EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA-BERICHT ZUR BETROHUNGSLAGE 2021

April 2020 bis Mitte Juli 2021

OKTOBER 2021

ÜBER ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einem hohen gemeinsamen Maß an Cybersicherheit in ganz Europa beizutragen. Sie wurde im Jahr 2004 gegründet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Leistungsfähigkeit und Sensibilisierung arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter: www.enisa.europa.eu.

KONTAKT

Um Kontakt mit den Autoren aufzunehmen, wenden Sie sich bitte an etl@enisa.europa.eu.
Medienanfragen zu diesem Dokument richtigen Sie bitte an press@enisa.europa.eu.

HERAUSGEBER

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agentur der Europäischen Union für Cybersicherheit

MITWIRKENDE

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

DANKSAGUNGEN

Wir möchten den Mitgliedern und Beobachtern der Ad-hoc-Arbeitsgruppe der ENISA für die Cyber-Bedrohungslage für ihr wertvolles Feedback und ihre Kommentare bei der Prüfung dieses Berichts danken. Ebenso möchten wir der ENISA-Beratungsgruppe und dem Netz der nationalen Verbindungsbeamten für ihr wertvolles Feedback danken.
Wir danken auch den ENISA-Teams für Situationsbewusstsein und Vorfallmeldung für ihren aktiven Beitrag und die Unterstützung bei der Konsolidierung verschiedener Informationen für die Bedrohungslage.

RECHTLICHER HINWEIS

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine rechtliche Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern diese nicht gemäß der Verordnung (EU) Nr. 2019/881 angenommen wurde. Die ENISA wird diese Veröffentlichung regelmäßig aktualisieren.

Quellen von Dritten werden ordnungsgemäß zitiert. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung dient ausschließlich Informationszwecken. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

HINWEIS ZUM COPYRIGHT

eingeholt werden.

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

Dies ist die neunte Ausgabe des ENISA-Berichts zur Bedrohungslage (ETL), ein Jahresbericht über den Status der Bedrohungslage der Cybersicherheit, der primäre Bedrohungen, wesentliche, beobachtete Trends im Hinblick auf Bedrohungen, Akteure der Bedrohungen sowie Angriffstechniken identifiziert und ebenso relevante Maßnahmen zur Risikominderung beschreibt. Bei dem Prozess der ständigen Verbesserung unserer Methodik für die Entwicklung von Bedrohungslagen wurde die diesjährige Arbeit von der neu gegründeten Ad-hoc-Arbeitsgruppe für Bedrohungslagen der Cybersicherheit (ad hoc Working Group on Cybersecurity Threat Landscapes, CTL) der ENISA unterstützt.

Der Zeitraum des ETL-Berichts 2021 entspricht April 2020 bis Juli 2021 und wird in dem Bericht als „Berichtszeitraum“ bezeichnet. Während des Berichtszeitraums umfassen die identifizierten primären Bedrohungen wie folgt:

- **Ransomware**
- **Schadprogramme**
- **Cryptojacking**
- **Bedrohung in Verbindung mit elektronischer Briefpost**
- **Bedrohung für Daten**
- **Bedrohung für Verfügbarkeit & Integrität**
- **Desinformation – Fehlinformation**
- **Nicht-arglistige Bedrohung**
- **Angriffe auf Lieferketten**

In diesem Bericht besprechen wir die 8 vorrangigen Kategorien der Bedrohung der Cybersicherheit. Die 9. Kategorie „Bedrohungen für die Lieferkette“ wurden aufgrund ihrer besonderen Bedeutung in einem eigenen ENISA-Bericht zur Bedrohungslage für Angriffe auf Lieferketten (ENISA Threat Landscape for Supply Chain Attacks) detailliert analysiert [1].

Für jede identifizierte Bedrohung werden neben den vorgeschlagenen Maßnahmen zur Risikominderung auch die Angriffstechniken, wesentliche Vorfälle und Trends erörtert. Im Hinblick auf Trends wird im Laufe des Berichtszeitraums Folgendes hervorgehoben:

- **Ransomware wurde als primäre Bedrohung für 2020–2021 bewertet.**
- **Regierungsorganisationen haben ihren Einsatz auf nationaler und internationaler Ebene verstärkt.**
- **Cyberkriminelle sind zunehmend durch die Monetarisierung** ihrer Aktivitäten, z. B. Ransomware, motiviert. Die **Cryptowährung** bleibt die geläufigste Zahlungsmethode für Bedrohungsakteure.
- Der **Rückgang von Malware**, der 2020 beobachtet wurde, setzt sich 2021 fort. 2021 erfolgte eine Zunahme von Bedrohungsakteuren, die auf relativ neue oder ungewöhnliche Programmiersprachen zurückgriffen, um deren Code zu übertragen.
- Die Menge an **Cryptojacking-Infektionen** erzielte im ersten Quartal 2021 im Vergleich zu den letzten Jahren ein **Rekord-Hoch**. Die mit Cryptojacking verbundenen **finanziellen Gewinne** regten die Bedrohungsakteure zu diesen Angriffen an.
- **COVID-19 ist in Kampagnen noch immer der hauptsächliche Köder** für Angriffe durch elektronische Post**.**
- Es kam zu einem **Anstieg von Datenschutzverletzungen in Zusammenhang mit dem Gesundheitssektor**.

