CYBER RISK AUDIT MATRIX

ENCRYPT 4.0

Kofinanziert von der Europäischen Union

Das Projekt ENCRYPT4.0 (2020-1-RO01-KA202-079983) wurde mit Unterstützung der Europäischen Kommission gefördert. Diese Veröffentlichung gibt nur die Ansichten des Verfassers wieder, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.

Inhalt

1. EINLEITUNG 3
2. CRAM WERTVERSPRECHEN 4
3. DIE METHODIK DER CYBER RISK AUDIT MATRIX 8
4. CYBER RISK AUDIT MATRIX (CRAM) 9
4.1 CYBER-RISIKEN AUDIT MATRIX KATEGORIEN 9
5. CYBERSICHERHEITS-AUDITS 11
6. PROJEKT UND PARTNER 23
BIBLIOGRAPHISCHE HINWEISE 24
ANHANG A - SAMMLUNG BESTEHENDER STANDARDS FÜR CYBERSICHERHEITSRISIKEN 25

1. EINLEITUNG

Produktivität, Qualität und Kosten in der Fertigung können potenziell von dramatischen Verbesserungen durch die zunehmende Konnektivität von Industrie 4.0, den Einsatz digitaler Berechnungen und die Speicherung von Off-Site-Daten profitieren. Für produzierende KMU sind jedoch Risiken verbunden, wenn z. B. Wettbewerber, oder Angreifer möglicherweise auf ihre Daten zugreifen. Cyberangriffe werden immer häufiger und werden in der Regel durchgeführt, um vertrauliche und/oder proprietäre Daten zu extrahieren oder zu stehlen, erfasste Daten zu manipulieren, um unerwünschte Effekte zu verursachen und Kapitalanlagen zu zerstören (Margot Hutchins & Stefanie Robinson, 2015). Cyberangriffe können definiert werden als "ein Angriff über den Cyberspace, der auf die Nutzung des Cyberspace durch ein Unternehmen abzielt, um eine Computerumgebung / -infrastruktur zu stören, zu deaktivieren, zu zerstören oder böswillig zu kontrollieren; oder die Integrität der Daten zu zerstören oder kontrollierte Informationen zu stehlen" (National Institute for Standards and Technology, 2012, S. B3). Das Weltwirtschaftsforum (2017) priorisiert zwei Lösungen zur Bewältigung innovationsgetriebener Cyberrisiken: i) Cyber-Risikomessung und ii) Cybersicherheitsbewertung. Im Jahr 2019 wurden Datenbetrug oder -diebstahl und Cyberangriffe vom Weltwirtschaftsforum als die viert- und fünftwahrscheinlichsten Risiken identifiziert (Weltwirtschaftsforum, 2020), im Jahr 2020 hat es Cyber-bezogene Probleme wie Cyberangriffe und Datenbetrug oder -diebstahl in der Liste der Top 10 der langfristigen Risiken identifiziert.

Die Fertigungsindustrie benötigt Werkzeuge, um Cyberrisiken in ihre bestehenden Risikomanagementprozesse zu integrieren. In diesem Zusammenhang adressiert Encrypt 4.0 diesen identifizierten Bedarf mit Schwerpunkt auf der Cybersicherheitsbewertung durch die Entwicklung der Cyber Risk Audit Matrix (CRAM). Das CRAM ist ein umfassendes Instrument, das Manager von produzierenden KMU dabei unterstützen soll, eine umfassende Analyse ihrer Prozesse unter Berücksichtigung des Einsatzes innovativer Industrie 4.0-basierter technologischer Lösungen durchzuführen, Cyberrisiken zu identifizieren und sie bei der Entwicklung und Einrichtung effektiver Kontrollen vor Ort zu unterstützen. Das CRAM wird unter Berücksichtigung der Expertise aus nationalen, EU- und weltweiten Standards (Anhang A) sowie des Feedbacks von Cybersicherheitsexperten aus sechs europäischen Ländern – Österreich, Portugal, Rumänien, Bulgarien, Zypern und Spanien – entwickelt.

- Dieses Dokument umfasst a) das CRAM-Wertversprechen, b) die CRAM-Methodik, c) die Beschreibung der Cyber Risk Audit Matrix-Kategorien, d) die Schritte zur Durchführung von Cybersicherheitsaudits e) bibliographische Referenzen.

