum Beispiel werden die neuen Bedrohungen und Risiken für die Bereiche Strom- und Wasserversorgung analysiert, da durch Ransomwareangriffe die industriellen Kontrollsysteme und Sicherheits- oder Management-Software zum Stillstand gekommen sind. In den restlichen Kapiteln zu den Angriffsvektoren sind die am meisten betroffenen Sektoren mit aufgelistet, wenn es Informationen dazu gab. [78]

MELANI - Threat Agents

Im Kapitel Spionage liegt der Fokus auf Threat Agents. Dabei wird über die aktivsten Hackergruppen und über ihre Methoden, Ziele und Motive berichtet. „Hack-for-Hire“ hat dabei ein eigenes Unterkapitel. Zum Beispiel wurden nicht nur finanzielle Motive für die Enthüllung der gestohlenen Daten genannt, sondern auch ideellen Gründe. Dabei wurde auf den Angriff von 200 amerikanischen Polizeidienststellen hingewiesen, die vermutlich im Zuge der Anti-Rassismus-Proteste gegen die Polizei in den USA verübt worden ist. [78, 113]

Der Bericht stellt Statistiken und Grafiken zu den beliebtesten Ransomwareprogramme zur Verfügung und beschreibt den Modus Operandi von Ransomware Angriffen sehr detailliert von der Infektion bis zur Verbreitung und Lösegeldforderung. Für die Ereignisse vor der Infektion ist zusätzlich eine Grafik über den Modus Operandi von Malwareversand nach Telefonanrufen vorhanden. [78]

MELANI - Angriffsvektor

Die Statistiken der Angriffsvektoren werden, inklusive den False-Positive Meldungen an das NCSC, veröffentlicht. Der Bericht [78] unterteilt die Bedrohungslandschaft in folgende Angriffsvektoren:

- Schadsoftware
- Angriffe auf Websites und –dienste
- Industrielle Kontrollsysteme
- Schwachstellen
- Datenabflüsse
- Spionage
- Social Engineering und Phishing
- Präventive Maßnahmen und Strafverfolgung

In den jeweiligen Kategorien beschreibt der Bericht die Angriffsvektoren sehr ausführlich. Dabei bezieht der Bericht sich auf reale Angriffe. Eine Einstufung oder Priorisierung der Angriffsvektoren wird nicht aufgestellt. [78]

MELANI - Prognosen

Im Kapitel „Ausblick und Tendenzen der Lage“ versucht der Bericht, eine Prognose für zukünftige Bedrohungen und Gefahren durchzuführen. Aufgrund der pandemischen Situation und erhöhter Remotearbeit sieht der Bericht zukünftig einen großen Zuwachs von Bedrohungen im Bereich Clouds, Remotezugriffen und Arbeit auf privaten Geräten. [78]

Am Ende unterstreicht der Bericht die Wichtigkeit von der Mitgliedschaft der Schweiz bei internationalen Organisationen wie der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) oder der UNO Gruppe „Group of Government Experts“, um internationale Normen und Prinzipien im Cyberraum zu präzisieren und Debatten zur Digitalisierung sowie dessen Governance zu führen. [78]

MELANI - Empfehlungen

Für Empfehlungen gibt es kein eigenes Kapitel, jedoch wird am Ende eines Kapitels oder Unterkapitels zu einem gewissen Thema immer eine Empfehlung, Hinweis oder Schlussfolgerung gelistet. Es sind technische und organisatorische Empfehlungen vorhanden. Zum Beispiel wird für die DoS-Angriffe die Etablierung eines Risikomanagementsystem empfohlen. [78]

MELANI - Besonderheiten

Das Schwerpunktthema ist eine Besonderheit des Berichts. Da MELANI halbjährlich erscheint, gibt es die Möglichkeit, ein sehr aktuelles Thema zu behandeln. Bei der Analyse zu den neuesten Bedrohungen verlässt sich MELANI auf öffentlich verfügbare Quellen. Zusätzlich liefert der Bericht spezifische Informationen zu Bedrohungen, die spezielle Angriffe auf die Bevölkerung durchführen. Zum Beispiel stellte der Bericht einen Screenshot zur Verfügung, indem Angreifende sich als schweizerische öffentliche Einrichtungen ausgegeben und Malware als Excel-Dateien mitgeliefert haben. Am Ende der Sektion werden Empfehlungen bezüglich des Angriffs beschrieben, wie das System komplett neu zu installieren, nachdem es durch Malware infiziert worden ist. [78]

5.1.4. Bericht BKA Österreich

Der „Bericht Cybersicherheit 2020“ [79] vom BKA wird jährlich in Zusammenarbeit mit anderen Ministerien veröffentlicht. Ziel des Berichtes ist eine Zusammenfassung der größten Bedrohungen und Entwicklungen der Cybersicherheit im vergangenen Jahr. Grundlage sind Berichte der einzelnen Ministerien zur Thematik.

Die österreichische Strategie für Cybersicherheit legt fest, dass durch die Cyber Sicherheit Steuerungsgruppe ein jährlicher Bericht zur Cybersicherheit in Österreich erstellt wird. [79]

Bericht BKA Österreich - Struktur

Der Bericht unterteilt die Bedrohungslage in vier Unterkapitel. Im ersten Unterkapitel wird die Bedrohungslage auf operativer Ebene analysiert. Im zweiten Unterkapitel wird die Bedrohungslage für Unternehmen und kritische Infrastruktur analysiert. In den letzten zwei Unterkapiteln wird speziell über Cybercrime und Bedrohungslage für die Landesverteidigung berichtet. [79]

Das nächste große Kapitel „Internationale Entwicklung“ handelt von internationalen und politischen Gremien und Foren, in denen sich Österreich beteiligt. Diese Gremien und Foren reichen vom Europarat bis hin zum OSZE und NATO. In diesem Kapitel werden die Zuständigkeiten und die Zusammenarbeit mit den internationalen Gremien und Foren beschrieben. [79]

Danach folgt das Kapitel „Nationale Akteure“ in denen alle nationalen Einrichtungen, wie das Abwehramt oder GovCERT, im Bereich Cybersicherheit aufgelistet. Dieses Kapitel beinhaltet Aufgaben, Zuständigkeiten und Projekte der nationalen Einrichtungen. Zusätzlich sind im Kapitel „Nationale Strukturen“ die nationalen Verbände, wie das CERT-Verbund Austria und Austrian Trust Circle, beschrieben. [79]

Im Kapitel „Cyberübungen“ werden Übungen beschrieben, die mit der Zusammenarbeit von nationalen oder internationalen Organisationen, stattgefunden haben. Zum Beispiel wurde die Cyberübung „Thors Hammer 2019“ beschrieben, die in Australien ausgetragen worden ist. [79]

Am Ende des Berichts wird eine Zusammenfassung und ein Ausblick getätigt. Die Ereignisse des Jahres 2019 werden zusammengefasst und potenzielle neue Bedrohungen vorgestellt. [79]

Bericht BKA Österreich - Methodologie und Quellen

Beobachtungszeitraum ist das Jahr 2019, einzelne aktuelle Entwicklungen im Jahr 2020 haben Eingang gefunden. Der aktuelle Bericht Cybersicherheit 2020 baut auf den Inhalten des letztjährigen Berichtes auf und ergänzt diesen um aktuelle Entwicklungen mit Fokusthemen in den Bereichen internationale und operationelle Entwicklungen. [79]

Für diesen Bericht wurden Befragungen an private Unternehmen aus der Cybersecurity-Branche durchgeführt. Die Befragten geben an, einen Zuwachs von allen Angriffsvektoren und Motivationsfaktoren zu beobachten. [79]

Bericht BKA Österreich - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [79]

Für die jeweiligen Größen der Unternehmen sind Statistiken zu den Vorfallsarten beschrieben. Zum Beispiel zeigen die Statistiken an, dass kleine Unternehmen weniger von DoS Angriffen betroffen sind als mittlere und große Unternehmen. [79]

Bericht BKA Österreich - Threat Agents

Einen Anstieg von Angriffen sieht der Bericht bei Threat Agents mit monetären oder staatlich-strategisch Motiven. Der Bericht erkennt auch die Bedrohungen, die von den Kompromittierungen der Supply-Chains ausgehen kann. Im Unterkapitel „Lage Cybercrime“ gibt der Bericht an, dass die polizeiliche Kriminalstatistik in dem Feld um etwa 50% gestiegen ist. [79]

Der Bericht beschreibt, dass APTs sowohl für die öffentliche Verwaltung als auch für Unternehmen in Österreich eine permanente Bedrohung darstellen. Dabei verweist der Bericht auf Angriffe von APT-Gruppen auf die EU-Delegation oder auf ein Netzwerk, welches von EU-Mitgliedstaaten gemeinsam genutzt wird. [79]

Bericht BKA Österreich - Angriffsvektor

Der Bericht behandelt bestimmte Angriffsvektoren in eigenen Kapiteln, wie Emotet, Ransomware, DoS, Schwachstellen, Advanced Persistent Threats (APTs) und Leaks von Zugangsdaten. Zu den beliebtesten Angriffsvektoren 2019 gehören jedoch Phishing, Ransomware und CEO-Fraud. [79]

In jedem Unterkapitel werden Angriffsvektoren beschrieben. Zum Beispiel wird im Unterkapitel „Lage Cybercrime“ Social Engineering als maßgeblicher Angriffvektor definiert. [79]

Bericht BKA Österreich - Prognosen

Im Kapitel „Cyberlage/Bedrohung“ werden Entwicklungen und Trends in der IT-Sicherheitsbranche analysiert. Der Bericht gibt an, dass Trends wie IoT oder Artificial Intelligence gegenüber der Cloud-Thematik mit deutlichem Abstand zurückfallen. Zusätzlich nimmt der Bericht an, dass die Angreifer in der Zukunft öfter Angriffe durchführen, die eine Kombination aus automatisierten und manuellen Elementen sind. Der Bericht sieht auch den Trend zur automatisierten Personalisierung von Angriffen. [79]

Am Ende des Berichts wird ein Ausblick aufkommende Bedrohungen, wie zum Beispiel 5G, und ausstehende Projekte zu dem Thema erläutert. [79]

Bericht BKA Österreich - Empfehlungen

Konkrete Empfehlungen aufgrund der vorherrschenden Bedrohungslage sind nicht vorhanden. [79]

Bericht BKA Österreich - Besonderheiten

Zwei Drittel des Berichts nimmt die Erläuterung von internationaler und nationaler Zusammenarbeit, sowie die Beschreibung der Aufgaben und Schnittpunkte nationaler Gremien und Verbände ein. Einer der Arbeitsgruppen ist die Zusammenarbeit zwischen CERT.at und GovCERT Austria. Dabei betreibt CERT.at und GovCERT Austria das aktive Community Management. Der Austrian Trust Circle ist eine Initiative von CERT.at und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur. Der nationale österreichische CERT-Verbund verbessert die Zusammenarbeit zwischen den österreichischen CERTs sowie die Förderung der CERT-Aktivitäten in Österreich. Ein flächendeckendes Netz an kooperierenden CERTs ist das wirksamste Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. [79]

5.1.5. Internet-Sicherheit Österreich

Der Bericht zur Internet-Sicherheit Österreich 2020 [80] von CERT.at und GovCERT Austria fasst die wichtigsten Themen des Jahres zusammen und gibt einen Überblick über die Aktivitäten der Computer Emergency Response Teams (CERT). Neben den Statistiken von CERT.at wird der aktuelle Stand der

politischen Entwicklungen des NIS-Gesetzes beschrieben sowie nationale und internationale Vernetzung und Kooperationen beleuchtet.

CERT.at ist das österreichische nationale CERT und in Kooperation mit dem GovCERT Austria und Bundeskanzleramt in Österreich. GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung in Österreich. [80]

Internet-Sicherheit Österreich - Struktur

Am Anfang des Berichts wird über die Public-Private Partnership zwischen CERT.at und GovCERT Austria berichtet. Zusätzlich wird auch die Aufgabenverteilung und Erfolge aus der Partnerschaft erläutert. [80]

Die Beschreibung der Bedrohungslandschaft fängt mit einer Statistik zu den Incident Reports, Incidents und Investigation an. Danach folgt eine ausführliche Beschreibung der verwendeten Taxonomie. Für die Klassifizierung von Incidents stützt sich Cert.at dabei auf die eCSIRT II Taxonomy [114]. Mithilfe der Taxonomie werden im Kapitel „2020 im Detail“ die erhobenen Daten und Statistiken präsentiert. Anschließend folgt die Erklärung der Methodologie und Quellenerhebung vom Bericht. Am Ende des Kapitels werden im Unterkapitel „Bedrohungen 2020“ die größten Bedrohungen erläutert. [80]

Das nächste Kapitel beschreibt die Arbeit und Projekte mit den Kooperationspartner. Am Ende wird der aktuelle Stand des Netz- und Informationssicherheitsgesetzes berichtet. [80]

Internet-Sicherheit Österreich - Methodologie und Quellen

Die Daten werden einerseits von CERT.at bzw. GovCERT Austria direkt erhoben und stammen andererseits von diversen externen Quellen. Bei einer eigenen Erhebung werden Suchmaschine wie shodan.io [115] oder Google verwendet. Bei einer Erhebung von externen Quellen wird auf die Daten von der Shadowserver Foundation [116] und Spamhaus [117] zurückgegriffen. Auch Archive von Defacement-Zielen, wie zone-h.org [118], werden verwendet. Zusätzlich erhält der Bericht Daten aus internationalen und nationalen CERTs. Kommerzielle IT-Firmen wie Microsoft oder Ermittlungsbehörden geben ebenfalls Daten an CERT.at weiter. [80]

Internet-Sicherheit Österreich - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [80]

Internet-Sicherheit Österreich - Threat Agents

Der Bericht formuliert keine speziellen Threat Agents. [80]

Internet-Sicherheit Österreich - Angriffsvektor

Die Informationen über die Angriffsvektoren sind in verschiedene Unterkapitel verteilt. Malware ist im Kapitel „2020 im Detail“ zu finden und die restlichen Angriffsvektoren unter „Bedrohungen 2020“. Unter Malware werden die beliebtesten Malware Programme aufgelistet. Insgesamt werden folgende Angriffsvektoren behandelt [80]:

- Malware
- Ransomware
- Emotet
- Vergessene Updates
- Leaks

Eine Einstufung oder Priorisierung der Angriffsvektoren wird nicht aufgestellt, jedoch werden die beliebtesten Incident Kategorien des jeweiligen Monats des Berichtszeitraumes präsentiert, dies sind Abusive Content, Phishing, Malicious Code, Vulnerable und Defacement. [80]

Internet-Sicherheit Österreich - Prognosen

Eine konkrete Prognose, Ausblick oder Fazit nicht vorhanden. [80]

Internet-Sicherheit Österreich - Empfehlungen

Konkrete Empfehlungen aufgrund der vorherrschenden Bedrohungslage sind nicht vorhanden. Obwohl die Hauptaufgabe von CERT.at und GovCERT Austria darin besteht, koordinierend zu unterstützen, gibt es jedoch seltene und besondere Fälle, in denen Hinweise oder Empfehlungen gegeben worden sind. [80]

Internet-Sicherheit Österreich - Besonderheiten

Die transparente Methodologie und Taxonomie ist eine Besonderheit des Berichts. Der Bericht hat ein eigenes Kapitel über die verwendete Datenbasis, erläutert im Detail die Zusammenarbeit mit anderen CERTs und gibt sogar die verwendeten Befehle konkret an. [80]

5.2. Cybersicherheits-Unternehmen

Diese Arbeit beinhaltet die CTI Landscapes aus diversen Cybersicherheits-Unternehmen. Die Berichte sind von Unternehmen, die Sicherheitssoftware entwickeln und verkaufen, wie Sophos [35] und Crowdstrike [36], sowie Unternehmen, die IT-Security Dienstleistungen anbieten, wie Bulletproof [119], NTT [120, 121], KPMG [122] und PwC [123].

5.2.1. Sophos

Sophos ist ein Entwickler und Verkäufer von Sicherheitssoftware, der sich auf Virenschutz, Datenschutz und Malware spezialisiert hat. Ziel seines Berichts [35] ist es, die Kunden bestmöglich auf den neuesten Stand der Bedrohungslandschaft zu bringen, um ihre Cybersicherheit optimal aufrüsten zu können.