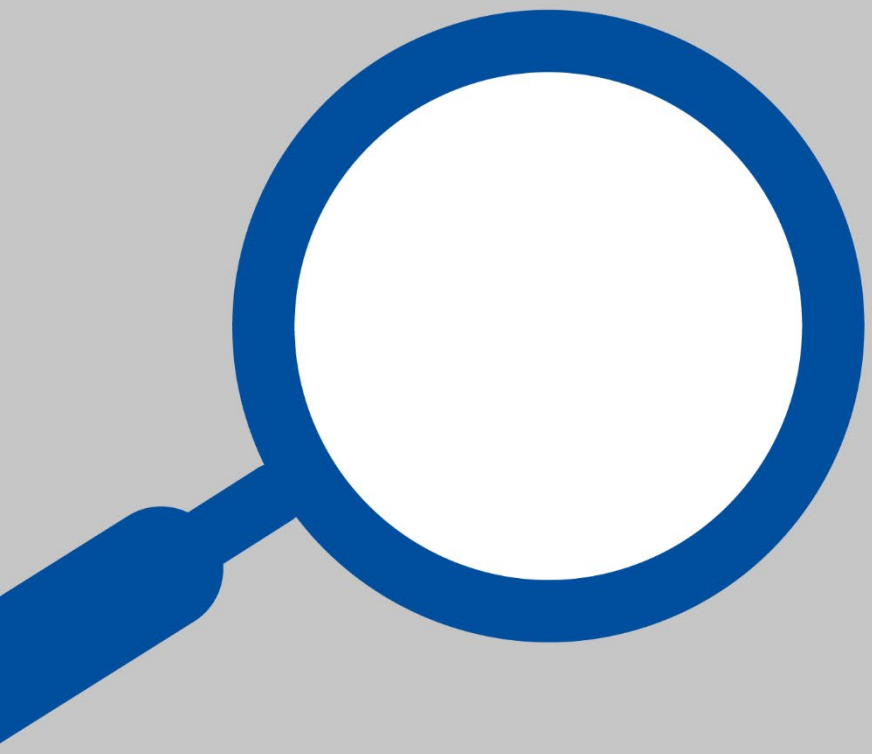
[1] ENISA Threat Landscape for Supply Chain Attacks, Juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- **Herkömmliche DDoS (Distributed Denial-of-Service)-Kampagnen** verliefen 2021 zielgerichteter, hartnäckiger und zunehmend breit gefächert. Das **IoT (Internet der Dinge)** in Verbindung mit **mobilen Netzwerken** führt zu einer neuen Welle von DDoS-Angriffen.
- 2020 und 2021, als die COVID-19-Pandemie zahlreiche **menschliche Fehlhandlungen** und **Systemfehlkonfigurationen** hervorbrachte, konnten wir eine **Steigerung nicht-arglistiger Vorfälle** beobachten, so dass die meisten Verstöße im Jahr 2020 durch Fehler verursacht wurden.

Das Verstehen der Trends in Verbindung mit Bedrohungsakteuren, ihrer Motivationen und Ziele trägt in hohem Maß zur Planung von Schutzmaßnahmen für die Cybersicherheit und Maßnahmen zur Risikominderung bei. Dies ist Teil unserer globalen Bedrohungsanalyse, da Sicherheitskontrollen somit priorisiert und eine spezielle Strategie basierend auf den möglichen Auswirkungen und der Wahrscheinlichkeit des Eintritts der Bedrohung ausgearbeitet werden kann. Vor diesem Hintergrund werden für die Zwecke des ETL 2021 die folgenden vier Kategorien von Bedrohungsakteuren im Bereich der Cybersicherheit betrachtet:

- **Staatlich geförderte Akteure**
- **Akteure der Computerkriminalität**
- **Hacker-for-hire-Akteure**
- **Hacktivisten**

Durch fortlaufende Analyse hat die ENISA Trends und Interessenschwerpunkte für jede bedeutende Bedrohung, die im ETL 2021 dargestellt wurde, ausgearbeitet. Die wesentlichen Erkenntnisse und Beurteilungen in dieser Bewertung beruhen auf mehreren öffentlich zugänglichen Ressourcen, die in den für die Ausarbeitung dieses Dokuments verwendeten Referenzen angegeben sind. Der Bericht ist hauptsächlich für strategische und politische Entscheidungsträger gedacht, ist jedoch auch für die technische Cybersicherheitsgemeinschaft interessant.



ÜBERBLICK ÜBER DIE BEDROHUNGSLAGE

In der 9. Ausgabe stellt der ENISA-Bericht zur Bedrohungslage (ETL) einen allgemeinen Überblick über die Bedrohungslage der Cybersicherheit bereit. Der ETL-Bericht ist teils strategisch, teils technisch und enthält Informationen, die sowohl für technisch versierte als auch für nicht versierte Leser relevant sind. Die diesjährige Arbeit wurde von der neu gegründeten Ad-hoc-Arbeitsgruppe für Bedrohungslagen der Cybersicherheit (CTL) der ENISA unterstützt.[2]

In den Jahren 2020 und 2021 haben sich die Angriffe auf die Cybersicherheit nicht nur im Hinblick auf die Überträger und die Anzahl, sondern auch bezüglich ihrer Auswirkungen gesteigert. Auch die COVID-19-Pandemie hat sich – wie erwartet – auf die Bedrohungslage der Cybersicherheit ausgewirkt. Eine der längerfristigen Entwicklungen der COVID-19-Pandemie ist der bleibende Wechsel zum hybriden Büromodell. Daher werden „Bedrohungen der Cybersicherheit“ in Verbindung mit der Pandemie und die Instrumentalisierung der „neuen Normalität“ nun zur Regel. Durch diesen Trend hat sich die Angriffsfläche vergrößert und wir konnten durch das Homeoffice einen Anstieg bei der Anzahl der Cyberangriffe auf Organisationen und Unternehmen verzeichnen.[3]

Insgesamt wird eine Zunahme der Bedrohungen der Cybersicherheit beobachtet. Angetrieben durch die zunehmende Online-Präsenz, den Wechsel von herkömmlichen Strukturen hin zu Online- und Cloud-basierten Lösungen, der besseren Vernetzung und der Nutzung neuer Funktionen aufstrebender Technologien wie z. B. Künstliche Intelligenz (KI)[4][5] hat sich die Bedrohungslage der Cybersicherheit im Zusammenhang mit der Raffinesse der Angriffe, ihrer Komplexität und ihren Auswirkungen verschärft. Insbesondere die Bedrohung von Lieferketten und deren Bedeutung aufgrund ihrer potenziell katastrophalen Kaskadeneffekte hat den höchsten Rang unter den Hauptbedrohungen erreicht, so sehr, dass die ENISA eine eigene Bedrohungslandschaft für diese Kategorie von Bedrohungen erstellt hat.[6]

Es soll darauf hingewiesen werden, dass in dieser Version des ETL besonderes Augenmerk auf die Auswirkungen von Cyber-Bedrohungen in verschiedenen Sektoren gelegt wurde, einschließlich derer, die in der Richtlinie über Netz- und Informationssicherheit (NISD) aufgeführt sind. Interessante Einsichten können aus den Besonderheiten jedes Bereichs in Zusammenhang mit der Bedrohungslage gewonnen werden, ebenso wie mögliche Abhängigkeiten und Themenbereiche. Entsprechend verdienen sektorbezogene Bedrohungslagen mehr Aufmerksamkeit.