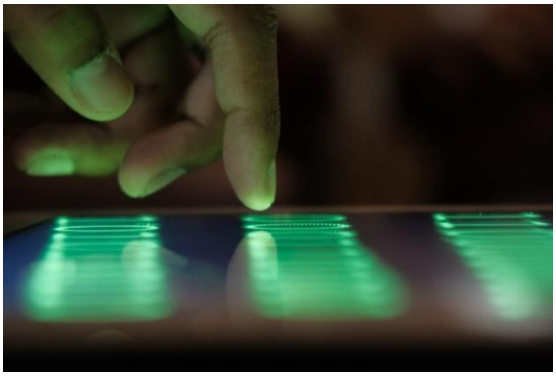
ENCRYPT 4.0 konzentriert sich auf die Bewertung der Cybersicherheit durch die Entwicklung der Cyber Risk Audit Matrix

2. CRAM WERTVERSPRECHEN

Die **Cyber Risk Audit Matrix (CRAM)** wird es intelligenten Fabriken ermöglichen, einen systematischen Überblick über ihre Cyber-Risikolandschaft zu geben und ein genaues Profil des Cyber-Bedrohungsrisikos zu erstellen. Das Encrypt 4.0 CRAM wird es intelligenten Fabriken ermöglichen, konsistente Echtzeit-Datenanalysen durchzuführen und ihre Cyber-Risiken basierend auf einer spezifischen und umfangreichen Matrix zu bewerten.

Die Cyber Risk Audit Matrix wird ein Analyseinstrument sein, das die produzierenden Unternehmen dabei unterstützt, Risiken zu identifizieren, zu analysieren, zu priorisieren und Schutzmaßnahmen zeitnah zu etablieren. Eines der drängendsten Probleme der digitalen Welt ist in den letzten Jahren die Cybersicherheit und der Datenschutz. Im Jahr 2019 zählte das Weltwirtschaftsforum (WEF) Cyberangriffe zu den fünf wichtigsten globalen Risiken.

Im Jahr 2020, mit der COVID-19-Pandemie, erhöhte die höhere Abhängigkeit von Konnektivität und digitaler Infrastruktur aufgrund des globalen Lockdowns die Möglichkeiten für Cyber-Intrusionen und -Angriffe. Gleichzeitig verlagern Cyberkriminelle, um den Schaden und den finanziellen Gewinn zu maximieren, ihre Ziele von Einzelpersonen und kleinen Unternehmen auf Großunternehmen, Regierungen und kritische Infrastrukturen, die eine entscheidende Rolle bei der Reaktion auf den Ausbruch spielen (INTERPOL G. S., 2020). "Cyberangriffe stellen eine größere Gefahr für Demokratien und Volkswirtschaften dar als Waffen und Panzer." (Juncker, 2017)



Cybersecurity Ventures, der weltweit führende Forscher in der globalen Cyberwirtschaft, prognostizierte, dass "die globalen Schäden im Zusammenhang mit Cyberkriminalität im Jahr 2021 sechs Billionen Dollar erreichen werden, was mehr sein wird als alle Naturkatastrophen in einem Jahr". Der offizielle jährliche Cybercrime-Bericht 2019 besagt, dass "Ende 2016 alle 40 Sekunden ein Unternehmen einem Ransomware-Angriff zum Opfer fiel", und die Prognosen gehen davon aus, dass diese Zahl bis 2021 auf alle 11 Sekunden steigen wird. (Cybersecurity Ventures, 2020)(Cybersecurity Ventures, 2019)

Cyberangriffe auf kritische Infrastrukturen, die vom WEF-Expertennetzwerk als fünftgrößtes Risiko im Jahr 2020 eingestuft werden, sind in Sektoren wie Energie, Gesundheitswesen und Transport zur neuen Normalität geworden. Die Fertigung leidet jedoch unter zunehmenden Cyberangriffen, wie der 2020 Data Breach Investigations Report zeigte, der allein in den USA 922 Vorfälle, 381 mit bestätigter Datenoffenlegung, detailliert beschreibt (Verizon, 2020). Die Organisationen der Cyberkriminalität schließen sich zusammen und ihre Wahrscheinlichkeit der Aufdeckung und Strafverfolgung wird in den Vereinigten Staaten auf bis zu 0,05% geschätzt, "Cybercrime-as-a-Service ist ein wachsendes Geschäftsmodell, da die zunehmende Komplexität

der Tools im Darknet bösartige Dienste erschwinglicher und für jedermann leichter zugänglich macht" (World Economic Forum, 2020).

Die Verteidigungsfähigkeit von KMU ist im Vergleich zu größeren Unternehmen in der Regel schwächer, und zahlen deuten darauf hin, dass sich nur 14 % der betroffenen KMU aus eigener Hand erholen können. Darüber hinaus stellt die National Cyber Security Alliance fest, dass 60% der KMU, die einem Cyberangriff unterzogen werden, ihr Geschäft innerhalb von 6 Monaten verlieren und "Hersteller aufgrund der Konnektivität in IT- und OT-Systemen (Operational Technologies) durch die Digitalisierung von Industrie 4.0 viel anfälliger für Bedrohungen ihrer Sicherheit sind". (Verizon, 2017)