Sophos - Struktur

Der Bericht beginnt mit einer Executive Summary und danach folgen vier Hauptteile. Das erste große Kapitel handelt von, Ransomware und wohin sich diese Bedrohung entwickelt. Danach folgt eine Analyse über die häufigsten Angriffe, mit denen große Unternehmen konfrontiert sind. Ein weiteres Fokusthema ist die Auswirkung der globalen Pandemie auf die Informationssicherheit. Am Ende werden über weitere Angriffsflächen auf bestimmte Plattformen berichtet. [35]

Sophos - Methodologie und Quellen

Der Bericht deckt Themenbereiche ab, die sich aus den Erkenntnissen der SophosLabs zur Malware- und Spam-Analyse sowie der Sophos Rapid Response-, Cloud Security- und Data Science-Teams im Berichtszeitraum ergeben hat. Da Sophos als hauptsächliche Arbeit seine Kunden schützt, haben sie einen Einblick in die aktuelle Bedrohungslandschaft. [35]

Sophos - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [35]

Sophos - Threat Agents

Die Methoden und Herangehensweise der Threat Agents werden in den jeweiligen Kapiteln konkret beschrieben. Zum Beispiel wird im Kapitel von Ransomware beschrieben, welche Tools, Terminal-Befehle und Cloud Technologien die Angreifer verwenden. Dabei ist die Beschreibung sehr konkret und technisch. Es werden nur eigene Quellen verwendet. [35]

Sophos berichtet ebenfalls über die Methoden und Herangehensweisen von anderen Unternehmen, die von Ransomware oder ähnlichen Angriffen betroffen sind. Sopohs gibt an, dass allein im letzten Quartal vom Berichtszeitraum die durchschnittliche Lösegeldauszahlung um 21 % gestiegen ist. Die durchschnittliche Lösegeldauszahlung im angesprochenen Quartal beläuft sich auf umgerechnet 233.817,30 US-Dollar. 2019 lag die durchschnittliche Auszahlung noch bei 84.116 Dollar. [35]

Wie detailliert Sophos über die Methoden und Herangehensweisen von Threat Agents berichtet, wird im folgenden Beispiel ersichtlich: Einer der häufigsten Malware-Typen ist der Loader. Loader verfügen über Funktionen, die darauf ausgerichtet sind, eine andere Malware-Payloads im Namen ihrer Betreiber oder von Personen, die einen Vertrag mit ihren Betreibern abgeschlossen haben, zu liefern. Die Malware-Familien Dridex und Zloader sind beide ausgereifte, etablierte Loader-Plattformen. Angreifer nutzen sowohl Dridex als auch Zloader, um Informationen über das Zielsystem zu sammeln und diese an die Kriminellen zurückzusenden, die dann nach eigenem Ermessen entscheiden können, welche Komponenten oder Payloads sie auf der Grundlage der vom Bot zurückgesendeten Informationen ausliefern werden. Die Hauptfunktion des Dridex-Loaders besteht darin, seinen Command-and-Control-Server zu kontaktieren, eine oder mehrere verschlüsselte Payloads abzurufen und sie zu verteilen. Zum Beispiel über ein verstecktes Fernsteuerungsanwendung oder einen SOCKS-Proxy. Diese Payloads geben Angreifern die Möglichkeit, Dinge im Kontext des Geräts des Benutzers zu tun. [35]

Sophos - Angriffsvektor

Sophos bietet Statistiken und persönliche Erfahrungen von den jeweiligen Teams, die mit den Angriffsvektoren direkt in Verbindung gekommen sind. Zum Beispiel wird im Kapitel Ransomware eine detaillierte Vorgehensweise des Sophos Rapid Response Teams bei einen Ransomware Angriff beschrieben. In anderen Kapiteln werden sogar technische Screenshots von Angriffen oder korrupten Dateien geteilt. Je nach Thema werden die dazu beliebtesten Angriffsvektoren präsentiert. Dabei werden fortschrittliche APT Taktiken von Threat Agents als einer der größten Bedrohungen im Jahr 2020 aufgestellt. [35]

Der Bericht von Sophos hat stark veränderte Angriffsvektoren während des Berichtszeitraums erkannt. Da Arbeitnehmer wegen der Pandemie plötzlich nicht mehr an ihren Arbeitsplatz konnten, aber weiterhin auf die Ressourcen innerhalb ihrer Unternehmensumgebung zugreifen mussten, überstieg die schnell wachsende Nachfrage nach virtuellen privaten Netzwerken (VPN) oder anderen vertrauensfreien Einrichtungen die vorhandenen Ressourcen. Zusammen mit den VPNs mussten die Unternehmen neue Firewalls und andere Sicherheitsanwendungen einführen. Dies war die erste große Welle. [35]

Sophos berichtet, dass diese Unternehmen schnell erkannten, dass die Mitarbeiter keine privaten Geräte von zu Hause aus für den Zugriff auf das VPN verwenden sollten, und der schwindende Vorrat an neuen Laptops stellte die Unternehmen vor eine neue Herausforderung. Aufgrund des Mangels an physischen Rechnern wendeten sich die Unternehmen vorerst den virtuellen Maschinen zu, um den Bedarf an einem sicheren Computerarbeitsplatz zu decken. Damit begann die zweite Welle - die Welle der virtuellen Desktops. [35]

Die unterschiedlichen Wellen haben ihre eigenen Herausforderungen im Berichtszeitraum gebracht. Jedoch brachte jede Welle ihre eigenen Risiken und Gefahren. Zum Beispiel hat Sophos festgestellt, dass die meisten Sicherheitsvorfälle mit virtuellen Maschinen in der Cloud auf zwei Hauptursachen zurückzuführen sind: gestohlene oder gefälschte Anmeldedaten oder Fehlkonfigurationen, die zu Sicherheitsverletzungen führten. [35]

Sophos - Prognosen

Prognosen werden vereinzelt am Ende der Fokusthemen gegeben. Eine konkrete Auflistung oder Trends sind nicht vorhanden. [35]

Sophos - Empfehlungen

Konkrete Empfehlungen aufgrund der vorherrschenden Bedrohungslage sind nicht vorhanden. [35]

Sophos - Besonderheiten

Der Bericht von Sophos sticht durch seine sehr technische und detaillierte Darstellung der Bedrohungslandschaft heraus. Dabei werden die Namen und Tools der Angreifer genau beschrieben und auch Screenshots von Codes und korrupten Dateien geteilt. [35]

5.2.2. Bulletproof

Bulletproof betreibt ein hauseigenes Security Operations Centre (SOC) in Großbritannien. Der jährliche Bericht [119] bietet Einblicke, warum Unternehmen Schwierigkeiten haben, mit der aktuellen Bedrohungslandschaft Schritt zu halten, sowie globale Herausforderungen im Cybersecurity Sektor.

Bulletproof - Struktur

Der Bericht beginnt mit einer Executive Summary und informativen Grafiken, welche die wichtigsten Punkte des Dokuments zusammenfassen. Danach folgen die größten Schwachstellen und Risiken. Darauf folgt das „Threat Protection & Intelligence“ Kapitel, in der aus Sicht des SOCs die größten Bedrohungen aufgelistet werden. Das nächste Kapitel „Compliance & Data Protection“ behandelt organisatorische Risiken und Diskrepanzen. Am Ende folgt eine weitere Zusammenfassung und „Final Thoughts“, wobei letztere einen Ausblick über zukünftige Herausforderungen geben. [119]

Bulletproof - Methodologie und Quellen

Bulletproof gibt an, dass dieser Bericht fast ausschließlich auf Originaluntersuchungen unter Verwendung anonymisierter Daten von Bulletproofs Cybersicherheit, Compliance- und Datenschutz-Services sowie auf den Erfahrungen der Mitarbeiter bei der Verwaltung und Erbringung der Dienstleistungen basiert. Das Security Information and Event Management (SIEM) System von Bulletproof bearbeitet eine Milliarde an Daten jeden Tag. Zusätzlich betreibt das Unternehmen Honeypots, um mehr Informationen über Angreifer sammeln zu können. [119]

Die restlichen Quellen bezieht Bulletproof von einer Cyber Security Breaches Studie aus Großbritannien. Ein paar technische Quellen werden von Sicherheitsunternehmen wie cloudfare.com und w3techs.com bezogen. Beim Zitieren von Nachrichten verwendet das Unternehmen bekannte Quellen wie wired.co.uk und theregister.com. [119]

Bulletproof - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [119]

Für die Sektoren Internettechnologien, professionelle Dienstleistungen und Finanzen werden die größten Bedrohungen aufgelistet. Für den Sektor Internettechnologien ist schwache Kryptografie der größte Angriffsvektor. Für den Sektor professionelle Dienstleistungen sind fehlerhafte Zugangskontrollen der größte Angriffsvektor. Für den Sektor Finanzen sind veraltete und anfällige Komponenten der größte Angriffsvektor. [119]

Bulletproof - Threat Agents

Bulletproof gibt an, über 9.000 bösartige IP-Adressen identifiziert haben, dabei gibt das Unternehmen an, dass chinesische IP-Adressen den größten Teil ausmachen. Zusätzlich hat Bulletproof mehrere Honeypots aufgestellt, um mehr Informationen über Angreifer und ihre Herangehensweise zu erhalten. Dabei haben sie die beliebtesten Kommandozeilen und „Benutzername/Passwort"-Kombinationen ermitteln können. [119]

Bulletproof - Angriffsvektor

Für das Jahr 2020 gibt Bulletproof an, dass die drei größten Schwachstellen veraltete Systeme, SQL Injections und defekte Zugangskontrollen sind. Der Bericht gibt auch weitere Informationen über die Trends und Entwicklungen der Angriffsvektoren über die letzten drei Jahre an. [119]

Bulletproof berichtet, eine erhöhte Forderung nach Sicherheit und Datenschutz in der Lieferkette beobachtet zu haben. Einige Unternehmen übertreiben es mit der Due-Diligence-Prüfung ihrer Lieferanten und stellen hohe Anforderungen an kleinere Unternehmen. Bulletproof berichtet, dass das Scheitern von Unternehmen in der Regel an Sicherheitsrichtlinien, veralteten Systeme und fehlendem Endpunktschutz liegt. [119]

Bulletproof - Prognosen

Im letzten Kapitel wird ein kurzer Ausblick beschrieben, dabei wird Remote Arbeit, Cloud und Compliance als zukünftige Herausforderungen gesehen. [119]

Bulletproof - Empfehlungen

Konkrete Empfehlungen werden nicht ausgesprochen. Nur nach dem Kapitel „Compliance & Data Protection" wird auf das interne Cyber Framework hingewiesen, um umfassende Security Policies im Unternehmen zu etablieren. [119]

Bulletproof - Besonderheiten

Eine Besonderheit des Berichts sind die Informationen und Statistiken der organisatorischen Risiken und Defizite. Zum Beispiel gibt der Bericht an, dass Security Policies die Ursache für die grundlegendsten Probleme waren und dass 77% der DSGVO Verletzungen aufgrund von fehlerhafte Rechteverteilung von Einzelpersonen. [119]

5.2.3. Crowdstrike

Crowdstrike ist ein US-amerikanisches Cybersicherheits-Unternehmen, welches Antivirensysteme für private Endnutzer und Unternehmen anbietet. Zusätzlich bietet das Unternehmen

Bedrohungsinformationen und Unterstützung bei Cyber-Angriffen. Neben den Berichten, die sich auf spezielle Dienste fokussieren, bietet Crowdstrike auch ein allgemeines CTI Landscape [36] an.

Crowdstrike - Struktur

Der Bericht beginnt mit einer Übersicht der Bedrohungslandschaft. Danach folgt ein Kapitel, das sich auf Ransomware fokussiert. Die nächsten Kapitel beschreiben die Trends der Angriffsvektoren und ein ganzes Kapitel ist den Threat Agents gewidmet. Am Ende werden die wichtigsten Erkenntnisse zusammengefasst. [36]

Crowdstrike - Methodologie und Quellen

Das Crowdstrike Team verfolgt 131 Angreifer aller Art, einschließlich staatlicher eCrime-Hacker und Hacktivisten. Das Team analysiert TTPs, um detaillierte Informationen zu sammeln und effektive Maßnahmen gegen neue Bedrohungen zu ermöglichen. Die Produkte von Crowdstrike liefern dafür die Informationen. Crowdstrike korreliert und analysiert Petabytes an Echtzeit- und historischen Daten, die von über drei Billionen Ereignissen pro Woche in 176 Ländern verarbeiten. Crowdstrike verwendet das MITRE ATT&CK framework für die Beschreibung der TTPs. [36]

Wenn der Bericht auf Ereignisse oder Aussagen verweist, dann werden keine Quellen genannt, sondern nur erwähnt, dass man sich auf öffentlich verfügbare Quellen bezieht. [36]

Crowdstrike - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [36]

Crowdstrike - Threat Agents

Im Ransomware Kapitel liefert Crowdstrike die Ergebnisse aus den Untersuchungen über die Herkunft von dieser Art der Malware. Dabei stößt Crowdstrike auf kriminelle Organisationen, die ihre Ransomware als Ransomware-as-a-service (RaaS) verkaufen. Dabei listet Crowdstrike nicht nur die wirtschaftlich erfolgreichste Ransomware auf, sondern auch, welche Sektoren von welcher Ransomware am öftesten angegriffen wird. [36]

Im Kapitel „Big Game Hunters“ nimmt Crowdstrike spezielle kriminelle Organisationen ins Visier, analysiert ihre Entwicklungen und beschreibt ihre Angriffskampagnen. Auch in den anderen Kapiteln werden detailliert die Methoden und Tools der Angreifer beschrieben. Von Staatszugehörigkeit, Angriffstempo, Nicknames, entwickelten Tools, Beziehungen zu anderer Malware und Angriffen ist alles in diesem Bericht dokumentiert. [36]

CrowdStrike verfolgt zahlreiche gezielte Einbruchsversuche auf der ganzen Welt. Die meisten gemeldeten Angriffe waren laut Crowdstrike Vorfälle, die mit russischen Angreifern in Verbindung gebracht werden konnten. In den weiteren Kapiteln beschreibt Crowdstrike die Angreifer von bestimmten Ländern und berichtet über ihre Kampagnen. Die Länder, die dabei im Fokus sind, sind Iran, Nordkorea, China und Russland. [36]

Crowdstrike - Angriffsvektor

Am Anfang des Berichts liefert Crowdstrike Statistiken zur Malware und der unterschiedlichen Verteilung der Malware Angriffe je nach Region. Zum Beispiel hat in Lateinamerika Malware eine höhere Quote als andere Angriffsvektoren. [36]

Crowdstrike verwendet die MITRE ATT&CK TTPs Matrix, um eine Heat Map von der Häufigkeit der

beobachteten Angriffe zu erstellen. Wenn das Crowdstrike Team eine gezielte eCrime- oder staatlich gesponserte Einbruchskampagne analysiert, verwendet es die MITRE ATT&CK-Matrix als Rahmen, um Verhalten des Gegners zu kategorisieren. Die folgende Abbildung ist eine Heatmap von gezielten eCrime Aktivitäten und staatlich gesponserten Eindringlingen im Jahr 2019. Das Crowdstrike Team hat die Telemetriedaten aller anvisierten Eindringlinge, die durch ihre Bedrohungsjagd aufgedeckt wurden, verwendet. [36]