In diesem Jahr haben einige Verfechter der Cyber-Gemeinschaft ebenso wie politische Entscheidungsträger bedeutende Schritte unternommen. Die weltweite Gemeinschaft hat mittlerweile die Bedeutung von Kommunikation und Zusammenarbeit bei der Untersuchung und Verfolgung von Cyberkriminellen begriffen, wobei insbesondere Ransomware (die herausragende Bedrohung für den Berichtszeitraum des ETL 2021) bei Führungskräften auf der ganzen Welt ganz oben auf der Agenda für Sitzungen im Zusammenhang mit Strategie steht.

Aufmerksame Leser der letzten Ausgaben des ETL 2021 werden eine unterschiedliche Darstellung der primären Bedrohungen feststellen. In diesem Jahr ist die ENISA einen Schritt zurückgetreten und hat die Bedrohungskategorien im Hinblick auf die Einbindung und bessere Darstellung ähnlicher Bedrohungen konsolidiert. Dies ist Bestandteil der fortlaufenden Bemühungen um eine aufgearbeitete Bedrohungstaxonomie und wird in den nächsten Jahren die methodische Bestimmung von Trends unterstützen.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Kosten einer Datenschutzverletzung, Bericht 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Threat Landscape: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA Threat Landscape for Supply Chain Attacks, Juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Der ETL 2021 basiert auf einer Vielzahl offener Informationsquellen sowie Quellen für Cyber-Bedrohungserkenntnisse. Er stellt die wesentlichen Bedrohungen, Trends und Befunde heraus und bietet entsprechende hochwertige Strategien zur Risikominderung an. Derzeit arbeitet die ENISA an der Untermauerung der Methodik zur Berichterstattung über die Bedrohungslage, um die Transparenz und Konsistenz der Arbeit zu fördern.

1.1. PRIMÄRE BEDROHUNGEN

Im Laufe der Jahre 2020 und 2021 sind eine Reihe von Cyberbedrohungen entstanden und sind eingetreten. Auf der Grundlage der in diesem Bericht vorgestellten Analyse identifiziert der ENISA-Bericht zur Bedrohungslage 2021 die folgenden 8 primären Bedrohungsgruppen und konzentriert sich auf diese (siehe Abbildung 1). Diese 8 Bedrohungsgruppen sind aufgrund ihrer Bedeutung während des Berichtszeitraums, ihrer Beliebtheit und der Auswirkungen, die das Eintreten dieser Bedrohungen mit sich brachte, hervorgehoben.

- **Ransomware**
  Ransomware ist eine Art von bösartigem Angriff, bei dem die Angreifer die Daten einer Organisation verschlüsseln und eine Zahlung für die Wiederherstellung des Zugangs fordern. Ransomware stellte während des Berichtszeitraums die primäre Bedrohung dar, wobei mehrere Vorfälle mit hohem Bekanntheitsgrad auftraten, die große Aufmerksamkeit auf sich zogen. Die Bedeutung und Auswirkung der Bedrohung durch Ransomware wurde auch durch eine Reihe von damit verbundenen politischen Initiativen innerhalb der Europäischen Union (EU) und auf internationaler Ebene nachgewiesen.

- **Schadprogramme**
  Ein Schadprogramm ist Software oder Firmware, die das Ziel hat, einen ungenehmigten Zugriff zu schaffen, der sich nachteilig auf die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems auswirkt. Die Bedrohung durch ein Schadprogramm wurde über viele Jahre durchgehend hoch eingestuft, obschon sie während des Berichtszeitraums des ETL 2021 zurückgegangen ist. Die Nutzung neuer Angriffstechniken und einiger bedeutender Gewinne für die Vertreter der Strafverfolgung haben die Vorgänge der jeweiligen Bedrohungsakteure beeinträchtigt.

- **Cryptojacking**
  Cryptojacking oder verdecktes Crypto-Mining ist eine Art von Cyberkriminalität, bei der ein Krimineller die Rechnerleistung eines Opfers insgeheime nutzt, um eine Cryptowährung zu generieren. Mit der Verbreitung von Cryptowährungen und deren zunehmender Akzeptanz durch die breite Bevölkerung wurde eine Zunahme der entsprechenden Vorfälle im Bereich der Cybersicherheit beobachtet.

- **Bedrohung in Verbindung mit elektronischer Briefpost**
  Angriffe im Zusammenhang mit elektronischem Postverkehr bestehen aus einem Bündel von Bedrohungen, die die Schwächen der menschlichen Psyche und die alltäglichen Gewohnheiten anstelle der technischen Schwächen von Informationssystemen ausnutzen. Interessanterweise und trotz den zahlreichen Sensibilisierungs- und Informationskampagnen gegen diese Art von Angriffen ist die Bedrohung weiterhin bemerkenswert groß. Insbesondere nimmt die Gefährdung durch geschäftliche elektronische Post und fortschrittlichen Techniken bei dem Herausschlagen von monetären Gewinnen weiterhin zu.

- **Bedrohung für Daten**
  Diese Kategorie umfasst die Verletzung des Datenschutzes / den Verlust von Daten. Eine Datenschutzverletzung oder ein Datenverlust ist die Freigabe von sensiblen, vertraulichen oder geschützten Daten an eine unsichere Umgebung. Datenschutzverletzungen können aufgrund eines Cyberangriffs, einem Insider-Job, unbeabsichtigtem Verlust oder der Offenlegung von Daten auftreten. Die Bedrohung ist weiterhin groß, da Datenzugriff aus zahlreichen Gründen ein primäres Ziel für Angreifer darstellt, z. B. Erpressung, Lösegeld, Verleumdung, Falschinformation usw.