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials From Web Browsers
Spear-phishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files
Spear-phishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry
Spear-phishing via Service	Execution Through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access
Supply Chain Compromise	Execution Through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-factor Authentication Interception
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification	
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets	
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass	
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification	
	Space After Filename	Launchctl	SID-History Injection	Hidden Files and Directories	
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users	
	Trap	Local Job Scheduling	Sudo	Hidden Window	
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL	
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection	
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking	
	Windows Remote Management	Modify Existing Service		Indicator Removal From Tools	
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host	
		New Service		Indirect Command Execution	
		Office Application Startup		Install Root Certificate	
		Path Interception		InstallUtil	
		Plist Modification		Launchctl	
		Port Knocking		LC_MAIN Hijacking	
		Port Monitors		Masquerading	
		PowerShell Profile		Modify Registry	
		Rc.common		Mshta	
		Re-opened Applications		Network Share Connection Removal	
		Redundant Access		NTFS File Attributes	
		Registry Run Keys / Startup Folder		Obfuscated Files or Information	
		Scheduled Task		Parent PID Spoofing	
		Screensaver		Plist Modification	
		Security Support Provider		Port Knocking	
		Server Software Component		Process Doppelgänging	
		Service Registry Permissions Weakness		Process Hollowing	
		Setuid and Setgid		Process Injection	
		Shortcut Modification		Redundant Access	
		SIP and Trust Provider Hijacking		Regsvcs/Regasm	
		Startup Items		Regsvr32	
		System Firmware		Rootkit	
		Systemd Service		Rundll32	
		Time Providers		Scripting	
		Trap		Signed Binary Proxy Execution	
		Valid Accounts		Signed Script Proxy Execution	
		Web Shell		SIP and Trust Provider Hijacking	
		Windows Management Instrumentation Event Subscription		Software Packing	
		Winlogon Helper DLL		Space After Filename	
				Template Injection	
				Timestomp	
				Trusted Developer Utilities	
				Valid Accounts	
				Virtualization/Sandbox Evasion	
				Web Service	
				XSL Script Processing	

Frequency of Observance
0-5% of intrusions
5-20%
20-50%
50-70%
>70%

Abbildung 8 - MITRE ATT&CK Heat Map of Tactics and Techniques [36]

Im nächsten Kapitel präsentiert Crowdstrike Statistiken zu den am meisten gemeldeten Bedrohungen. Zu den größten Bedrohungen gehört Ransomware, Banking Trojans und Malware Downloader, wie zum Beispiel Emotet. [36]

Im nächsten Kapitel werden die beliebtesten Methoden der Angreifer präsentiert [36]. Dazu gehören

- die Überlistung von SIEM und Endpoint Protection
- DNS-Tunneling
- Verwendung von kompromittierten Websites
- Dropper, die eigenständig Computerviren freisetzen
- E-Mail Thread Hijacking

Crowdstrike - Prognosen

Am Ende der Kapitel wird ein kleiner Ausblick durchgeführt. Die weiterzunehmende Monetarisierung von Tools und Malware sieht Crowdstrike als ein großes Problem für die Zukunft. Bei der Analyse von bestimmten kriminellen Organisationen sieht Crowdstrike den Trend immer größere Unternehmen und Organisationen anzugreifen. Zusätzlich sieht Crowdstrike den Trend, dass Threat Agents ihre Angriffe immer gezielter ausführen und spezifischer werden. [36]

Crowdstrike - Empfehlungen

Bei der Analyse von der Malware der kriminellen Organisation liefert Crowdstrike am Ende technische Details, wie ihre Produkte die Methoden erkennen können und liefern allgemeine Empfehlungen, wie zum Beispiel die Nutzung von komplexen Passwörtern oder Multifaktor Authentifizierung. [36]

Bei der Zusammenfassung am Ende des Berichts werden wieder weitere Empfehlungen für die wichtigsten Bedrohungen abgegeben. Für Social Engineering Angriffe werden Awareness Programme empfohlen. Für raffinierte Angreifer wird die „1-10-60 rule“ empfohlen, indem Eindringlinge in weniger als einer Minute erkannt, in 10 Minuten die Bedrohung verstanden und in 60 Minuten die Bedrohung eliminiert und eingedämmt wird. Zusätzlich wird eine Partnerschaft mit externen Lösungsanbietern empfohlen, um kritische Talentlücken zu füllen. [36]

Crowdstrike - Besonderheiten

Die Besonderheit dieses Berichts ist der große Fokus auf Angreifende. Crowdstrike bietet detaillierte Informationen über die angreifende Partei, ihre Tools und ihre Methoden. [36]

5.2.4. NTT

NTT Security ist ein Cybersicherheits-Unternehmen in München und bietet Beratungsdienstleistungen, Managed Security Services und technische Lösungen an. NTT Security veröffentlicht jährlich den Global Threat Intelligence Report [120], inklusive einem Executive Guide [121] vom Bericht.

NTT - Struktur

Der Executive Guide ist der Leitfaden für die Führungskräfte. Fokus liegt dabei auf besondere Herausforderungen der Regionen und welche operativen, taktischen und strategischen Überlegungen Unternehmen anstellen sollten, um Risiken zu managen. Zusätzlich möchte NTT, dass Cyber-Sicherheitsverantwortliche diese Informationen nutzen, um identifizierte Bedrohungen mit ihren

Bedrohungen im Hinblick auf ihr eigenes Risikoprofil und ihren technologischen Fußabdruck zu bewerten, um gezielte Maßnahmen zur Erkennung und Bekämpfung von Bedrohungen zu unterstützen. [121]

Ein besonderes Augenmerk legt das Executive Guide dabei auf COVID-19 und in welcher Art es die Bedrohungslandschaft verändert hat. Weiters werden die größten sechs Erkenntnisse des Berichtes geteilt. Im nächsten Kapitel werden Erkenntnisse geteilt, die sich speziell auf Regionen beziehen. Darauf folgen Empfehlungen, die sich auf die vorherigen Kapitel beziehen. Am Ende folgt die Erläuterung der Methodologie. [121]

Der Hauptbericht beginnt mit einer Executive Summary, inklusive einer Zusammenfassung der Empfehlungen. Danach folgt eine Zeitlinie der COVID-19 Pandemie und der darauffolgenden Cyber Angriffe. Anschließend folgt eine globale und auf bestimmte Kontinente abgestimmte Analyse der Bedrohungslandschaft. Im nächsten Kapitel wird über die Cyber-Resilienz geschrieben, dabei wird erläutert, wie ein Unternehmen Secure-By-Design implementieren kann. Darauf folgen die einzelnen Kapitel der jeweiligen Sektoren im Bericht, in der die beliebtesten Angriffstypen, Schwachstellen und Malware gelistet werden. Im nächsten Kapitel wird das Thema „Governance, Risk and Compliance“ behandelt, in der neue Informationen zur Datenschutz-Grundverordnung (DSGVO) und Brexit geteilt werden. Am Ende des Berichts werden alle Ergebnisse des Berichts zusammengefasst. [121]

NTT - Methodologie und Quellen

NTT gibt an, dass die Berichte globale Angriffsdaten von NTT und unterstützenden Betriebsgesellschaften enthalten. Der Berichtszeitraum ist vom 1. Oktober 2018 bis 30. September 2019. Die Analyse basiert auf Log-, Ereignis-, Angriffs-, Vorfall- und Schwachstellendaten von Kunden. Die Nutzung der Indikator-, Kampagnen- und Gegneranalyse aus ihrer Global Threat Intelligence Platform hat maßgeblich dazu beigetragen, Aktivitäten mit Akteuren und Kampagnen in Verbindung zu bringen. [121]

Die Größe und Vielfalt des Kundenstamms, mit über tausenden Kunden verteilt auf sechs Kontinenten, versorgt NTT Ltd. mit Sicherheitsinformationen, die repräsentativ für die Bedrohungen sind, denen die meisten Organisationen ausgesetzt sind. NTT gibt im Executive Guide 4.000 Kunden und im Hauptbericht 10.000 Kunden an. [121]

NTT - Zielgruppe

NTT hat sich für zwei Berichte entschieden, um die Zielgruppen aufzuteilen. Das Executive Guide ist für Führungskräfte und Cyber-Sicherheitsverantwortliche gedacht, während der Hauptbericht die operativen, taktischen und strategischen Aspekte fokussiert. [121]

Im Hauptbericht wird eine Übersicht gegeben, wie sich die veränderte Bedrohungslandschaft durch die COVID-19 Pandemie auf die verschiedenen Sektoren ausgewirkt hat. Dabei liegen Gesundheits-, Finanz-, Industrie-, Verkaufs- und Technologiesektor besonders im Fokus. Am Ende des Berichts haben die jeweiligen Sektoren eigene Kapitel, um näher auf Details eingehen zu können. [121]

Im nächsten Kapitel gibt NTT an, welche Sektoren weltweit am öftesten angegriffen wird. Dabei macht der Technologiesektor mit 25% den größten Teil aus, darauf folgen Behörden und Regierungen mit 16%. Zusätzlich wird über die häufigsten Angriffsvektoren des jeweiligen Sektors berichtet. [121]

NTT - Threat Agents

Der Bericht enthält keine speziellen Statistiken oder weiterführende Analysen zu Threat Agents. [121]

NTT - Angriffsvektor

Im Kapitel „Key Findings“ sind die beliebtesten Angriffsvektoren je nach Sektor aufgelistet. Für den Technologiesektor sind anwendungsspezifische Angriffe mit 31%, Denial of Service (DoS) mit 25 % und Netzwerk-Manipulation mit 13% die beliebtesten Angriffsvektoren. Weitere Statistiken sind für die Finanzbranche, Bildungssektor, Business Dienstleistungen und Behörden sowie Regierungen vorhanden. Darauf folgt eine globale Statistik zu den Angriffsvektoren, in der anwendungsspezifische Angriffe mit 33%, Angriffe auf Webapplikationen mit 22% und DoS mit 14% zu den beliebtesten Angriffsvektoren weltweit gelistet sind. In den nächsten Kapiteln wird über die Angriffsvektoren für die jeweiligen Kontinente, wie Amerika, Asien-Pazifik, Europa, Naher Osten und Afrika berichtet. [121]

NTT - Prognosen

Im Kapitel “Governance, Risk and Compliance” wird über die kommenden Datenschutzverordnungen berichtet, die gerade in der Erstellung sind. Zum Beispiel wird über die California Consumer Privacy Act (CCPA) oder die Brazilian General Data Protection Law (LGPD) berichtet. [121]

NTT - Empfehlungen

Direkt am Anfang des Berichtes [121] ist eine Zusammenfassung der Empfehlung. NTT rät

- eine ausgereifte Secure-By-Design Herangehensweise im Unternehmen zu etablieren,
- informationsgesteuerte Cybersicherheit zu verfolgen,
- die Bedrohungslage zu beobachten und
- Standardisierung von Kontrollen zu fokussieren.

Im Kapitel zur COVID-19 Pandemie folgen viele Empfehlungen für Organisationen, die Auswirkungen der Pandemie zu managen. NTT empfiehlt, den Fokus auf Cybersicherheit, trotz veränderter Arbeitsumgebung, nicht zu vernachlässigen. [121]

Im Kapitel „Cyber-Resilienz“ erklärt NTT sehr detailliert, auf welche Aspekte man achten muss, damit man im Unternehmen erfolgreich ein Secure-By-Design Konzept etablieren kann. Dieses Kapitel ist sehr theoretisch und weist auf das NIST Cybersecurity Framework hin. [121, 124]

NTT - Besonderheiten

Der starke Fokus auf die jeweiligen Sektoren ist eine Besonderheit der Berichte von NTT. In den jeweiligen Kapiteln der Sektoren wird sehr spezifisch die Bedrohungslandschaft dargestellt, inklusive Statistiken. Eine weitere Besonderheit ist die Bedrohungslandschaft hinsichtlich „Governance, Risk and Compliance“, in der nicht nur technische Bedrohungen, sondern auch organisatorische Defizite beachtet werden. [121]

5.2.5. KPMG

KPMG ist weltweit eines der größten Wirtschaftsprüfungs- und Beratungsunternehmen. KPMG Austria bietet Lösungen in den Bereichen Audit, Tax, Advisory und Law. Mit der „Cyber Security Studie 2020“ [122] berichtet KPMG über die wichtigsten Trends aus den Vorjahren und wie gut österreichische Unternehmen auf Cyberangriffe vorbereitet sind.

KPMG - Struktur

Am Anfang des Berichts folgt eine Zusammenfassung und die wesentlichsten Ergebnisse. Im Kapitel „Aug in Aug mit der Gefahr“ wird beschrieben, wie Unternehmen bei Angriffen reagieren. KMPG erwartet, dass

Cyber Security in der Zukunft ein noch wichtigerer Teil des Qualitätsversprechens eines Unternehmens wird. Im nächsten Kapitel „Breit aufgestellt“ wird berichtet, wie sich österreichische Unternehmen auf Cyberattacken vorbereiten. Darauffolgend wird im Kapitel „Mit dem Strom“ die Wünsche der österreichischen Unternehmen vom Staat präsentiert. Am Ende wird die Methode der Umfrage und zukünftige Zusammenarbeit mit KPMG beschrieben. [122]

KPMG - Methodologie und Quellen

Die KPMG Studie berichtet über die Ergebnisse eines Online-Fragebogens von 652 österreichischen Unternehmen in dem Zeitraum von Februar bis März 2020. Die Teilnehmer bestehen aus kleinen und mittleren Unternehmen aus verschiedensten Branchen in Österreich. Der Online-Fragebogen wurde je nach Funktion des Teilnehmers angepasst. Die Ergebnisse wurden von einem KPMG Cyber Security-Expertenteam aus dem Bereich IT-Advisory ausgewertet. Zusätzlich wurde in zwei Round Tables mit Experten die Chancen und Herausforderungen diskutiert. Einmal wurde eine externe Quelle von pionline.com verwendet, die Ergebnisse einer Studie über IT-Budgets präsentiert. [122]

Zusätzlich wurde eine spezielle Umfrage im Oktober 2020 mit 3.249 Teilnehmern zum Thema COVID-19 durchgeführt. [122]

KPMG - Zielgruppe

Der Bericht hat keine Inhalte für eine spezielle Zielgruppe definiert. [122]

KPMG - Threat Agents

Der Bericht enthält keine speziellen Statistiken oder weiterführende Analysen zu Threat Agents. [122]

KPMG - Angriffsvektor

Explizite Informationen oder Statistiken zu Angriffsvektoren werden nicht definiert. [122]

KPMG - Prognosen

Prognosen finden in jedem Kapitel des Berichts statt. Am Anfang werden Prognosen und neue Trends analysiert, welche durch die veränderte Bedrohungslandschaft durch die COVID-19 Pandemie und fortschreitende Digitalisierung verstärkt wird. Im nächsten Kapitel werden weitere Prognosen zur veränderten Bedrohungslandschaft durch COVID-19 Pandemie und der Digitalisierung aus der Sicht eines Vorstandsmitglieds von einem der größten Elektrizitätsversorgungsunternehmen in Österreich durchgeführt. [122]

Im Kapitel „Breit aufgestellt“ wird aus der Sicht eines österreichischen Unternehmens dargestellt, wie aus der kontinuierlichen Beobachtung der Bedrohungslandschaft und Gefährdungsanalysen Maßnahmen zur Stärkung der Verteidigungsfähigkeit abgeleitet werden können. [122]

KPMG - Empfehlungen

KPMG liefert Empfehlungen durch Interviews von österreichischen Unternehmen. KPMG berichtet zum Beispiel, wie 7% der befragten Unternehmen ihren Dienstleistern in Sachen Sicherheit vertrauen. Die Empfehlung eines CISOs von einem österreichischen Unternehmen ist es, klare Sicherheitsvorgaben zu erstellen und regelmäßig die jeweiligen Dienstleistungen zu messen. Zusätzlich wird empfohlen Schulungsmaßnahmen in Bezug auf Informationssicherheit durchzuführen, hinzukommend weil diese Maßnahmen die Grundlage für jede gute Cybersicherheits-Strategie ist. [122]

KPMG - Besonderheiten

Die Besonderheit des Berichts von KPMG sind die praxisnahen Empfehlungen von der Perspektive österreichischer Unternehmen. [122]

5.2.6. PwC

PwC Österreich ist weltweit einer der größten Wirtschaftsprüfungs- und Beratungsunternehmen. PwC Österreich bietet branchenspezifische Dienstleistungen und hat Kunden von dem öffentlichen Sektor, Banken sowie lokal und global führende Unternehmen. [123]

PwC - Struktur

Der Bericht beginnt mit fünf Kapiteln, die jeweils die zentralen Forderungen widerspiegeln. [123]

- Im ersten Kapitel soll die Cybersicherheits-Strategie neu aufgesetzt und die Unternehmensführung weiterentwickelt werden.
- Im zweiten Kapitel soll das Cyber-Budget überdenkt werden, um es optimal zu nutzen.
- Im dritten Kapitel soll in jeden Vorsprung investiert werden, um mit Angreifern gleichzuziehen.
- Im vierten Kapitel soll eine Resilienz für jedes Szenario aufgebaut werden.
- Im fünften Kapitel soll das Sicherheitsteam zukunftssicher gemacht werden.

Am Ende des Berichts folgen weitere Details zur Erhebung der Daten und weitere Statistiken zur Demographie der Umfrage. [123]

PwC - Methodologie und Quellen

Der Bericht ist eine Umfrage von 3.249 Führungskräften aus dem Wirtschafts- und Technologiesektor, die im Juli und August 2020 durchgeführt wurde. Die Befragten sind 34 % in Westeuropa, 29 % in Nordamerika, 18 % in Asien-Pazifik, 8 % in Lateinamerika, 4 % in Osteuropa, 3 % in Naher Osten und 3 % in Afrika. [123]

Die Global Digital Trust Insights Umfrage ist formell bekannt als „Global State of Information Security Survey“. PwC Research, PwCs globales Centre of Centre of Excellence für Marktforschung und Insights, führte diese Umfrage durch. [123]

Zusätzlich wurde im Bericht auf „The Global Risks Report 2020“ [125] vom WEF hingewiesen. Der Bericht weist auch auf Nachrichten- und Magazinportale hin, um auf den Mangel von Cybersicherheits-Fähigkeiten hinzuweisen, wie zum Beispiel csoonline.com, securitymagazine.com und cybersecurityventures.com. [123]

PwC - Zielgruppe

Die Zielgruppe des Berichts sind CISO, die eine strategische Perspektive auf die Bedrohungslandschaft benötigen. [123]

PwC - Threat Agents

Der Bericht gibt im vierten Kapitel Statistiken zu den Threat Agents. Dabei wurden die Teilnehmer der Umfrage gebeten, die Threat Agents ihrer Meinung nach auf Auswirkung und Eintrittswahrscheinlichkeit zu bewerten. Dabei haben die Teilnehmer angegeben, dass Hacktivisten und Cyber Kriminelle größere Auswirkungen auf das Unternehmen haben als ehemalige Mitarbeiter. [123]

PwC - Angriffsvektor

Der Bericht gibt im vierten Kapitel an, dass die Teilnehmer der Umfrage meinen, dass Angriffe auf Cloud Dienste, Störsoftware und Ransomware am wahrscheinlichsten sind. Zusätzlich wurde den WEF Bericht [125] hingewiesen, welcher Desinformationsangriffe, Bedrohungen gesponsert von Nationalstaaten und Angriffe von Wettbewerbern, als wesentliche Bedrohungen auflistet. [123]

PwC - Prognosen

Durch die Auswertung der Umfragen sieht PwC den Trend, dass Unternehmen mehr Erfolge im Bereich Risikomanagement, Ausfallsicherheit, Vertrauen der Stakeholder und digitale Transformation haben. PwC sieht den Trend weg von statischen, inhärent unsicheren Legacy-Systeme zugunsten von dynamischeren, flexibleren und integrierten Cloud-/Netzwerksystemen, die Secure-By-Design sind. [123]

PwC - Empfehlungen

Beim Präsentieren der Umfrageergebnisse werden am Ende der jeweiligen Kapitel Empfehlungen definiert. Im ersten Kapitel wird empfohlen, auf eine geschäftsorientierte Cybersicherheits-Strategie zu setzen, um das Cyber-Budget neu festzulegen, in neue Sicherheitslösungen zu investieren, neue Pläne zur Ausfallsicherheit zu planen und seine neue Sicherheitsorganisation zu verbessern. [123]

Im zweiten Kapitel wird empfohlen sich nicht auf die Kostenseite von Cybersicherheit zu fokussieren, sondern Cybersicherheit in jede Geschäftsentscheidung einzubinden. Im dritten Kapitel wird empfohlen, auf Zero Trust Architekturen, Real-Time Threat Intelligence, Security Orchestration and Automation, Advanced Endpoint Protection und Identity and Access Management zu setzen. Zusätzlich wird empfohlen, bei der Umstellung zur Cloud auf automatisierte Hygienemechanismen zu setzen. [123]

Im vierten Kapitel wird empfohlen, eine gute Cyber-Hygiene zu haben, um Bedrohungen abzuwehren. Der Bericht sieht große Fortschritte dabei, dass Unternehmen Talente und Werkzeuge aufbauen, die Daten in Echtzeit nutzen, um Bedrohungen zu erkennen und darauf reagieren zu können. Im fünften Kapitel empfiehlt der Bericht aufgrund des Mangels an Cybersicherheits-Talenten die Fähigkeiten der aktuellen Mitarbeiter zu verbessern und von innen heraus einzustellen. Zusätzlich empfiehlt der Bericht auf professionelle Managed-Services zu setzen. [123]

PwC - Besonderheiten

Die Besonderheit des Berichts von PwC ist die globale Verteilung der Teilnehmer. Über 3.249 Teilnehmer aus der ganzen Welt und aus den verschiedensten Sektoren haben bei dieser Umfrage mitgemacht. [123]

6. Evaluation

In diesem Kapitel wird mit den ausgewählten CTI Landscapes von Kapitel 5 und der Methode aus Kapitel 4 eine Evaluation durchgeführt. Die Inhalte der CTI Landscapes werden bewertet, Besonderheiten unterstrichen und die Mustertabelle beantwortet.

6.1. Regierungsstellen

Angefangen wird die Evaluation mit den CTI Landscapes von Regierungsstellen.

6.1.1. ENISA

Gleich zu Beginn erwähnt der Bericht die größte Änderung – die neue Struktur. ENISA geht weg von einer langatmigen und statischen Art von Berichten. Mit seiner neuen visuellen Identität und seinem neuen Format soll der Bericht zu einem vielseitigen, dynamischen und einfach zu bedienenden digitalen Bericht geworden sein, der versucht, die Erwartungen eines wachsenden und anspruchsvollen Publikums zu erfüllen. [33]

Mit dieser Struktur bietet ENISA ein CTI Landscape, welches auf Zielgruppe und Zweck der Berichte abgestimmt ist und behebt somit das Problem unspezifischer oder zu allgemeiner Analysen. Die eigene Bedrohungslandschaft zur COVID-19 Pandemie zeigt, dass ENISA in der Lage ist, die Bedrohungslandschaft auf aktuelle Ereignisse anzupassen. [33]

Die Methodologie ist ausführlich beschrieben. Im Vergleich zu den restlichen Berichten von Regierungsstellen listet ENISA alle Quellen auf. Diese Quellen reichen von Expertenkreisen bis hin zu Geheimdienstberichten. Die Quellen stammen somit von eigenen oder von öffentlich zugänglichen Quellen. Die externen Quellen sind ordnungsgemäß und vollständig gelistet. Neben den Daten aus dem Berichtszeitraum, wird auch eine Analyse zu aktuellen Themen wie COVID-19 beschrieben. [33]

Das Einzigartige an ENISAs Bericht [33] ist die hohe Anzahl an weiteren Berichten, jeder Bericht hat eine passende Zielgruppe definiert. Es sind auch Berichte vorhanden, die eigene Bedrohungslandschaften für die Sektoren beschreiben. Dabei wird zwischen strategischen, technischen und generischen Zielgruppen unterschieden. Viele Berichte dieser Arbeit haben keine oder nur einzelne Zielgruppen für ihre Berichte definiert.

Die Motive und die Motivationsfaktoren der Threat Agents werden genau beschrieben. Während Statistiken zu Threat Agents in vielen Berichten dargestellt werden, werden die Motivationsfaktoren in den meisten Berichten, wie PwC oder NTT, nicht berücksichtigt. ENISA verfolgt über Jahre die Trends und Motive von Threat Agents und stellt diese Informationen im Bericht da. [33]

Statistiken zu den Angriffsvektoren sind vorhanden und werden eingestuft sowie mit dem vorherigen Jahr verglichen. Für jeden einzelnen der 15 größten Cyber Threats hat ENISA jeweils einen speziellen Bericht erstellt. Keiner der anderen Berichte in dieser Arbeit gehen dabei so sehr in die Tiefe, wie die speziellen Berichte von ENISA. In diesen Berichten werden Prognosen sowie Trendanalysen der Bedrohungslandschaft und von neuen Technologien durchgeführt. Die Berichte enthalten technische und organisatorische Empfehlungen, sowie spezielle Empfehlungen für Forschungseinrichtungen. [33]

Die Berichte von ENISA [33] gehen sehr in die Tiefe und bieten mit mehreren Berichten zugeschnittene Informationen für die jeweiligen Zielgruppen. Die Berichte von ENISA erfüllen somit nicht nur alle Anforderungen, um von Unternehmen als Basis für die Cybersicherheits-Strategie verwendet zu werden, sondern die Berichte haben ebenfalls nützliche Informationen für weitere Zielgruppen, wie zum Beispiel Forschungseinrichtungen.

ENISA - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
ENISA	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	12

Tabelle 6 - Bewertung ENISA

6.1.2. BSI

Der Bericht [34] verwendet direkte Informationen aus staatlichen und privatwirtschaftlichen Quellen. Die zweite Hälfte fokussiert sich weniger auf die Bedrohungslandschaft, sondern erläutert mehr die Aufgaben, Projekte und Zusammenarbeit mit anderen Unternehmen, die das BSI in dem Berichtzeitraum durchgeführt hat.

Die Methodologie wird ordentlich beschrieben. Besonders ist dabei das Model des gesellschaftlichen Dialogs, da nicht nur die Nachvollziehbarkeit von der Erstellung des Berichts gegeben ist, sondern auch die Auswahl der Themen oder Zusammenarbeit mit anderen Stakeholdern. Das Quellenverzeichnis am Ende des Berichts ist vollständig und strukturiert vorhanden. [34]

Die Inhalte für Zielgruppen und Sektoren sind in Kapitel unterteilt. Neben den Daten aus dem Berichtszeitraum wird auch eine Analyse zu aktuellen Themen wie COVID-19 beschrieben. Der BSI hat zusätzlich die Aufgabe, die Betreiber kritischer Infrastruktur zu prüfen, daher hat der Bericht besonders für diese hilfreiche Informationen zu neuen Erkenntnissen und Projekten in dem Umfeld zu bieten. Der BSI bietet einen sektorspezifischen Überblick zu bieten über die 358 Betriebe, die als kritische Infrastruktur zählen und daher nachweispflichtig gegenüber dem BSI sind. Dieser Überblick unterscheidet den Bericht groß von den anderen Berichten. [34]

Über Threat Agents und ihre Motivationsfaktoren wird berichtet. Der Fokus des Berichtes [34] lag dabei bei APT Gruppen. Diesen Fokus haben Berichte wie MELANI, Sophos und „Bericht BKA Österreich“ ebenfalls. Die Beschreibung der Angriffsvektoren findet nur über die Anzahl der Angriffe statt, jedoch findet keine Auflistung oder Priorisierung der Angriffsvektoren statt.

Am Ende des Berichts fehlt eine konkrete Prognose in die Zukunft, nur ein allgemeiner Ausblick ist festzustellen. Über neue Technologien wird berichtet. Die technischen und organisatorischen Empfehlungen werden sehr praxisnah und je nach Sachverhalt beschrieben. Für Unternehmen, die Lösungen und Empfehlungen je nach realen Ereignissen oder Vorfällen benötigen, ist der Bericht von BSI [34] ideal.

BSI - Fragen

Die Fragen werden wie folgt beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden NICHT beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird NICHT durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
BSI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	10

Tabelle 7 - Bewertung BSI

6.1.3. MELANI

MELANI [78] wird halbjährlich veröffentlicht, dadurch ist es in der Lage aktuelle Themen zu behandeln. Das Schwerpunktthema des Berichts ist die veränderte Bedrohungslandschaft hinsichtlich der COVID-19 Pandemie.

Die Methodologie des Berichts wird nicht beschrieben, jedoch sind die Quellen gelistet und nummeriert. MELANI hat als einziger Bericht nicht ihre Methodologie geteilt. Die fehlende Transparenz könnte sich negativ auf die Vertrauenswürdigkeit und Nachvollziehbarkeit des Berichts auswirken. Da MELANI zusätzlich Informationen aus dem NCSC teilt, bietet es wie die restlichen Berichte von Regierungsstellen eine Übersicht über die Sicherheitsmeldungen im Berichtszeitraum. [78]

Eine Zielgruppe, wie bei den Berichten von BSI [34] oder ENISA [33], wird explizit nicht definiert. Dies könnte daran liegen, dass in der Schweiz keine Meldepflicht für kritische Infrastrukturen existiert, im Gegensatz zu europäischen Staaten. Der Austausch zu Cybervorfällen bei kritischen Infrastrukturen wie Energieversorgung, Telekommunikation oder Finanz- und Versicherungswesen erfolgt nur auf einer freiwilligen Basis über MELANI. [126]

Über die Motive und Werkzeuge von Threat Agents wird berichtet. Dabei werden im Bericht nicht nur die Threat Agents speziell für die Region analysiert, sondern auch Angriffe weltweit oder von Nachbarn wie Österreich. Dabei sind die analysierten Angriffe auf Österreich in MELANI aktueller als im Bericht „Bericht BKA Österreich“, da der Bericht halbjährlich erscheint. Die Angriffsvektoren erhalten eigene Kapitel und Statistiken zu den beliebtesten Angriffsvektoren werden veröffentlicht, zum Beispiel über Phishing. Am Ende des Berichts werden Prognosen über zukünftige Bedrohungen gestellt. Die Empfehlungen finden immer am Ende der jeweiligen Kapitel statt und sind von technischer und organisatorischer Natur. [78]

MELANI - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist NICHT beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind NICHT explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird NICHT durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
MELANI	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	10

Tabelle 8 - Bewertung MELANI

6.1.4. Bericht BKA Österreich

Der jährliche „Bericht Cybersicherheit 2020“ [79] vom BKA und der Cyber Sicherheit Steuerungsgruppe soll eine zusammenfassende Darstellung der Cyber-Bedrohungen und wesentlicher nationaler und internationaler Entwicklungen darstellen.

Die Methodologie wird kurz und prägnant erläutert. Zum größten Teil werden eigene Quellen verwendet, jedoch sind Informationen aus externen Quellen ebenfalls aufgeführt. Der größte Unterschied dieses Berichts ist, dass er Informationen über das Jahr 2019 enthält, während die restlichen Berichte aktueller sind. Hauptgrund dafür ist, dass der Bericht der älteste von den vorhandenen Berichten ist. Dadurch schafft es der Bericht auch nicht, aktuelle Themen wie COVID-19 zu berücksichtigen. Genau wie der BSI Bericht [34] fokussiert sich dieser Bericht mehr darauf, über die Projekte und Verantwortungsbereiche der öffentlichen Organisation zu behandeln. [79]

Explizit ist keine Zielgruppe definiert, jedoch sind Informationen je nach Unternehmensgröße beschrieben. Das ist für Unternehmen sinnvoll, die wissen möchten, ob ihre Firma mit wenigen Mitarbeitern denselben Gefahren gegenübersteht, wie Unternehmen mit einer hohen Anzahl an Mitarbeitern. [79]

Über Threat Agents und Angriffsvektoren wird berichtet. Zusätzlich findet eine Beschreibung mit Statistiken statt. Der Bericht stellt nicht nur Grafiken zur Verfügung, sondern befragt Cybersicherheits-Unternehmen oder Betreiber kritischer Infrastruktur nach ihren Cybersichereitsmaßnahmen. Prognose werden durchgeführt und die Auswirkung neuer Technologien analysiert. Im gesamten Bericht werden weder technische noch organisatorische Empfehlungen gegeben. [79]

Genau wie der Bericht vom BSI [34] ist ein großer Teil die Dokumentation von Kooperationen mit anderen Organisationen, Projekten oder Auflistung von Verantwortlichkeiten. Für Personen, die einen Überblick von den staatlichen Organisationen haben möchten, die sich mit Cybersicherheit auseinandersetzen, ist der Bericht ideal. „Internet-Sicherheit Österreich“ verfolgt eine ähnliche Struktur, jedoch weniger detailliert und die beiden Berichte überschneiden sich in ihrer Berichterstattung. [79]

Bericht BKA Österreich - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind NICHT explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden NICHT gegeben.
- E2: Technische UND organisatorische Empfehlungen werden NICHT gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
Bericht BKA Österreich	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	9

Tabelle 9 - Bewertung Bericht BKA Österreich

6.1.5. Internet-Sicherheit Österreich

Der Bericht [80] ist sehr strukturiert und transparent in seiner Beschaffung der Daten und Erläuterung der Datenbasis. Jedoch enthält der Bericht neben der Beschreibung der Bedrohungslandschaft eine Auflistung von Kooperationen oder Projekten. Die Zusammenarbeit mit Kooperationspartnern ist detailliert

beschrieben und hat ein eigenes Kapitel. Die Hauptaufgabe von CERT.at und GovCERT Austria besteht darin, koordinierend zu unterstützen. Jedoch gibt es seltene und besondere Fälle, in denen CERT.at und GovCERT Austria Hinweise oder Empfehlungen gegeben haben. Diese Hinweise oder Empfehlungen werden jedoch nicht im Bericht zusammengefasst. Zum Beispiel wird beschrieben, wie sich Emotet Malware verbreitet, jedoch nicht wie sich Unternehmen davor schützen können. Dasselbe gilt für den Ransomware Beitrag. [80]

Die Methodologie ist klar und die Quellen sind angegeben. Der größte Unterschied des Berichtes [80] ist, dass sogar die Kommandos für die Informationsgewinnung detailliert beschrieben sind und daher maximale Nachvollziehbarkeit bieten. Als zentrale Meldestelle liefert dieser Bericht ebenfalls, wie MELANI [78] und BSI [34], Informationen über Meldungen von Cybersicherheitsvorfällen.