- **Bedrohung für Verfügbarkeit und Integrität**
  Verfügbarkeit und Integrität sind das Ziel einer Fülle von Bedrohungen und Angriffen, wobei die Gruppen der Denial-of-Service- (DoS) und Internetangriffe herausstechen. DDoS ist eng mit Internetangriffen verbunden und

stellt eine der größten Bedrohungen für IT-Systeme dar, mit dem Ziel, deren Verfügbarkeit durch Erschöpfen der Ressourcen zu verhindern, was wiederum zu Leistungsverlust, Datenverlust und Ausfällen führt. Diese Bedrohung steht dauerhaft hoch auf der Liste der Bedrohungslage der ENISA, und dies sowohl aufgrund ihrer Manifestation in tatsächlichen Vorfällen als auch wegen ihres Potenzials für bedeutende Auswirkungen.

- **Desinformation – Fehlinformation**
  Desinformations- und Fehlinformationskampagnen sind auf dem Vormarsch und werden durch die erhöhte Nutzung von Social-Media-Plattformen und Online-Medien sowie aufgrund der verstärkten Online-Präsenz der Menschen durch die COVID-19-Pandemie angetrieben. Die Bedrohungsgruppe erscheint zum ersten Mal im ETL; dennoch ist ihre Bedeutung in der Cyberwelt groß. Desinformations- und Fehlinformationskampagnen werden häufig bei Hybridangriffen genutzt, um die Gesamtwahrnehmung von Vertrauen, einer wichtigen Voraussetzung für Cybersicherheit, zu mindern.

- **Nicht-arglistige Bedrohung**
  Bedrohungen werden gemeinhin als freiwillige und arglistige Tätigkeiten erachtet, die von Widersachern stammen, die einen Anreiz haben, ein bestimmtes Ziel anzugreifen. Diese Kategorie umfasst Bedrohungen, deren arglistige Absicht nicht offensichtlich ist. Sie beruhen meist auf menschlichen Fehlhandlungen und Systemfehlkonfigurationen, allerdings können sie auch auf physische Katastrophen verweisen, die auf IT-Infrastrukturen ausgerichtet sind. Auch aufgrund ihrer Natur sind diese Bedrohungen ständig in der jährlichen Bedrohungslage aufgeführt und stellen ein Hauptanliegen in Risikobewertungen dar.

Abbildung 1: ENISA-Bedrohungslage 2021 - Primäre Bedrohungen

Es ist zu vermerken, dass die zuvor erwähnten Bedrohungen Kategorien und die Sammlung von Bedrohungen umfassen, die in den oben genannten acht Bereichen zusammengefasst sind. Jede der Bedrohungsgruppen ist in einem eigenen Kapitel dieses Berichts, das auch ihre Besonderheiten herausarbeitet und genauere Informationen, Erkenntnisse, Trends, Angriffstechniken und Abwehrträger bereitstellt, gründlich analysiert.

1.2. WESENTLICHE TRENDS

Die folgende Liste fasst die wichtigsten Trends zusammen, die im Berichtszeitraum in Bezug auf die Cyber-Bedrohungslage beobachtet wurden. Diese wurden auch in den verschiedenen Kapiteln einschließlich des ENISA-Berichts zur Bedrohungslage 2021, ausführlich überprüft.

- Wie im ENISA-Bericht zur Bedrohungslage für Lieferketten hervorgehoben, **nahmen hochentwickelte und wirkungsvolle Gefährdungen der Lieferkette zu**. **Managed-Service-Providers** sind hochwertige Ziele für Cyberkriminelle.
- **COVID-19 hat die Beauftragung von Cyberspionage angetrieben und Möglichkeiten für Cyberkriminelle geschaffen.**
- **Regierungsorganisationen haben ihren Einsatz** auf nationaler und internationaler Ebene **verstärkt.** So haben Regierungen verstärkte Bemühungen beobachtet, Störungen hervorzurufen und rechtliche Schritte gegen staatlich geförderte Bedrohungsakteure zu ergreifen.
- **Cyberkriminelle sind zunehmend durch die Monetarisierung** ihrer Aktivitäten, z. B. Ransomware, motiviert. Die **Cryptowährung** bleibt die geläufigste Zahlungsmethode für Bedrohungsakteure.
- Cyberkriminelle Angriffe haben **zunehmend wichtige Infrastrukturen und deren Beeinträchtigung** als Ziel.
- **Gefährdungen durch Phishing-E-Mails und brutale Gewaltausübung auf Remote Desktop Services (RDP)** bleiben die beiden geläufigsten **Infektionsträger von Ransomware**.
- Der Fokus auf **Geschäftsmodellen wie Ransomware as a Service (RaaS)** hat sich 2021 verstärkt, was eine richtige Zuweisung einzelner Bedrohungsakteure erschwert.
- Das Auftreten von **Ransomware-Systemen mit dreifacher Erpressung** hat im Laufe des Jahres 2021 stark zugenommen.
- Der **Rückgang von Malware**, der 2020 beobachtet wurde, setzt sich 2021 fort. 2021 erfolgte eine Zunahme von Bedrohungsakteuren, die auf relativ neue oder ungewöhnliche Programmiersprachen zurückgriffen, um deren Code zu übertragen.
- Auf **Container-Umgebungen ausgerichtete Malware** hat sich sehr viel stärker verbreitet, wobei neue Entwicklungen wie dateilose Malware vom Speicher ausgeführt wird.
- Malware-Entwickler finden immer neue Wege, um **Reverse-Engineering und dynamische Analysen zu erschweren**.
- Die Menge an **Cryptojacking-Infektionen** erzielte im ersten Quartal 2021 im Vergleich zu den letzten Jahren ein **Rekord-Hoch**. Die mit Cryptojacking verbundenen **finanziellen Gewinne** regten die Bedrohungsakteure zu diesen Angriffen an.
- **Die Menge an Crypto-Mining- und Cryptojacking-Aktivitäten im Jahr 2021 haben Rekordhöhen erreicht.**
- Wir erkennen, dass ein **Wechsel von Browser- zu dateibasiertem Cryptojacking** stattfindet.
- **COVID-19 ist in Kampagnen noch immer der hauptsächliche Köder** für Angriffe durch elektronische Post**.**
- **Business E-mail Compromise (BEC)** hat **zugenommen**, ist **ausgefeilter** geworden und wird **gezielter** eingesetzt.
- Das Geschäftsmodell **Phishing-as-a-Service (PhaaS)** verbreitet sich immer mehr.
- Bedrohungsakteure richten ihre Aufmerksamkeit im Zusammenhang mit der Gefahr für Daten und Informationen vermehrt auf **Informationen zu Impfstoffen**.
- Es kam zu einem **Anstieg von Datenschutzverletzungen in Zusammenhang mit dem Gesundheitssektor**.
- Die herkömmlichen DDoS (Distributed Denial-of-Service)-Angriffe gehen allmählich auf **mobile Netzwerke und IoT (Internet der Dinge)** über.
- **Ransom Denial-of-Service (RDoS)** ist die neue Grenze der Denial-of-Service-Angriffe**.**
- Das Teilen von Ressourcen in virtualisierten Umgebungen wirkt wie eine Verstärkung von DDoS-Angriffen.
- DDoS-Kampagnen sind 2021 zielgerichteter und sehr viel nachdrücklich sowie zunehmend breitgefächert angelegt.
- **Durch künstliche Intelligenz (KI) ermöglichte Desinformation** unterstützt die Angreifer bei der Durchführung ihrer Angriffe.