Der Bericht [80] hat, im Gegensatz zu den Berichten von den anderen Regierungsstellen, explizit keine Zielgruppe definiert und keine Bedrohungen für spezielle Sektoren gelistet. Über Threat Agents oder ihre Motivationsfaktoren wird ebenfalls nicht berichtet. Damit ist dieser Bericht der Einzige von den Berichten der Regierungsstellen, der keine Informationen zu Threat Agents oder ihren Motivationsfaktoren darstellt. Aus der Gruppe der Cybersicherheits-Unternehmen haben nur die zwei Studien von KPMG und NTT ebenfalls keine Informationen zu Threat Agents berichtet.

Informationen und Statistiken zu Angriffsvektoren werden geteilt. Trotz der fehlenden Einstufung oder Priorisierung der Angriffsvektoren erhält die Leserschaft einen Leitfaden über die Bedrohungsumgebung und Angriffsvektoren. Jedoch sind eine konkrete Prognose, Ausblick oder Fazit nicht vorhanden. Empfehlungen werden nicht gegeben. Verglichen mit den restlichen Berichten erfüllt dieser Bericht die wenigsten Anforderungen. [80]

Internet-Sicherheit Österreich - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind NICHT explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist NICHT vorhanden.
- T1: Über Threat Agents wird NICHT berichtet.
- T2: Über die Motivationsfaktoren wird NICHT berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird NICHT durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird NICHT beschrieben.
- E1: Empfehlungen werden NICHT gegeben.
- E2: Technische UND organisatorische Empfehlungen werden NICHT gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
Internet-Sicherheit Österreich	Ja	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	4

Tabelle 10 - Bewertung Internet-Sicherheit Österreich

6.2. Cybersicherheits-Unternehmen

Als nächstes werden die CTI Landscapes von Cybersicherheits-Unternehmen evaluiert.

6.2.1. Sophos

Der Bericht [35] beschreibt sehr technisch detailliert die Bedrohungslandschaft mit Fokusthemen zu COVID-19 und Ransomware. Die Executive Summary fasst die wichtigsten Punkte der Bedrohungslandschaft einfach zusammen. Diese Zusammenfassung ist besonders bei Berichten wichtig, die auf den technischen Aspekt fokussiert sind.

Die Methodologie wird in der Executive Summary prägnant dargelegt und Sophos verwendet hauptsächlich eigene Quellen. Ein positives Merkmal des Berichts sind die Analysen und Informationen von SophosLabs, obwohl verglichen zu den restlichen Berichten keine explizite Zielgruppe für die Inhalte oder eine Aufteilung von Sektoren vorhanden ist. [35]

Die Tools und Herangehensweise von Threat Agents werden detailliert behandelt, jedoch fehlen die Motivationsfaktoren. Angriffsvektoren und ihre Statistiken werden beschrieben. Die größte Stärke des Berichts [35] ist die Beschreibung der Herangehensweise der Threat Agents und die Analyse der Angriffsvektoren. Verglichen mit den Berichten von BSI [34] oder MELANI [78] beschreibt Sophos den Modus Operandi mit Screenshots und Beispielcode.

Eine Prognose oder die Bedrohungslandschaft von neuen Technologien wird nicht behandelt. Konkrete Empfehlungen werden nicht abgegeben. [35]

Sophos - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind NICHT explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist NICHT vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird NICHT berichtet.
- A1: Über Angriffsvektoren wird berichtet.

- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird NICHT durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird NICHT beschrieben.
- E1: Empfehlungen werden NICHT gegeben.
- E2: Technische UND organisatorische Empfehlungen werden NICHT gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
Sophos	Ja	Ja	Nein	Nein	Ja	Nein	Ja	Ja	Nein	Nein	Nein	Nein	5

Tabelle 11 - Bewertung Sophos

6.2.2. Bulletproof

Der Bericht von Bulletproof [119] setzt viel auf leicht verständliche Grafiken und stellt Informationen zu Angriffsvektoren übersichtlich da. Jedoch zielt der Bericht mehr darauf ab, Werbung für ihre neuen Produkte und Lösungen zu machen, als hilfreiche Empfehlungen weiterzugeben. Zum Beispiel werden im Kapitel „Compliance & Data Protection“ Bedrohungen aus organisatorischer Sicht betrachtet, jedoch ist die Empfehlung, das neue Cyber Essentials Framework von Bulletproof zu verwenden, ohne auf Details einzugehen.

Die Methodologie und Quellen sind beschrieben. Der Bericht von Bulletproof [119] fällt durch die Executive Summary und einfachen Grafiken auf, die am Anfang des Berichts sind. Die Berichte von Crowdstrike [36] und PwC [123] setzen am Anfang auf ein kurzes Vorwort, aber nicht auf eine Zusammenfassung der Bedrohungslage. Die Executive Summary fasst die wichtigsten Punkte der Bedrohungslandschaft einfach zusammen und bietet leicht verständliche Grafiken.

Der Bericht [119] gibt keine klare Zielgruppe bekannt, jedoch ist eine kleine Aufteilung von Sektoren vorhanden. Die Aufteilung ist klein, da nur der beliebteste Angriffsvektor von drei verschiedenen Sektoren geteilt wurde. Die Statistiken der Threat Agents werden geteilt, jedoch wird nicht über Motivationsfaktoren berichtet.

Über die Angriffsvektoren sind viele Grafiken und Statistiken vorhanden. Das Besondere an dem Bericht [119] ist, dass spezielle Bedrohungen aus organisatorischer Sicht beschrieben werden. Ganz im Gegensatz dazu sind die restlichen Berichte von Cybersicherheits-Unternehmen, wie die von Sophos [35] oder Crowdstrike [36], welche oft den organisatorischen Aspekt keine große Bedeutung zuweisen.

Eine Prognose über die veränderte Bedrohungslandschaft wird durchgeführt, jedoch werden die neuen Technologien dazu nicht beschrieben. Empfehlungen wurden nicht ausgesprochen, lediglich auf eigene Dienstleistungen und Produkte hingewiesen. [119] Auch der Bericht von Sophos [35] vernachlässigen Empfehlungen und verweisen auf eigene Services. Der Bericht von Crowdstrike [36] präsentiert auch eigene Service, jedoch bieten sie weiterhin Empfehlungen.

Bulletproof - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit NICHT definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird NICHT berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird NICHT beschrieben.
- E1: Empfehlungen werden NICHT gegeben.
- E2: Technische UND organisatorische Empfehlungen werden NICHT gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
Bulletproof	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Nein	7

Tabelle 12 - Bewertung Bulletproof

6.2.3. Crowdstrike

Der große Fokus des Berichts liegt auf Threat Agents. Das zeigt, wie unterschiedlich die Fokuspunkte der Verfassenden von CTI Landscapes sein kann. Von der detaillierten Methodologie bis zur Verwendung des MITRE ATT&CK framework für die Beschreibung der TTPs ist Crowdstrike sehr fokussiert auf die Threat Agents.

Die Methodologie ist sehr detailliert beschrieben, jedoch werden keine Quellen genannt, sondern nur erwähnt, dass man sich auf öffentlich verfügbaren Quellen bezieht. Damit ist der Bericht von Crowdstrike der einzige Bericht [36] dieser Arbeit, welcher keine Quellen listet. Dies macht die Nachvollziehbarkeit der beschriebenen Bedrohungslandschaft für Lesende sehr schwer.

Zielgruppen sind explizit nicht definiert, jedoch werden die verschiedenen Sektoren in die Berichterstattung eingebunden. Den größten Teil des Berichts machen die Informationen über Threat Agents aus. Der Bericht von Crowdstrike [36] beschreibt die Threat Agents am detailliertesten. Der Bericht von Sophos [35] beschreibt die Threat Agents zwar auch sehr detailliert, wie zum Beispiel durch eine Beschreibung der verwendeten Tools und Technologien, jedoch hat der Bericht von Crowdstrike [36] eigene Kapitel zu den verschiedenen Sektoren und Ländern, in denen die Threat Agents operieren. Dies gibt einen globalen Überblick über die Angreifenden und ihre beliebtesten Methoden.

Die Informationen über Angriffsvektoren sind gegeben und Statistiken werden geteilt. Im Vergleich zu den restlichen Berichten hat Crowdstrike [36] als einziger eine Heat Map von der MITRE ATT&CK-Matrix erstellt. Die Matrix stellt die Häufigkeit der beobachteten Angriffe dar.

Eine Prognose über die veränderte Bedrohungslandschaft wird durchgeführt, jedoch werden die neuen Technologien dazu nicht beschrieben. Technische und organisatorische Empfehlungen werden weitergegeben. [36]

Crowdstrike - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind NICHT gelistet.
- Z1: Zielgruppen sind explizit NICHT definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird NICHT beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
Crowdstrike	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	9

Tabelle 13 - Bewertung Crowdstrike

6.2.4. NTT

NTT beschreibt die Bedrohungslandschaft mit zwei Berichten [120, 121], die auf unterschiedliche Zielgruppen ausgerichtet sind. Die Methodologie der beiden Berichte ist identisch, nur die Anzahl der Clients ist unterschiedlich, dabei dürfte es sich jedoch um einen Tippfehler handeln.

Die Methode ist ausführlich am Ende der Berichte beschrieben. Die Quellen sind gelistet. Während die Berichte von Bulletproof [119] und Sophos [35] die Executive Summary am Anfang des Berichts beschrieben haben, hat NTT als einziges Cybersicherheits-Unternehmen die Executive Summary in einen eigenen Bericht erfasst. Dadurch verliert NTT die Vorteile einer kurzen Übersicht, jedoch verschafft es neue Möglichkeiten, eine organisatorische Perspektive einzubinden. Zum Beispiel beschreibt die Executive Summary die Empfehlungen speziell für strategische Themen und Governance, während der zweite Bericht technische Empfehlungen teilt. Dadurch verfügen beide Berichte über technische und organisatorische Empfehlungen. [120, 121]

Die Zielgruppen sind definiert und eine Aufteilung von Sektoren ist vorhanden. Eine große Stärke des Berichts ist der Fokus auf die Industrien und Sektoren. NTT sind die einzigen Publizierenden in dieser Arbeit, die zu den jeweiligen Sektoren spezielle Empfehlungen bezüglich MITRE ATT&CK abhandeln. [120, 121]

Der Bericht enthält keine speziellen Statistiken oder weiterführende Analysen zu Threat Agents oder ihren Motivationsfaktoren. Über Angriffsvektoren wird berichtet und Statistiken aufgeführt. Genau wie bei den Threat Agents wird auch bei den Angriffsvektoren zwischen den Sektoren und Industrien unterschieden. Im technischen Bericht ist ein eigenes Kapitel zur Cyber-Resilienz und empfohlenen Maßnahmen zu Secure-By-Design zu finden. [120, 121]

Prognosen sind vorhanden und Bedrohungen von neuen Technologien werden beschrieben. Zum Beispiel wird der Trend von IoT Weaponization erläutert. [120, 121]

NTT - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird NICHT berichtet.
- T2: Über die Motivationsfaktoren wird NICHT berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
NTT	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	10

Tabelle 14 - Bewertung NTT

6.2.5. KPMG

Der Bericht [122] der KPMG fällt durch die praxisnahen Empfehlungen auf, die aus der Sicht von österreichischen Unternehmen gestellt werden. Der Bericht präsentiert Ergebnisse eines Online-Fragebogens von Unternehmen in Österreich. Eine explizite Zielgruppe für die Studie wurde nicht definiert. Da die Inhalte einen starken Bezug auf Österreich haben und Diskussion über CERT-Verbünde führen, ist diese Studie für Unternehmen aus Österreich und CERT-Betreiber relevant.

Die Methodologie ist vollständig beschrieben und die Quellen sind gelistet. Im Vergleich zu der Studie von PwC [123] sind die Umfrageteilnehmer vom Bericht der KPMG [122] nicht aus der ganzen Welt, sondern nur aus Österreich. Dies ermöglicht Fragen und Analysen speziell für den österreichischen Markt.

Zielgruppen wurden explizit nicht definiert und eine Aufteilung in Sektoren ist nicht vorhanden. Über Threat Agents und ihre Motivationsfaktoren sind keine Analysen vorhanden. Bei der Beschreibung von Angriffsvektoren werden nur die Ergebnisse der Umfrage präsentiert. Ein Abgleich mit fundierten Informationen zu Angriffsvektoren wird nicht durchgeführt oder ohne die Angabe von Quellen beschrieben. [122]

Prognosen sind in jedem Kapitel vorhanden, jedoch wird die veränderte Bedrohungslage durch neue Technologien nicht beschrieben. Der Bericht verfügt über technische und organisatorische Empfehlungen. Das Besondere an dem Bericht von KPMG ist, dass die Empfehlungen direkt aus der Sicht von österreichischen Unternehmen dargestellt werden. Während die anderen Berichte dieser Arbeit auf theoretische Empfehlungen zurückgreifen, gibt der Bericht von KPMG Empfehlungen von Unternehmen aus erster Hand. [122]

KPMG - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit NICHT definiert.
- Z2: Eine Aufteilung von Sektoren ist NICHT vorhanden.
- T1: Über Threat Agents wird NICHT berichtet.
- T2: Über die Motivationsfaktoren wird NICHT berichtet.
- A1: Über Angriffsvektoren wird NICHT berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden NICHT beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird NICHT beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
KPMG	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	5

Tabelle 15 - Bewertung KPMG

6.2.6. PwC

Der Bericht [123] von PwC ist eine weitere Studie, die jedoch weltweit durchgeführt worden ist. Schon im Vorwort steht, dass der Bericht darauf abzielt, CISO ein strategisches Verständnis über die

Bedrohungslandschaft zu geben. Zudem wird darauf aufmerksam gemacht, dass Cybersicherheit nicht mehr so technologiefokussiert ist.

Die Methodologie ist ausführlich beschrieben und Quellen sind gelistet. Ähnlich wie der Bericht von Crowdstrike [36] analysiert PwC die Bedrohungslage weltweit, jedoch liegt der Fokus dabei nicht auf den Threat Agents, sondern auf den Angriffsvektoren. Der Bericht von PwC [123] teilt auch Informationen über Threat Agents, jedoch nicht über ihre Motivationsfaktoren.

Die Zielgruppe ist definiert, jedoch werden die Informationen nicht in Sektoren aufgeteilt. Von allen Berichten dieser Arbeit ist der Bericht von PwC [123] der Einzige, welcher CISO speziell als Zielgruppe definiert hat. Die Ergebnisse der weltweiten Umfrage sollen CISO einen strategischen Überblick über die Bedrohungslandschaft geben, dabei fällt der Bericht mit 37 Seiten prägnant aus. [123] Im Vergleich dazu ist der Bericht von Sophos [35] ebenfalls kurz.