- Phishing ist der Kern von Angriffen mit Desinformation und nutzt die Überzeugung der Menschen schamlos aus.
- Fehlinformation und Desinformation sind das Herz von Cyberkriminalität und nehmen in beispiellosem Ausmaß zu.
- **Das Geschäftsmodell Disinformation-as-a-Service (DaaS)** hat sich erheblich verbreitet, angetrieben von den zunehmenden Auswirkungen der COVID-19-Pandemie und dem zunehmendem Informationsbedarf.
- 2020 und 2021, als die COVID-19-Pandemie zahlreiche **menschliche Fehlhandlungen** und **Systemfehlkonfigurationen** hervorbrachte, konnten wir eine **Steigerung nicht-arglistiger Vorfälle** beobachten, so dass die meisten Verstöße im Jahr 2020 durch Fehler verursacht wurden.
- Es gab ein **Rekordhoch an nicht-arglistigen Vorfällen der Cloud-Sicherheit.**

1.3. EU-NÄHE VON PRIMÄREN BEDROHUNGEN

Ein wichtiger Aspekt, der im Zusammenhang mit dem ENISA-Bericht zur Bedrohungslage zu beachten ist, betrifft die Nähe einer Cyberbedrohung im Hinblick auf die Europäische Union (EU). Dies ist besonders wichtig, um Analytiker bei der Bewertung der Bedeutung von Cyberbedrohung zu unterstützen, sie mit potentiellen Bedrohungsakteuren und Trägern in Beziehung zu setzen und sogar die Auswahl der angemessenen zielgerichteten Begrenzungsträger zu leiten. Entsprechend der vorgeschlagenen Klassifizierung der Gemeinsame Sicherheits- und Verteidigungspolitik der EU (CSDP)[7], ordnen wir Cyberbedrohungen in vier Kategorien ein, wie dargestellt in **Tabelle 1**.

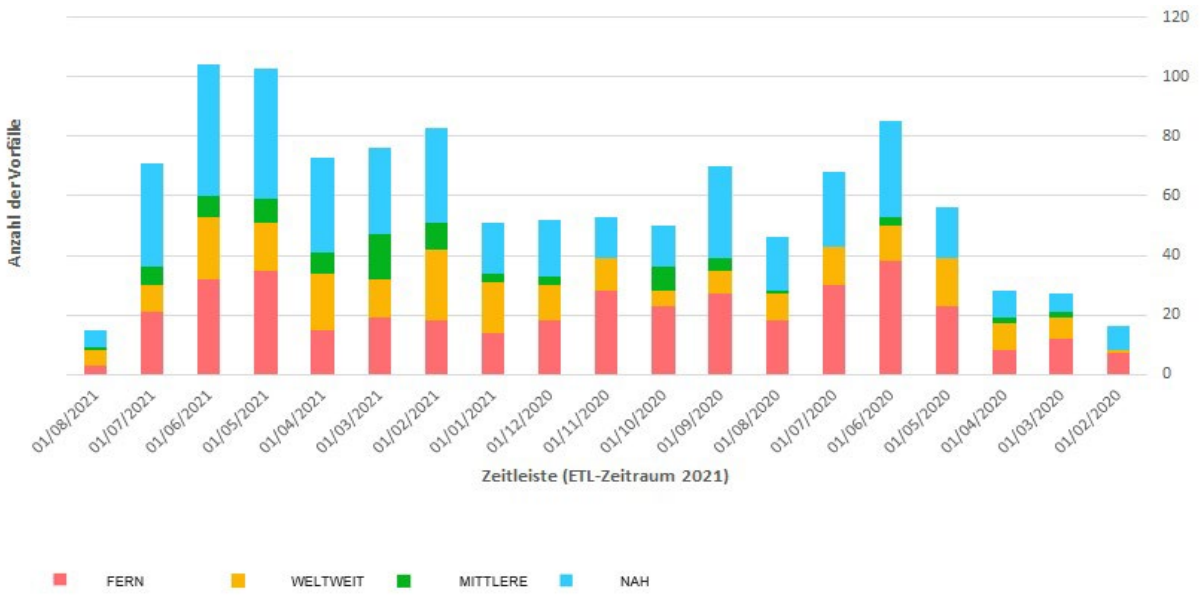
Tabelle 1: Klassifizierung der Nähe von Cyberbedrohungen