Bei der Beschreibung der Angriffsvektoren wurden nicht nur die Ergebnisse der Umfrage präsentiert, sondern auch mit Informationen aus externen Quellen, wie dem WEF Bericht [125], abgeglichen. Im Gegensatz dazu steht der Bericht von KPMG [122], welcher keinen Abgleich mit externen Quellen durchführt. [123]

Statistiken zu Angriffsvektoren sind nicht vorhanden. Prognosen werden durchgeführt, jedoch nicht über neue Technologien, welche die Bedrohungslandschaft verändern könnten. Im Bericht sind technische und organisatorische Empfehlungen vorhanden, auch wenn die Empfehlungen kurz und prägnant bleiben. [123]

PwC - Fragen

Die Fragen werden folgendermaßen beantwortet:

- M1: Die Methodologie ist beschrieben.
- M2: Die Quellen sind gelistet.
- Z1: Zielgruppen sind explizit definiert.
- Z2: Eine Aufteilung von Sektoren ist vorhanden.
- T1: Über Threat Agents wird berichtet.
- T2: Über die Motivationsfaktoren wird berichtet.
- A1: Über Angriffsvektoren wird berichtet.
- A2: Statistiken zu den beliebtesten Angriffsvektoren werden NICHT beschrieben.
- P1: Eine Prognose ODER Trendanalyse wird NICHT durchgeführt.
- P2: Die Bedrohungslage von neuen Technologien wird beschrieben.
- E1: Empfehlungen werden gegeben.
- E2: Technische UND organisatorische Empfehlungen werden gegeben.

In tabellarischer Form sehen die Antworten folgendermaßen aus:

	Methodologie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
PwC	Ja	Ja	Ja	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja	Ja	8

Tabelle 16 - Bewertung PwC

6.3. Ergebnis

Am Ende des Kapitels werden die Tabellen zusammengefasst und nach der Bewertung sortiert. Je höher die Bewertung, desto mehr Kriterien hat das CTI Landscape erfüllt.

	Methodo-logie und Quellen-analyse		Zielgruppe		Threat Agents		Angriffs-vektor		Prognose		Empfehlung		Bewer-tung gesamt
	M1	M2	Z1	Z2	T1	T2	A1	A2	P1	P2	E1	E2	
ENISA	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	12
BSI	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	10
MELANI	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	10
NTT	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	10
Bericht BKA Öster-reich	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	9
Crowd-strike	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	9
PwC	Ja	Ja	Ja	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja	Ja	8
Bullet-proof	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Nein	7
KPMG	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	5
Sophos	Ja	Ja	Nein	Nein	Ja	Nein	Ja	Ja	Nein	Nein	Nein	Nein	5
Internet-Sicher-heit Öster-reich	Ja	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein	Nein	4

Tabelle 17 - Zusammengefasste Tabelle aller Bewertungen

7. Diskussion

Diese Arbeit hat die Herausforderungen von CTI Landscapes aufgezeigt und eine Methodik zur Bewertung entwickelt. Die Kriterien der Methodik wurden nach einer tiefgründigen Analyse der Literatur erstellt. Die Analyse eine Auflistung von Kriterien, die einen hohen Stellenwert bei der Erstellung Cybersicherheits-Strategie und Einbindung eines ISMS sowie Risikomanagementsystems haben.

Die Bewertungsmethode hat gezeigt, dass CTI Landscapes bewertet und evaluiert werden können. Entscheidend dabei ist, dass vorher die Anforderungen an die CTI Landscapes klar definiert werden. Die Auswahl der Anforderungen ist mithilfe der Literaturanalyse durchgeführt worden. Die Literaturanalyse bestand nicht nur aus der Untersuchung von bestimmten CTI Landscapes, sondern hat mit dem theoretischen Rahmen eine Grundlage für die Selektion der Kriterien geschaffen.

Das Ergebnis ist eine tiefgründige Analyse und übersichtliche Darstellung von CTI Landscapes, die nach ihrer Bewertung sortiert ist. Dies ermöglicht es Verfassenden von Cybersicherheits-Strategien, eine effiziente und kompakte Auswahl bei der Suche nach ihrer Quelle für die Bedrohungslandschaft zu treffen. Die CTI Landscapes mit der höchsten Bewertung erfüllen die meisten Kriterien. Zusätzlich muss nicht befürchtet werden, dass die Bedrohungslandschaft durch unterschiedliche Perspektiven verzerrt wird. Am Ende muss der Verfassende nur noch eine kompakte Auswahl treffen, da zu viele Empfehlungen von Fachkundigen zu einer uneffektiven Priorisierung führt.

Da nicht alle CTI Landscapes alle Kriterien erfüllt haben, können die Ergebnisse dieser Arbeit von CTI Landscape Verfassenden verwendet werden, um die fehlenden Aspekte in den nächsten Bericht zu integrieren.

7.1. Interpretation der Ergebnisse

Die Ergebnisse zeigen, dass die Berichte von ENISA [33], BSI [34], MELANI [78] und NTT [120, 121] die meisten Kriterien erfüllen, da diese Berichte das Ziel haben, die bestmögliche Übersicht über die Bedrohungslandschaft zu geben und mit Empfehlungen Unternehmen bei der Risikobewältigung zu unterstützen. KPMG [122], Sophos [35] und Internet-Sicherheit Österreich [80] haben die wenigsten Kriterien erfüllt, das liegt vermutlich daran, dass diese Berichte den Fokus auf andere Aspekte hatten.

Die Berichte von Regierungsstellen wie MELANI [78], BSI [34] und Bericht Cybersicherheit Österreich beziehen ihre Informationen hauptsächlich auf die eigenen Länder. Für Unternehmen empfiehlt es sich weiterhin, die CTI Landscapes von dem eigenen Land zu betrachten. Zum Beispiel ist der Bericht von MELANI [78] weiterhin empfehlenswert für Unternehmen aus der Schweiz oder der Bericht von BSI [34] empfehlenswert für deutsche Unternehmen. Für europaweite Unternehmen sind die Berichte von ENISA ideal.

Die Berichte von ENISA [33] haben sich von einem großen Bericht verabschiedet und konzentrieren sich auf mehrere kleineren Berichte. Das gibt ENISA [33] die Möglichkeit, die verschiedenen Berichte auf ihre Zielgruppen zu verteilen. Dies ist besonders für Unternehmen sinnvoll, die CTI strategisch einbeziehen und für die diese kein exklusives Thema für die technische Abteilung ist. Die Berichte von ENISA [33] haben es als einzige Organisation geschafft, alle Aspekte der erstellten Methode zu erfüllen.

Der Bericht von MELANI [78] ist für Unternehmen ideal, welche sehr aktuelle Informationen und Analysen zu Schwerpunktthemen erhalten möchten. Dabei ist der Bericht sehr detailliert, liefert spezifische Empfehlungen und listet die neuesten Bedrohungen bezüglich der Schwerpunktthemen auf.

Im Bericht „Internet-Sicherheit Österreich“ [80] lag der Fokus mehr auf der Berichterstattung eigener Statistiken, gemeinsamen Projekten oder Kooperationen als auf der Darstellung der Bedrohungslandschaft, ähnlich wie beim „Bericht Cybersicherheit 2020“ vom BKA [79]. Jedoch hat der Bericht der BKA [79], dabei die Beschreibung der Bedrohungslandschaft nicht zu sehr vernachlässigt und Prognosen sowie Threat Agents ausführlich beschrieben. Da „Internet-Sicherheit Österreich“ [80] insgesamt die wenigsten Anforderungen erfüllt und die Berichterstattung über Projekte oder Kooperationen

sich überschneiden, wird empfohlen, den „Bericht Cybersicherheit 2020“ dem „Internet-Sicherheit Österreich“ [80] vorzuziehen.

Der Bericht von Sophos [35] ist ideal für Lesende, die viel Wert auf die technische Analyse legen oder an der Herangehensweise der Angreifenden interessiert sind. Besonders für Betreiber von SOCs können die Informationen zu verwendeten Tools, Terminal-Befehlen und Cloud Technologien hilfreich für die Erstellung von Cybersicherheits-Alarmen sein.

Zusätzlich zeigen die Berichte von Sophos [35] und Bulletproof [119], dass es nicht ausreicht, nur Angriffsvektoren oder Methoden von Angreifenden zu beschreiben, sondern auch Empfehlungen und Prognosen dargestellt werden sollten. Beide Cybersicherheits-Unternehmen nutzen die Analysen zu Angriffsvektoren in ihren Berichten, um auf eigene Dienstleistungen oder Produkte hinzuweisen, dabei wird sich mit den Empfehlungen nicht befasst. Diese Aspekte machen für die Verfassenden von Cybersicherheits-Strategien die Analyse von solchen Berichten ineffizient.

Jedoch ist der Bericht von Bulletproof [119] für alle Unternehmen empfehlenswert, die neugierig auf organisatorische Risiken sind und auch aus dieser Perspektive die veränderte Bedrohungslandschaft beobachten möchten.

Der Bericht von Crowdstrike [36] ist für weltweit operierende Unternehmen interessant, welche über die verschiedenen APT Gruppen und ihrer Herangehensweise informiert werden wollen. Dabei bietet Crowdstrike [36] detaillierte Analysen über die APT Gruppen von diversen Kontinenten und teilt dementsprechend die beliebtesten Angriffsmethoden mit.

Zusätzlich ist der Bericht von Crowdstrike [36] für Unternehmen interessant, die für ihre Bedrohungslandschaft ebenfalls das MITRE ATT&CK-Framework verwenden. Für diese Unternehmen hat Crowdstrike [36] eine Heat Map von der Häufigkeit der beobachteten Angriffe erstellt.

Der technische Bericht von NTT [120] enthält ebenfalls Empfehlungen bezüglich MITRE ATT&CK Elemente, jedoch spezifisch auf die verschiedenen Sektoren und Industrien. Verglichen mit den restlichen Berichten fokussiert sich der Bericht von NTT sehr stark auf die Sektoren. Dabei werden Threat Agents und die Angriffsvektoren spezifisch auf die jeweiligen Sektoren getrennt analysiert. Die Executive Summary enthält ebenfalls sektorspezifische Empfehlungen. Die Berichte von NTT [120, 121] sind nicht nur für Anwender des MITRE ATT&CK-Frameworks interessant, sondern auch für Unternehmen, die ausführliche Berichte suchen, welche die Bedrohungslandschaft auf einer organisatorischen und strategischen sowie technischen Perspektive anbietet.

Die Berichte von KPMG [122] und PwC [123] legen eher den Fokus, die Ergebnisse ihrer Studie und Umfrage zu veröffentlichen, als die Bedrohungslandschaft zu beschreiben. Der wesentliche Unterschied zwischen den beiden Berichten und der Hauptgrund für die geringe Bewertung des KPMG Berichts [122] ist, dass der Bericht von PwC [123] die Ergebnisse der Studie um externe Informationen ergänzt, da die Umfrageergebnisse für die Beschreibung der Bedrohungslandschaft alleine nicht ausreichen.

Jedoch ist der Bericht von KPMG [122] für Unternehmen empfehlenswert, welche einen Einblick in die Bedrohungslage von österreichischen Unternehmen erhalten möchten. In diesem Fall werden sehr praxisnahe Empfehlungen und Informationen zu den Angriffsvektoren geliefert.

Im Gegensatz dazu steht der Bericht von PwC [123], welcher für Unternehmen empfehlenswert ist, die an einer weltweiten Studie zur Bedrohungslandschaft interessiert sind. Für diese Unternehmen liefert PwC [123] Analysen zu globalen Angriffen auf Cloud Systeme und weitere Trends.

7.2. Beschränkung der Forschung

Es muss berücksichtigt werden, dass sich diese Forschung mit CTI Landscapes befasst, die sich nicht nur auf eine bestimmte Branche, Trend oder Vorfall spezialisiert haben. Bei Berücksichtigung weiterer spezialisierten CTI Landscapes kommen weitere Aspekte zu, welche die Bewertungsmethode verändern würden. Anhand weiterer Studien mit der Bewertungsmethode und den neuen Aspekten könnte die Auswirkung auf die Bewertungsmethode untersucht werden.

7.3. Empfehlung für weiterführende Forschung

Durch diese Bewertungsmethode wurden CTI Landscapes erfolgreich bewertet und evaluiert. Anhand weiterer Studien mit der Bewertungsmethode und einer Gewichtung von länderspezifischen Aspekten könnte die Evaluierung auch für Unternehmen untersucht werden, die CTI Landscapes von Regierungsstellen aus dem eigenen Land bevorzugen. Dafür macht die Unterteilung in Regierungsstellen und Cybersicherheits-Unternehmen dieser Arbeit den ersten Schritt. Zum Beispiel stellt sich die Frage, ob ein Unternehmen aus der Schweiz den Bericht von MELANI [78] statt dem Bericht vom BSI [34] bevorzugen würde. Die Durchführung von Interviews mit Unternehmen würde die Forschung ergänzen.

8. Fazit

Das Ziel dieser Diplomarbeit war es, herauszufinden, mit welcher Methode CTI Landscapes analysiert und evaluiert werden können. Dabei ist es wichtig herauszufinden welche Kriterien eines CTI Landscapes einen hohen Stellenwert bei der Erstellung einer Cybersicherheits-Strategie haben und welche Anforderungen an die Berichte dadurch gewonnen werden kann.

Dafür wurde zuerst eine theoretische Grundlage für das Thema im Kapitel 2 „Background“ geschaffen. Dabei wurde der Zusammenhang zwischen ISMS, Risikomanagement und CTI Landscapes dargestellt. Danach wurde der aktuelle Stand der Technik erfasst, indem weitere Analysen und die Bedeutung von CTI Landscapes beschrieben worden sind. Bei der Literaturanalyse konnten die Probleme und Herausforderungen von aktuellen CTI Landscapes erfasst werden.

Mithilfe der Literaturanalyse konnte eine fundierte Basis erstellt werden, um im nächsten Kapitel die Anforderungen und Kriterien festzulegen, die bei der Erstellung einer Cybersicherheits-Strategie und eine problemlose Einbindung in das ISMS oder Risikomanagementsystems einen hohen Stellenwert haben. Dadurch wurde eine Zielsetzung dieser Arbeit erreicht: Es wurden nicht nur die Kriterien festgestellt, sondern auch eine Methode zu Bewertung von CTI Landscapes entwickelt. Am Ende des Kapitels wurde eine Methode vorgestellt, die eine tiefgründige Analyse und übersichtliche Darstellung der Bewertung ermöglicht.

Vor der Durchführung der Bewertung wurde zuerst eine Auswahl und Selektion von bestimmten CTI Landscapes durchgeführt. Am Ende der Selektion wurde zwischen zwei Kategorien unterschieden: CTI Landscapes von Regierungsstellen und Cybersicherheits-Unternehmen. Diese CTI Landscapes wurden auf die Kriterien von Kapitel 4 untersucht.

Nach der Entwicklung der Methode und der Auswahl von bestimmten CTI Landscapes wurde eine Evaluation durchgeführt. Dabei wurde die entwickelte Methode auf die ausgewählten CTI Landscapes angewendet, um die wesentlichen Unterschiede der Berichte zum Vorschein zu bringen und eine Bewertung durchzuführen. Das Ergebnis der Bewertung ist eine tiefgründige Analyse und übersichtliche Darstellung von CTI Landscapes, welche die Ergebnisse der Methode listet. Am Ende der Evaluation werden alle Ergebnisse zusammengefasst und nach der Bewertung sortiert. Je höher die Bewertung, desto mehr Kriterien hat der Bericht erfüllt.

Aus den Ergebnissen lässt sich ableiten, dass ENISA aktuell das einzige der geprüften CTI Landscapes dieser Arbeit ist, welches alle Kriterien für die problemlose Verwendung beim Entwickeln einer Cybersicherheits-Strategie erfüllt.