Nähe	Bedenken
NAH	Betroffene Netze, Systeme, die innerhalb der EU-Grenzen kontrolliert und gesichert werden. Betroffene Bevölkerung innerhalb der Grenzen der EU.
MITTLERE	Netze und Systeme, die für operative Ziele innerhalb der Reichweite des digitalen Binnenmarkts der EU und der Sektoren der Richtlinie zur Netz- und Informationssicherheit wichtig sind, deren Kontrolle und Sicherung von institutionellen Nicht-EU-Gremien oder öffentlichen oder privaten Behörden der MS. Betroffene Bevölkerung in geographischen Gebieten nahe der Grenzen der EU.
FERN	Netze und Systeme, die, falls sie beeinflusst werden, große Auswirkungen auf operative Ziele innerhalb der Reichweite des digitalen Binnenmarkts der EU und der Sektoren der Richtlinie zur Netz- und Informationssicherheit haben. Die Kontrolle und Sicherung dieser Netze und Systeme liegt jenseits der institutionellen Gremien der EU oder der öffentlichen oder privaten Behörden der Mitgliedsstaaten (MS). Betroffene Bevölkerung in geographischen Gebieten, die weit von der EU entfernt sind.
WELTWEIT	Alle zuvor genannten Gebiete

Abbildung 2 Zeigt eine Zeitleiste von Vorfällen in Bezug auf die primärem Bedrohungskategorien, die im ETL 2021 gemeldet wurden. Es ist zu beachten, dass die Informationen in dem Diagramm auf OSINT (Open Source Intelligence) zurückzuführen sind und aus Arbeiten der ENISA im Bereich des Situationsbewusstseins resultieren[8].

Abbildung 2: Zeitleiste der beobachteten Vorfälle im Zusammenhang mit wesentlichen ETL-Bedrohungen (OSINT-basiertes Situationsbewusstsein) hinsichtlich ihrer Nähe.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] In Übereinstimmung mit dem Rechtsakt zur Cybersicherheit der EU Art. 7, Abs. 6https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN



Wie aus den oben genannten Zahlen hervorgeht, traten 2021 im Vergleich zu 2020 mehr Vorfälle auf. Insbesondere zeigt die Kategorie NAH eine ständig steigende Anzahl von beobachteten Vorfällen in Bezug auf primäre Bedrohungen, was auf deren Bedeutung im Zusammenhang mit der EU hinweist. Es überrascht nicht, dass die monatlichen Trends (diese sind aufgrund der Kürze nicht in der Abbildung dargestellt) bei den verschiedenen Klassifizierungen recht ähnlich sind, da die Cybersicherheit keine Grenzen kennt und die Bedrohungen sich in den meisten Fällen auf allen Ebenen der Nähe auftreten. Es ist bemerkenswert, dass in den letzten vom ETL 2021 erfassten Monaten in der EU eine Zunahme in der Kategorie NAH zu beobachten ist, ein Trend, den die ENISA weiter beobachten wird, um zu sehen, wie er sich entwickelt und wie er mit den Aktivitäten von Bedrohungsakteuren und aktuellen Bedrohungsvektoren zusammenhängt.

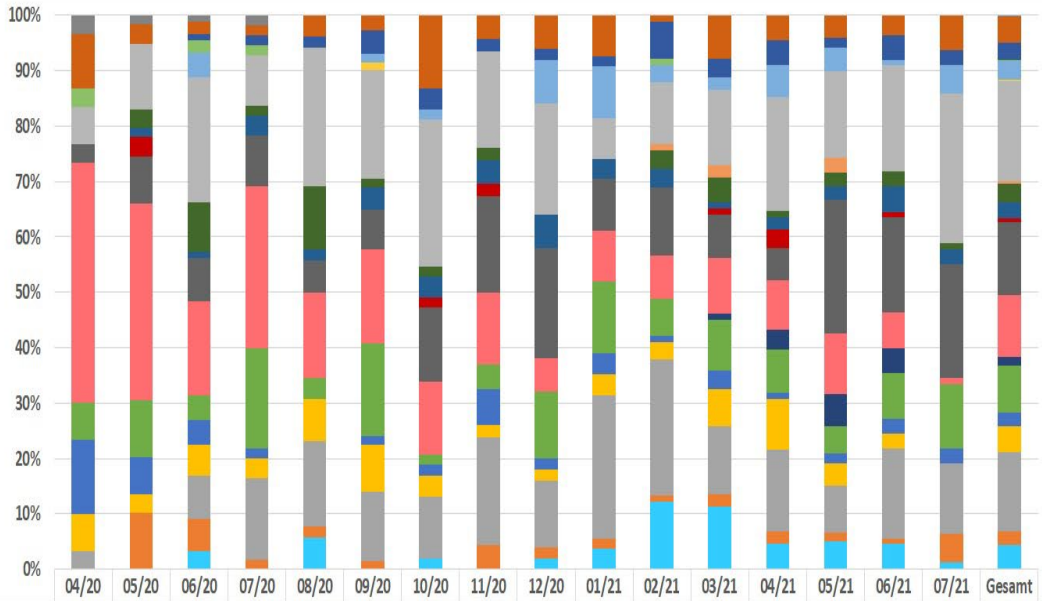
1.4. PRIMÄRE BEDROHUNGEN PRO SEKTOR

Cyberbedrohungen beschränken sich normalerweise nicht auf einen besonderen Sektor und betreffen in den meisten Fällen mehr als einen Sektor. Dies stimmt tatsächlich, da die Bedrohungen in den meisten Fällen durch die Ausnutzung von Schwächen in den zugrunde liegenden IKT-Systemen erfolgt, die in einer Vielzahl von Sektoren verwendet werden. Allerdings sind gezielte Angriffe sowie Angriffe, bei denen die verschiedenen Reifegrade der Cybersicherheit in allen Sektoren und die Beliebtheit/Bedeutung bestimmter Sektoren ausgenutzt werden, alles Faktoren, die zu berücksichtigen sind. Diese Faktoren tragen zu Bedrohungen bei, die als Vorfälle in bestimmten Sektoren auftreten und aus diesem Grunde ist es wichtig, die sektorbezogenen Aspekte der beobachteten Vorfälle und Bedrohungen genau zu analysieren. Darüber hinaus sind Trends, die in jedem Sektor und den Abhängigkeiten der Sektoren untereinander aufgefallen sind, Wahrnehmungen, die aus einer solchen Analyse verwendet werden können.

Abbildungen 3 und 4 heben die betroffenen Sektoren in Bezug auf Vorfälle hervor, die auf der Grundlage von OSINT (Open Source Intelligence) beobachtet wurden und die aus Arbeiten der ENISA im Bereich des Situationsbewusstseins resultieren[9]. Sie verweisen auf Vorfälle im Zusammenhang mit den primären Bedrohungen des ETL 2021. Dies ist der erste Versuch der ENISA, die Auswirkungen von Bedrohungen für bestimmte Sektoren zu kartieren. In den kommenden Jahren und in zukünftigen Neuauflagen der Bedrohungslage geht es darum, die Sektoren mit den in der Richtlinie zur Netz- und Informationssicherheit (NISD) aufgeführten und dem Vorschlag für deren Überprüfung (NISD 2.0) abzugleichen.

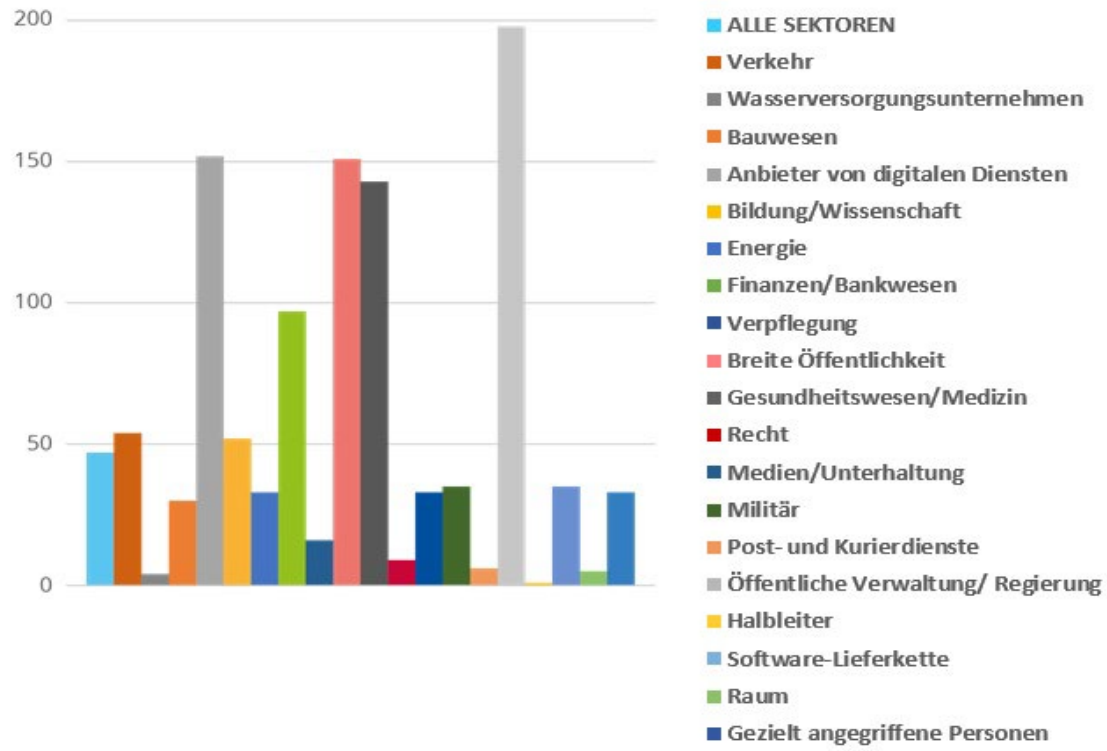
[9] In Übereinstimmung mit dem Rechtsakt zur Cybersicherheit der EU Art. 7, Abs.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Abbildung 3: Zeitleiste der beobachteten Vorfälle mit Bezug auf primäre ETL-Bedrohungen für betroffene Sektoren.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Gesamt
Wasserversorgungsunternehmen	1	1	1	1													2
Verkehr	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Gezielt angegriffene Personen			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Raum	1		2	1							1						4
Software-Lieferkette			4			1	1		4	5	3	2	5	5	1	4	35
Halbleiter						1											1
Öffentliche Verwaltung/ Regierung	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Post- und Kurierdienste											1	2		3			6
Militär		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Medien/Unterhaltung		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Recht		2					1	1				1	3		1		7
Gesundheitswesen/Medizin	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Breite Öffentlichkeit	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Verpflegung												1	3	7	5		16
Finanzen/Bankwesen	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energie	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Bildung/Wissenschaft	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Anbieter von digitalen Diensten	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Bauwesen		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
ALLE SEKTOREN			3		3		1		1	2	11	10	4	6	5	1	47

Abbildung 4: Gezielt ausgewählte Sektoren nach Anzahl der Vorfälle (April 2020-Juli 2021)



Während dieses Berichtszeitraums waren eine große Anzahl von Vorfällen auf die öffentliche Verwaltung, die Regierung und digitale Dienstleister ausgerichtet. Letzteres ist aufgrund der horizontalen Bereitstellung von Dienstleistungen für diesen Sektor zu erwarten und wird sich somit auf viele andere Sektoren auswirken. Auch haben wir eine bedeutende Anzahl von Vorfällen bemerkt, deren Ziel Endnutzer und nicht unbedingt ein bestimmter Sektor waren. Das Gesundheitswesen war auch in hohem Maß betroffen, und diese Aktivität stieg während der letzten Monate des Berichtszeitraums (Mai-Juli 2021) spürbar an. Interessanterweise weist auch der Finanzsektor eine beständige Anzahl von Vorfällen über das gesamte Jahr auf. Auch die Lieferkette für Software zeigt für 2021 eine erhöhte Anzahl von Vorfällen an, eine Beobachtung, die auch im ENISA-Bericht zur Bedrohungslage für Lieferketten vermerkt ist[10].