Somit lässt sich die Forschungsfrage folgendermaßen beantworten: Mithilfe der Kriterien, die einen hohen Stellenwert bei der Erstellung einer Cybersicherheits-Strategie haben, konnte die Bewertungsmethode dieser Diplomarbeit die Analyse und Evaluation von CTI Landscapes ermöglichen.

Weiters konnten aus den Ergebnissen die Anforderungen aus aktuellen CTI Landscapes gewonnen werden. Die Ergebnisse ermöglichen es Verfassenden von Cybersicherheits-Strategien, eine effiziente und kompakte Auswahl bei der Suche nach ihrer Quelle für die Bedrohungslandschaft zu treffen.

Durch die Untersuchungen lassen sich neue Erkenntnisse zu CTI Landscapes feststellen. In dieser Arbeit wurde im Kapitel 6 und 7 registriert, wie sich die CTI Landscapes voneinander unterscheiden können. Eine große Erkenntnis ist, dass CTI Landscapes unterschiedliche Schwerpunkte, Perspektiven und Zielgruppen ansprechen. In der Evaluation und Diskussion dieser Arbeit wurden die Unterschiede der aktuellen CTI

Landscapes festgehalten. Diese können nun von Unternehmen verwendet werden, die nach Berichten suchen, welche bestimmte Schwerpunkte, Perspektiven oder Zielgruppen mit einbeziehen möchten.

Weiterführende Forschung könnte die Bewertung der CTI Landscapes aus einer neuen Perspektive mit einbeziehen. Dies könnte beispielsweise die Einbindung von länderspezifischen Aspekten und die Einführung einer Gewichtung sein. Zukünftige Forschung könnte an der Unterteilung von Regierungsstellen und Cybersicherheits-Unternehmen dieser Arbeit anknüpfen und weitere Analysen aus diesem Gesichtspunkt durchführen.

9. Anhang 1

In der folgenden Tabelle werden die exkludierten Berichte dargestellt:

Nr.	Titel
1	ENISA Threat Landscape For 5G Networks Report [127]
2	European Cybersecurity Month 2020 - Deployment Report [128]
3	ECSC 2020 Analysis Report [129]
4	Situational Report On Microsoft Exchange Vulnerabilities [130]
5	EU Cybersecurity Initiatives In The Finance Sector [131]
6	Security In 5G Specifications [132]
7	Cybersecurity Challenges In The Uptake Of Artificial Intelligence In Autonomous Driving [133]
8	2020 Report On CSIRT-LE Cooperation: Study Of Roles And Synergies Among Selected Countries [134]
9	Cloud Security For Healthcare Services [135]
10	Artificial Intelligence Cybersecurity Challenges [136]
11	Sectoral CSIRT Capabilities - Energy And Air Transport [137]
12	Telecom Security During A Pandemic [138]
13	Cybersecurity Stocktaking In The CAM [139]
14	Railway Cybersecurity [140]
15	Guidelines For Securing The Internet Of Things [141]
16	National Capabilities Assessment Framework [142]
17	Industry 4.0 - Cybersecurity Challenges And Recommendations [143]
18	Franco-German Common Situational Picture [81]
19	IT-Sicherheit Im Home-Office Im Jahr 2020 [144]
20	Industrial Control System Security: Top 10 Bedrohungen Und Gegenmaßnahmen V1.3 [145]
21	Register Aktueller Cybergefährdungen Und -Angriffsformen [146]
22	Internet Resilience In France 2015 [147]
23	Controlling The Digital Risk – The Trust Advantage [148]
24	ASEAN Cyberthreat Assessment 2020 [149]
25	Evasive Threats, Pervasive Effects [150]
26	Web Attacks And Gaming Abuse [151]
27	ITRC's 2019 Annual Data Breach Report [152]
28	Cheats, Hacks, And Cyberattacks - Threats To The Esports Industry In 2019 And Beyond [153]
29	The State Of Ransomware [154]
30	A LOOK AT LINUX - Threats, Risks, And Recommendations [155]
31	Malicious Uses And Abuses Of Artificial Intelligence [156]
32	The Hacker Infrastructure And Underground Hosting - An Overview Of The Cybercriminal Market [157]
33	Securing The Pandemic-Disrupted Workplace [158]
34	2019 Mobile Threat Landscape [159]
35	Trend Micro Cloud App Security Report 2019 [160]
36	Cybersecurity Trends 2020 [161]

37	2020 Cybersecurity Landscape [162]
38	Financial Cyberthreats In 2020 [163]
39	5G Security And Privacy For Smart Cities [164]
40	Kids On The Web In 2020 [165]
41	Explicit Content And Cyberthreats: 2019 Report [166]
42	Incident Response Analyst Report 2019 [167]
43	Digital Education: The Cyberrisks Of The Online Classroom [168]
44	An Overview Of Targeted Attacks And Apts On Linux [169]
45	Digital Footprint Intelligence Report [170]
46	The State Of Stalkerware In 2020 [171]
47	COVID-19: Examining The Threat Landscape A Year Later [172]
48	2020 Cyber Threatsacape Report [173]
49	Accenture Adaptive Security [174]
50	Accenture Technology Vision [175]
51	Cyber Risk And Financial Stability [176]
52	Cyber Resilience Oversight Expectations For Financial Market Infrastructures [177]
53	Cyber Risk Surveillance: A Case Study Of Singapore [178]
54	The Global Cyber Threat To Financial Systems [179]
55	Financial Cyber Survey [180]
56	Forces Shaping The Cyber Threat Landscape For Financial Institutions [181]
57	Covid-19 And Cyber Risk In The Financial Sector [182]
58	Cyber Threat Landscape For The Finance Sector [183]
59	2021 Technology Industry Cyber Threat Landscape Report [184]
60	The Cyber Threat Landscape Of The Telecommunications Industry [63]
61	2021 Banking And Financial Services Industry Cyber Threat Landscape Report [62]
62	Beyond Car Hacking: The Cyber Threat Landscape For Automotive Companies [64]
63	The Dark Side Of China: The Evolution Of A Global Cyber Power [185]
64	GDPR Complicates Italy's Cyber Threat Landscape [186]
65	Health Scare: Data Privacy Concerns In The Age Of COVID-19 [187]
66	The Cyber Threat Impact Of COVID-19 To Global Business [188]
67	Gaming, Leisure, & Hospitality Industry Cyber Threat Report [189]
68	Financial Services Threat Landscape Report: The Dark Web Perspective [190]
69	Retail & Ecommerce Threat Landscape Report [191]
70	Cyberthreat Intelligence For Retail & E-Commerce [192]
71	Reinventing Government: 20 Innovations For 2020 [193]
72	Vaulting Cybersecurity Up To The Cloud [194]
73	2019 Mobile Threat Landscape Report [195]
74	2020 Threat Hunting Report [196]
75	Cyber Risk In Retail [197]
76	Deloitte Cyber Security Report [198]
77	2020 Deloitte Cyber Survey [199]
78	Threat Landscape Snapshot Retail [200]
79	Understanding The Mobile Threat Landscape [201]

80	Mobile Telecommunications Security Threat Landscape [202]
81	2020 Threat Landscape Report [203]
82	Demystifying The Threat Landscape [204]
83	Payment-Security-Report [205]
84	National Cyber Threat Assessment 2020 [206]
85	Cyber Threat Landscape Report 2020 Singapore [207]
86	2019 Application Protection Report [208]
87	2020 Phishing And Fraud Report [209]
88	ACSC Annual Cyber Threat Report July 2019 To June 2020 [210]
89	2020 Sector Snapshot: Health [211]
90	The Commonwealth Cyber Security Posture In 2019 [212]
91	Cyber Threat Report 2019/20 [213]
92	CISA 2020 Year In Review [214]
93	CISA Global [215]
94	Election Infrastructure Cyber Risk Assessment [216]
95	Mail-In Voting In 2020 Infrastructure Risk Assessment [217]
96	Cloud Threat Landscape Report 2020 [218]
97	Oracle And KPMG Cloud Threat Report 2020 [219]
98	The State Of Cloud (In)Security [220]
99	Cyber Security Threat Trends 2020 [221]
100	Brace For The Breach - Bdo Cyber Threats Insights [222]
101	2021 Horizon Report [223]
102	2020 Healthcare Threat Landscape [224]
103	New Technologies, New Cyberthreats [225]
104	BaFin Perspectives - Cyber Security [226]
105	Cybersecurity In Automotive [227]

Tabelle 18 - Auflistung der exkludierten Berichte

10. Literaturverzeichnis

[1] K. Namuduri und M. Varanasi, „The chief security officer problem," in *2011 45th Annual Conference on Information Sciences and Systems*, 2011.

[2] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens und M. L. Mazurek, „A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[3] K. M. Caramancion, „An Exploration of Disinformation as a Cybersecurity Threat," in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, Los Alamitos, CA, USA, 2020.

[4] J. R. Langevin, M. T. McCaul, S. Charney und H. Raduege, „Securing cyberspace for the 44th presidency," Washington, DC, 2008.

[5] Interpol, „National Cybercrime Strategy Guidebook," 2021.

[6] H.-J. Kam und P. Katerattanakul, „Diversifying cybersecurity education: A non-technical approach to technical studies," in *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*, 2014.

[7] World Economic Forum, „weforum.org," 4 Februar 2021. [Online]. Available: https://www.weforum.org/events/the-davos-agenda-2021.

[8] World Economic Forum, „The Global Risks Report 2021," World Economic Forum, 2021.

[9] L. Eagle, „Digital Pulse - Coronovirus Flash Survey October 2020," 451Research, 2020.

[10] M. Bartsch und S. Frey, Cyberstrategien für Unternehmen und Behörden: Maßnahmen zur Erhöhung der Cyberresilienz, Springer Fachmedien Wiesbaden, 2017.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI), „ISMS.1: Sicherheitsmanagement," BSI, 2020.

[12] M. A. Dogaheh, „Introducing a framework for security measurements," in *IEEE International Conference on Information Theory and Information Security*, 2010.

[13] A-SIT Zentrum für sichere Informationstechnologie – Austria, „Österreichisches Informationssicherheitshandbuch," 2021.

[14] A-SIT Zentrum für sichere Informationstechnologie – Austria, „onlinesicherheit.gv.at," [Online]. Available: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Sicherheitsmanagement/Informationssicherheits-Managementsystem.html. [Zugriff am 20 07 2021].

[15] R. Sarno und I. Iffano, „Sistem manajemen keamanan informasi berbasis ISO 27001," in *Surabaya: ITSPress*, 2009.

[16] V. Mavroeidis und S. Bromander, „Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017.

[17] OASIS Open, „github.io," [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html. [Zugriff am 25 07 2021].

[18] W. Gibb und D. Kerr, „https://www.fireeye.com/," [Online]. Available: https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html. [Zugriff am 2021 07 10].

[19] IBM Security, „Cost of a Data Breach Report 2019," IBM Security, 2019.

[20] R. Baskerville, P. Spagnoletti und J. Kim, „Incident-centered information security: Managing a strategic balance between prevention and response," in *Information & Management*, 2014.

[21] Kaspersky Lab, „Kaspersky Cybersecurity Services 2018," 2018.

[22] Recorded Future, „recordedfuture.com," [Online]. Available: https://www.recordedfuture.com/threat-intelligence/. [Zugriff am 20 07 2021].

[23] S. E. Dog, A. Tweed, L. Rouse, B. Chu, D. Qi, Y. Hu, J. Yang und E. Al-Shaer, „Strategic cyber threat intelligence sharing: A case study of ids logs," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 2016.

[24] C. P. Pfleeger, Security in computing, Prentice Hall, 2006.

[25] C. Viveros , „Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts," in *Tartu University*, 2016.

[26] C. Johnson, L. Badger, D. Waltermire, J. Snyder und C. Skorupka, „Guide to cyber threat information sharing," in *NIST special publication*, 2016.

[27] R. D. Steele, „Open source intelligence," in *Handbook of intelligence studies*, 2007.

[28] B. Cho, „A System for National Intelligence Activity Based on All Kinds of OSINT (Open Source INTelligence) on the Internet," in *Journal of Information and Security*, 2003.

[29] The MITRE Corporation, „mitre.org," [Online]. Available: https://attack.mitre.org/. [Zugriff am 20 07 2021].

[30] The MITRE Corporation, „MITRE ATT&CK: Design and Philosophy," 2020.

[31] Financial Action Task Force (FATF), „National Money Laundering and Terrorist Financing Risk Assessment," FATF, 2013.

[32] Resilient Energy Platform, „resilient-energy.org," [Online]. Available: https://resilient-energy.org/cybersecurity-resilience. [Zugriff am 22 07 2021].

[33] ENISA, „The Year In Review," ENISA, 2020.

[34] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2020," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020.

[35] Sophos Ltd, „Sophos 2021 Threat Report," 2020.

[36] CrowdStrike, Inc, „2020 Global Threat Report," 2020.

[37] S. Samtani, K. Chinn, C. Larson und H. Chen, „Azsecure hacker assets portal: Cyber threat intelligence and malware analysis," in *2016 IEEE conference on intelligence and security informatics (ISI)*, 2016.

[38] SANS Institute, „The SANS State of Cyber Threat IntelligenceSurvey: CTI Important and Maturing," 2016.

[39] I. Deliu, C. Leichter und K. Franke, „Collecting Cyber Threat Intelligence from Hacker Forums via a Two-Stage, Hybrid Process using Support Vector Machines and Latent Dirichlet Allocation," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018.

[40] R. Brown und R. M. Lee, „2021 SANS Cyber Threat Intelligence (CTI) Survey," 2021.

[41] The Open Group, Technical Standard Risk Taxonomy, Berkshire: The Open Group, 2009.

[42] Accenture & Ponemon Institute LLC, „The Cost Of Cybercrime," Accenture , 2019.

[43] Accenture, „Securing The Digital," Accenture, 2019.

[44] Accenture, „Cyber Threatscape Report 2018," Accenture, 2018.

[45] Accenture, „Accenture Technology Vision 2019," Accenture, 2019.

[46] F. Adelmann, J. A. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz und C. Wilson, „Cyber Risk and Financial Stability : It's a Small World After All," International Monetary Fund, 2020.

[47] Intsights, „Banking & Financial Services - Cyber Threat Landscape Report," Intsights, 2019.

[48] European Central Bank, „Cyber resilience oversight expectations for financial market infrastructures," European Central Bank, 2018.

[49] R. McMillan, „Definition: Threat Intelligence," Gartner, 2013.

[50] C. Johnson, L. Badger, D. Waltermire, J. Snyder und C. Skorupka, „Guide to Cyber Threat Information Sharing," NIST, 2016.

[51] W. Tounsi und H. Rais, „A survey on technical threat intelligence in the age of sophisticated cyber attacks," in *Computers & security*, 2018.

[52] C. Herley, „The Unfalsifiability of Security Claims," in *Proceedings of the National Academy of Sciences*, 2016.

[53] K. Müller. [Online]. Available: https://confare.at/assume-breach-muss-das-leitmotiv-fuer-jedes-unternehmen-sein/. [Zugriff am Februar 2021].

[54] S. Bradshaw und P. N. Howard, „The global disinformation order: 2019 global inventory of organised social media manipulation," Project on Computational Propaganda, 2019.

[55] D. A. Martin und J. N. Shapiro, „Trends in online foreign influence efforts," in *Princeton University, Princeton, NJ, Working Paper*, 2013.

[56] M. Wu, R. C. Miller und S. L. Garfinkel, „Do Security Toolbars Actually Prevent Phishing Attacks?," in *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2006.

[57] S. Egelman, L. F. Cranor und J. Hong, „You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2006.

[58] T. D. Wagner, E. Palomar, K. Mahbub und A. E. Abdallah, „A novel trust taxonomy for shared cyber threat intelligence," in *Security and Communication Networks*, 2018.

[59] H. Zhu und R. Y. Wang, Information quality framework for verifiable intelligence products, Data Engineering, Springer, 2009, pp. 315-333.

[60] L. C. Botega, J. O. de Souza, . F. R. Jorge, C. S. Coneglian, M. R. de Campos, V. P. d. A. N. Neris und R. Borges de Araújo , „Methodology for data and information quality assessment in the context of emergency situational awareness," in *Universal Access in the Information Society*, 2017.

[61] ENISA, „enisa.europa.eu," Oktober 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020. [Zugriff am Februar 2021].

[62] Intsights, „2021 Banking and Financial Services Industry Cyber Threat Landscape Report," Intsights, 2021.

[63] Intsights, „The Cyber Threat Landscape of the Telecommunications Industry," Intsights, 2021.

[64] Intsights, „Beyond Car Hacking: The Cyber Threat Landscape for Automotive Companies," Intsights, 2021.

[65] Bundesverfassungsgericht, „bundesverfassungsgericht.de," Mai 2020. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html.

[66] M. A. Specter, J. Koppel und D. Weitzner, „The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[67] T. Kovanen, V. Nuojua und M. Lehto, „Cyber threat landscape in energy sector," in *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, 2018.

[68] K. Sachin , B. Krishnamurthy und D. Katabi, „Collaborating against common enemies," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005.

[69] A. Albakri, E. Boiten und R. De Lemos, „Risks of sharing cyber incident information," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018.

[70] A. Albakri, E. Boiten und R. Smith, „Risk Assessment of Sharing Cyber Threat Intelligence," in *European Symposium on Research in Computer Security*, 2020.

[71] A. Zibak und A. Simpson, „Cyber threat information sharing: Perceived benefits and barriers," in *Proceedings of the 14th international conference on availability, reliability and security*, 2019.

[72] A. Albakri, E. Boiten und R. de Lemos, „Sharing cyber threat intelligence under the general data protection regulation," in *Annual Privacy Forum*, 2019.

[73] ENISA, „europa.eu," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive. [Zugriff am 20 07 2021].

[74] ENISA, „Übersicht über Cyberthreat Intelligence," 2020.

[75] M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke, E. Zamani und L. A. Maglaras, „Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI): IEEE CNS 20 Poster," in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020.

[76] R. Borum, J. Felker, S. Kern, K. Dennesen und T. Feyes, „Strategic cyber intelligence," in *Information & Computer Security*, 2015.

[77] Intel Security and Privacy Office, „Understanding Cyberthreat Motivations to Improve Defense," 2015.

[78] Nationale Zentrum für Cybersicherheit (NCSC) & Nachrichtendienst des Bundes (NDB), „Melde- und Analysestelle Informationssicherung - Lage in der Schweiz und International," Nationale Zentrum für Cybersicherheit (NCSC), 2020.

[79] Bundeskanzleramt, „Bericht Cybersicherheit 2020," 2020.

[80] GovCert Austria & Cert.at, „Bericht Internet-Sicherheit Österreich 2020," Cert.at, 2020.

[81] Bundesamt für Sicherheit in der Informationstechnik & Agence nationale de la sécurité des systèmes d'information , „Third edition of the Franco-German common situational picture," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020.

[82] ENISA, „Cyber threat intelligence overview," ENISA, 2020.

[83] ENISA, „Sectoral/thematic threat analysis," ENISA, 2020.

[84] ENISA, „Main incidents in the EU and worldwide," ENISA, 2020.

[85] ENISA, „Research topics," ENISA, 2020.

[86] ENISA, „Emerging trends," ENISA, 2020.

[87] ENISA, „List of top 15 threats," ENISA, 2020.

[88] ENISA, „Malware - ENISA Threat Landscape," 2020.

[89] ENISA, „Web-based attacks - ENISA Threat Landscape," 2020.

[90] ENISA, „Phishing - ENISA Threat Landscape," 2020.

[91] ENISA, „Web application attacks - ENISA Threat Landscape," 2020.

[92] ENISA, „Spam - ENISA Threat Landscape," 2020.

[93] ENISA, „Distributed denial of service - ENISA Threat Landscape," 2020.

[94] ENISA, „Identity theft - ENISA Threat Landscape," 2020.

[95] ENISA, „Data breach - ENISA Threat Landscape," 2020.

[96] ENISA, „Insider Threat - ENISA Threat Landscape," 2020.

[97] ENISA, „Botnet - ENISA Threat Landscape," 2020.

[98] ENISA, „Physical manipulation/ damage/ theft/ loss - ENISA Threat Landscape," 2020.

[99] ENISA, „Information leakage - ENISA Threat Landscape," 2020.

[100] ENISA, „Ransomware - ENISA Threat Landscape," 2020.

[101] ENISA, „Cyber espionage - ENISA Threat Landscape," 2020.

[102] ENISA, „Cryptojacking - ENISA Threat Landscape," 2020.

[103] ENISA, „ENISA Threat Landscape Report 2018," ENISA, 2018.

[104] Kaspersky, „Kaspersky.com," [Online]. Available: https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection. [Zugriff am 24 07 2021].

[105] S. Cook, „comparitech.com," [Online]. Available: https://www.comparitech.com/antivirus/malware-statistics-facts/. [Zugriff am 22 07 2021].

[106] Luatix , „opencti," [Online]. Available: https://www.opencti.io/en/. [Zugriff am 10 03 2021].

[107] Mcafee, „mcafee.com," [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html. [Zugriff am 23 07 2021].

[108] K. Scarfone und P. Mell, „Guide to intrusion detection and prevention systems (idps)," in *NIST special publication*, 2007.

[109] AV-Test, „av-test.org," [Online]. Available: https://www.av-test.org/de/institut/. [Zugriff am 02 04 2021].

[110] BSI, „bsi.bund.de," [Online]. Available: https://www.bsi-fuer-buerger.de/. [Zugriff am 20 03 2021].

[111] Kantonspolizei Zürich, „cybercrimepolice," [Online]. Available: https://www.cybercrimepolice.ch/. [Zugriff am 15 03 2021].

[112] Swiss Government Computer Emergency Response Team, „govcert," [Online]. Available: https://www.govcert.admin.ch/. [Zugriff am 22 03 2021].

[113] Krebs on Security, „krebsonsecurity.com," [Online]. Available: https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/. [Zugriff am 20 03 2021].

[114] eCSIRT.net, „Incident Classification / Incident Taxonomy," 2012.

[115] Shodan , „shodan.io," [Online]. Available: https://www.shodan.io/. [Zugriff am 05 02 2021].

[116] The Shadowserver Foundation, „shadowserver.org," [Online]. Available: https://www.shadowserver.org/. [Zugriff am 14 04 2021].

[117] The Spamhaus Project SLU, „spamhaus.org," [Online]. Available: https://www.spamhaus.org/. [Zugriff am 14 04 2021].

[118] Zone-H, „zone-h.org," [Online]. Available: https://zone-h.org/. [Zugriff am 14 04 2021].

[119] Bulletproof Cyber Limited, „Bulletproof Annual Cyber Security Industry Report 2021," 2021.

[120] NTT ltd., „2020 Global Threat Intelligence Report," 2020.

[121] NTT ltd., „Executive Guide to the 2020 Global Threat Intelligence Report," 2020.

[122] KPMG Security Services GmbH, „Cyber Security in Österreich," 2020.

[123] PwC, „Global Digital Trust Insights Survey 2021," 2020.

[124] National Institute of Standards and Technology, „nist.gov," [Online]. Available: https://www.nist.gov/cyberframework. [Zugriff am 10 03 2021].

[125] WEF, „The Global Risks Report 2020," 2020.

[126] Der Bundesrat, „admin.ch," [Online]. Available: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-77526.html. [Zugriff am 2021 07 25].

[127] ENISA, „ENISA Threat Landscape for 5G Networks," 2020.

[128] ENISA, „European Cybersecurity Month 2020 - Deployment Report," 2021.

[129] ENISA, „ECSC 2020 Analysis Report," 2021.

[130] ENISA, „Situational Report on Microsoft Exchange Vulnerabilities," 2021.

[131] ENISA, „EU Cybersecurity Initiatives in the Finance Sector," 2021.

[132] ENISA, „Security in 5G Specifications - Controls in 3GPP," 2021.

[133] ENISA, „Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving," 2021.

[134] ENISA, „2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries," 2021.

[135] ENISA, „Cloud Security for Healthcare Services," 2021.

[136] ENISA, „Artificial Intelligence Cybersecurity Challenges," 2020.

[137] ENISA, „Sectoral CSIRT Capabilities - Energy and Air Transport," 2020.

[138] ENISA, „Telecom Security During a Pandemic," 2020.

[139] ENISA, „Cybersecurity Stocktaking in the CAM," 2020.

[140] ENISA, „Railway Cybersecurity," 2020.

[141] ENISA, „Guidelines for Securing the Internet of Things," 2020.

[142] ENISA, „National Capabilities Assessment Framework," 2020.

[143] ENISA, „Industry 4.0 - Cybersecurity Challenges and Recommendations," 2019.

[144] BSI, „IT-Sicherheit im Home-Office im Jahr 2020," 2021.

[145] BSI, „Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen v1.3," 2019.

[146] BSI, „Register aktueller CyberGefährdungen und -Angriffsformen," 2018.

[147] ANSSI, „Internet Resilience in France 2015," 2015.

[148] ANSSI, „Controlling the digital risk - The trust advantage," 2017.

[149] Interpol, „ASEAN Cyberthreat Assessment 2020," 2020.

[150] Trend Micro, „Evasive Threats, Pervasive Effects," 2019.

[151] Akamai, „Web Attacks and Gaming Abuse," 2019.

[152] CyberScout, „ITRC's 2019 Annual Data Breach Report," 2019.

[153] Trend Micro, „Cheats, Hacks, and Cyberattacks Threats to the Esports Industry in 2019 and Beyond," 2019.

[154] Trend Micro, „The State Of Ransomware 2020," 2020.

[155] Trend Micro, „A Look At Linux - Threats, Risks, And Recommendations," 2021.

[156] Trend Micro, „Malicious Uses And Abuses Of Artificial Intelligence," 2020.

[157] Trend Micro, „The Hacker Infrastructure And Underground Hosting - An Overview Of The Cybercriminal Market," 2020.

[158] Trend Micro, „Securing The Pandemic-Disrupted Workplace," 2020.

[159] Trend Micro, „2019 Mobile Threat Landscape," 2020.

[160] Trend Micro, „Trend Micro Cloud App Security Report 2019," 2020.

[161] Fireeye, „Cybersecurity Trends 2020," 2020.

[162] D. Trott, „Making Security an Enabler by Delivering Business Outcomes," 2019.

[163] Kaspersky, „securelist.com," [Online]. Available: https://securelist.com/financial-cyberthreats-in-2020/101638/. [Zugriff am 20 03 2021].

[164] A. Hasbini, D. Jordan, A. Seow und C. Cerrudo, „5G Security and Privacy for Smart Cities," 2019.

[165] A. Larkina, „securelist.com," [Online]. Available: https://securelist.com/children-report-2020/97191/. [Zugriff am 20 03 2021].

[166] Kaspersky, „securelist.com," [Online]. Available: https://securelist.com/explicit-content-and-cyberthreats-2019-report/97310/. [Zugriff am 10 03 2021].

[167] Kaspersky, „Incident Response Analyst Report 2020," 2020.

[168] Kaspersky, „securelist.com," [Online]. Available: https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/. [Zugriff am 20 03 2021].

[169] Kaspersky, „securelist.com," [Online]. Available: https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/. [Zugriff am 20 03 2021].

[170] A. Akhmetov, „securelist.com," [Online]. Available: https://securelist.com/digital-footprint-intelligence-report/99452/. [Zugriff am 15 02 2021].

[171] Kaspersky, „The State of Stalkerware in 2020," 2020.

[172] Kaspersky, „securelist.com," [Online]. Available: https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154/. [Zugriff am 22 03 2021].

[173] Accenture Security, „2020 Cyber Threatscape Report," 2020.

[174] Accenture, „Adaptive Security," 2020.

[175] Accenture, „Accenture Technoloy Vision," 2019.

[176] F. Adelmann, I. Ergen, T. Gaidosch, N. Jenkinson , T. Khiaonarong, A. Morozova, N. Schwarz und C. Wilson, „Cyber Risk and Financial Stability," 2020.

[177] ECB, „Cyber resilience oversight expectations for financial market infrastructures," 2018.

[178] J. Goh, H. Kang, Z. X. Koh , . J. W. Lim, C. W. Ng, G. Sher und C. Yao, „Cyber Risk Surveillance: A Case Study of Singapore," 2020.

[179] IMF F&D, „The Global Cyber Threat to Financial Systems," 2021.

[180] Deloitte, „Financial Cyber Survey," 2021.

[181] W. A. Carter, „Forces Shaping the Next Generation of Cyber Threats to Financial Institutions," 2017.

[182] I. Aldasoro, J. Frost, L. Gambacorta und D. Whyte, „Covid-19 And Cyber Risk In The Financial Sector," 2021.

[183] F-Secure, „Cyber threat landscape for the finance sector," 2019.

[184] Intsights, „2021 Tech Industry Cyber Threat Landscape Report," 2021.

[185] Intsights, „The Dark Side of China: The Evolution of a Global Cyber Power," 2021.

[186] Intsights, „GDPR Complicates Italy's Cyber Threat Landscape," 2021.

[187] Intsights, „Health Scare: Data Privacy Concerns in the Age of COVID-19," 2021.

[188] Intsights, „The Cyber Threat Impact of COVID-19 to Global Business," 2021.

[189] Intsights, „Gaming, Leisure, & Hospitality Industry Cyber Threat Report," 2021.

[190] Intsights, „Financial Services Threat Landscape Report The Dark Web Perspective," 2018.

[191] Intsights, „Retail & eCommerce Threat Landscape Report," 2018.

[192] Blueliv, „Cyberthreat Intelligence For Retail & E-Commerce," 2021.

[193] Govloop, „Reinventing Government: 20 Innovations For 2020," 2020.

[194] Crowdstrike, „Vaulting Cybersecurity up to the Cloud," 2020.

[195] Crowdstrike, „2019 Mobile Threat Landscape Report," 2019.

[196] Crowdstrike, „2020 Threat Hunting Report," 2020.

[197] Deloitte, „Cyber Risk in Retail," 2015.

[198] Deloitte, „Deloitte Cyber Security Report 2021," 2021.

[199] Deloitte, „2020 Deloitte Cyber Survey," 2020.

[200] Cyberint, „Threat Landscape Snapshot Retail Report," 2020.

[201] Wandera, „Understanding the mobile threat landscape," 2019.

[202] GSMA, „Mobile Telecommunications Security Threat Landscape," 2019.

[203] Avast, „2020 Threat Landscape Report," 2020.
[204] F5, „Demystifying The Threat Landscape," 2017.
[205] Verizon, „Payment Security Report," 2020.
[206] Communications Security Establishment Canada, „National Cyber Threat Assessment 2020," 2020.
[207] Ensign Infosecurity, „Cyber Threat Landscape Report 2020 Singapore," 2020.
[208] F5, „2019 Application Protection Report," 2019.
[209] D. Warburton, „2020 Phishing And Fraud Report," 2020.
[210] ACSC , „ACSC Annual Cyber Threat Report July 2019 To June 2020," 2020.
[211] Australian Cyber Security Centre, „2020 Sector Snapshot: Health," 2020.
[212] ACSC, „The Commonwealth Cyber Security Posture In 2019," 2020.
[213] The National Cyber Security Centre, „Cyber Threat Report 2020," 2020.
[214] CISA, „2020 Year in Review," 2021.
[215] CISA , „CISA GLOBAL," 2021.
[216] CISA, „Election Infrastructure Cyber Risk Assessment," 2020.
[217] CISA, „Mail-In Voting In 2020 Infrastructure Risk Assessment," 2020.
[218] X-Force, „Cloud Threat Landscape Report 2020," 2020.
[219] Oracle, KPMG, „Cloud Threat and Security Report," 2020.
[220] Fireeye, „The State of Cloud (In)Security," 2019.
[221] GovCERT.HK, „Cyber Security Threat Trends 2020-M05," 2020.
[222] BDO, „Brace For The Breach - Bdo Cyber Threats Insights," 2019.
[223] Fortified Health Security, „2021 Horizon Report - The State of Cybersecurity in Healthcare," 2021.
[224] Proofpoint, „2020 Healthcare Threat Landscape," 2020.
[225] Kaspersky, „New Technologies, New Cyberthreats," 2017.
[226] BaFin, BSI, „BaFin Perspectives - Cyber Security," 2020.
[227] McKinsey & Company, „Cybersecurity In Automotive," 2020.