1.5. METHODIK

Der ENISA-Bericht zur Bedrohungslage (ETL) 2021 beruht auf Informationen aus offenen Quellen, hauptsächlich strategischer Art, und den eigenen Cyber Threat Intelligence (CTI)-Quellen der ENISA, und deckt mehr als einen Sektor, eine Technologie und den Kontext ab. Der Bericht versucht, branchen- und herstellerunabhängig zu sein und verweist oder zitiert die Arbeit verschiedener Sicherheitsforscher, Sicherheitsblogs und Nachrichtenmedienartikeln, die im gesamten Text in mehreren Endnoten klar angegeben sind. Der Zeitraum des ETL-Berichts 2021 entspricht April 2020 bis Juli 2021 und wird in dem Bericht als „Berichtszeitraum“ bezeichnet.

Für die Verfassung des ETL-Berichts 2021 wurde folgender Ansatz verfolgt. Die ENISA hat über den entsprechenden Zeitraum mittels Situationsbewusstsein eine Liste der wesentlichen Vorfälle entsprechend ihrem Erscheinen in offenen Quellen gesammelt. Diese Liste diente als Grundlage für die Identifizierung der Liste der primären Bedrohungen, sowie als Quellenmaterial für mehrere Trends und Statistiken in dem Bericht.

Dann führten die ENISA und externe Experten eine eingehende Recherche der verfügbaren Literatur aus offenen Quellen wie Nachrichtenmedienartikeln, Expertenmeinungen, Geheimdienstberichten, Vorfallanalysen und Sicherheitsforschungsberichten durch. Durch fortlaufende Analyse hat die ENISA Trends und

[10] ENISA Threat Landscape for Supply Chain Attacks, Juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Interessenschwerpunkte für jede bedeutende Bedrohung, die im ETL 2021 dargestellt wurde, ausgearbeitet. Die wesentlichen Erkenntnisse und Beurteilungen in dieser Bewertung beruhen auf mehreren öffentlich zugänglichen Ressourcen, die in den für die Ausarbeitung dieses Dokuments verwendeten Referenzen angegeben sind.

Im Bericht bemühen wir uns, zwischen den Meldungen aus unseren offenen Quellen und unserer eigenen Bewertung zu unterscheiden. (Dies ist insbesondere durch den Wortlaut „in unserer Bewertung“ dargestellt). Schließlich weisen wir bei der Bewertung auf die Wahrscheinlich hin, indem wir Wörter verwenden, die eine Einschätzung der Wahrscheinlichkeit ausdrücken (z. B. wahrscheinlich, sehr wahrscheinlich, sicherlich)[11].

MITRE ATT&CK® Rahmenumgebung[12] wurde in diesem Bericht zur Hervorhebung der Angriffstaktiken und -techniken für eine bestimmte Bedrohung verwendet (siehe Anhang A). Für jede ATT&CK®-Taktik werden die Techniken des Gegners vorgestellt. Dies führt zu einer Liste von ATT&CK-Schutzmaßnahmen[13], die angewendet werden kann. MITRE ATT&CK® ist eine Wissensbasis, eine gemeinsame Sprache für feindliche Taktiken und Techniken, die auf realen Beobachtungen beruhen. Die Wissensbasis MITRE ATT&CK® wird als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und Methodologien im Privatsektor, in der Regierung und der Produkt- und Dienstleistungsgemeinschaft für Cybersicherheit verwendet.

Der Bericht wurde von der Ad-hoc-Arbeitsgruppe für Bedrohungslagen der Cybersicherheit der ENISA[14] validiert, der im April 2021 verfasst wurde. Diese Gruppe besteht aus Experten aus Unternehmen des europaweiten und internationalen öffentlichen und privaten Sektors.

Für die zukünftige Erstellung von Bedrohungslagen bestärkt die ENISA derzeit formell eine neue Methodik, um mehr Transparenz zu erlangen und die Grundlagen für strukturierte und gut abgestimmte Prozesse festzulegen. Mit diesen Bemühungen und einer überarbeiteten Bedrohungstaxonomie wird die Methodik für Bedrohungslagen zukünftig veröffentlicht.

1.6. AUFBAU DES BERICHTS

Für den ENISA-Bericht zur Bedrohungslage (ETL) 2021 wurde die Struktur früherer ETL-Berichte durch die Verwendung einer ähnlichen Struktur zum Hervorheben von primären Cyberbedrohungen im Jahr 2021 erhalten. Leser der letzten Ausgaben werden feststellen, dass die Bedrohungskategorien entsprechend einer Bemühung hin zu einer neuen Bedrohungstaxonomie der Cybersicherheit, die zukünftig eingesetzt werden soll, konsolidiert wurden.

Dieser Bericht ist wie folgt gegliedert:

Kapitel 2 untersucht die Trends in Verbindung mit Bedrohungsakteuren (z. B. staatlich geförderte Akteure, Computerkriminelle, Hacker-for-hire-Akteure und Hacktivisten).
Kapitel 3 bespricht wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Ransomware.
Kapitel 4 stellt wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Schadprogrammen vor.
Kapitel 5 beschreibt wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Cryptojacking.
Kapitel 6 hebt wesentliche Erkenntnisse, Vorfälle und Trends mit Bedrohungen durch elektronische Post hervor.
Kapitel 7 bespricht wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Bedrohungen für Daten.
Kapitel 8 stellt wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Bedrohungen für Verfügbarkeit und Integrität vor.
Kapitel 9 betont die Bedeutung von hybriden Bedrohungen und beschreibt wesentliche Erkenntnisse, Vorfälle und Trends im Zusammenhang mit Desinformation und Fehlinformation.
Kapitel 10 legt den Schwerpunkt auf wesentliche Erkenntnisse, Vorfälle und Trends mit Bezug auf nicht-arglistige Bedrohungen.
Anhang A stellt die für jede Bedrohung üblicherweise eingesetzten Techniken auf der Grundlage des Rahmens MITRE ATT&CK® vor.

[11] CIA - Words of Estimative Probability https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

Anhang B umfasst bemerkenswerte Vorfälle für jede Bedrohung, die im Laufe des Berichtszeitraums beobachtet wurden.