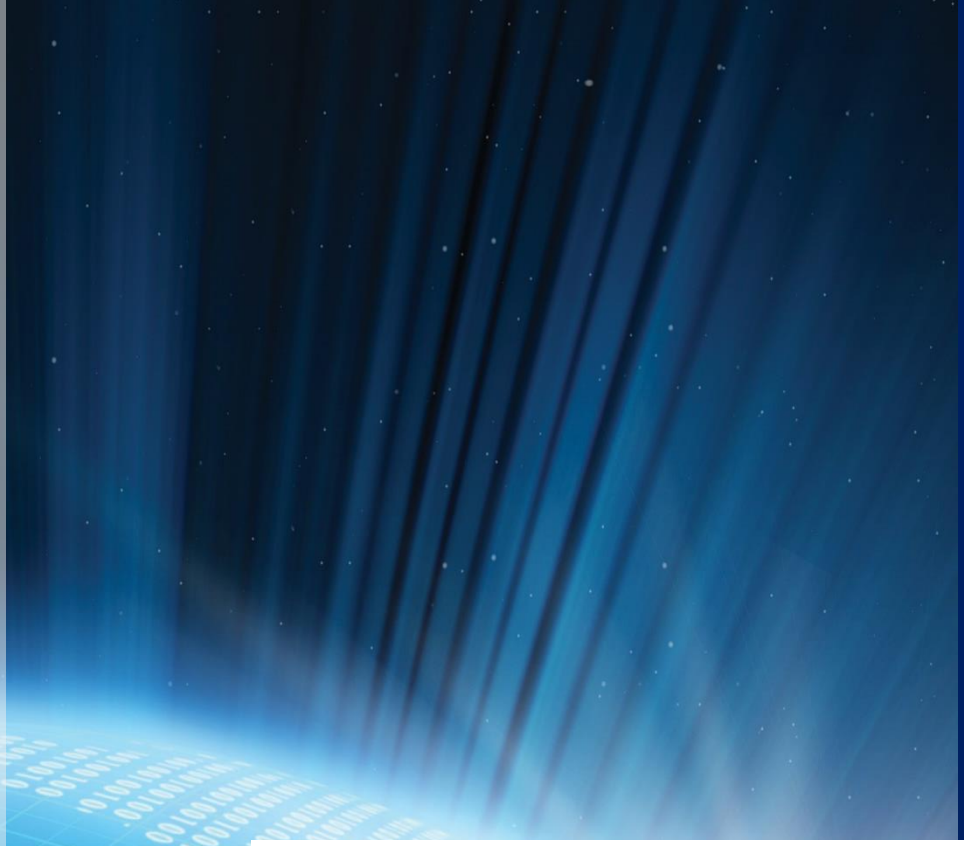
Die meisten produzierenden Unternehmen, die versuchen, einen Wettbewerbsvorteil zu erhalten, der sich an die Praktiken von Industrie 4.0 anpasst, unternehmen sporadische Anstrengungen, investieren in Kontrollsysteme und externe Berater, aber ihnen fehlt ein integrierter Ansatz für das Cyber-Risikomanagement. Ihre Bemühungen scheitern daran, die sich schnell entwickelnden Cyberbedrohungen effektiv zu bekämpfen, da die meisten Fertigungssysteme traditionell so entwickelt wurden, dass sie sich auf Betriebssicherheit und hohe Leistung und nicht auf IT-Sicherheit konzentrieren. Darüber hinaus waren die Hersteller in Bezug auf die Sicherheit in der Vergangenheit hauptsächlich um die Sicherung ihrer OT-Umgebung besorgt und vernachlässigten oft die IT-Sicherheit, "das Aufkommen von Industrie 4.0 führt neue Technologien in traditionelle OT-Umgebungen ein und daher müssen sich mit OT vertraute Menschen, die in solchen Umgebungen arbeiten, anpassen". Mitarbeiter verwenden häufig potenziell widersprüchliche Informationen, um einige Aspekte des Cyberrisikos zu beschreiben oder zu bewerten. (EU-Agentur für Cybersicherheit, 2019)

Die Cyber Risk Audit Matrix (CRAM) wird wichtige Risikoindikatoren skizzieren, die leicht auf Echtzeitdaten angewendet werden können. Das CRAM wird es den Mitarbeitern ermöglichen, nicht nur eine langfristige Cybersicherheitsstrategie zu entwickeln, sondern auch schnell tägliche Berichte zu erstellen. Dies zeigt das tatsächliche Risikoniveau für die Prozesse zu einem bestimmten Zeitpunkt, von entscheidender Bedeutung in der Fertigungsumgebung, da die Aufrechterhaltung der Produktion eine kritische ist und die kürzeste Minderung bestimmter Prozesse irreparable Auswirkungen haben und einen großen finanziellen Verlust verursachen kann. Sicherheitsrisiken in der Fertigung werden immer komplexer und entwickeln sich weiter, so dass es von großer Bedeutung ist, produzierende KMU mit dem geeigneten Analysewerkzeug auszustatten, um die Vorsichtsmaßnahmen zu skizzieren, die täglich im Fertigungsumfeld zu berücksichtigen sind. Im Gegensatz zu Fehlern in mechanischen Prozessen, die als statisch eingestuft werden können, sind Cybersicherheitsfehler dynamisch, da sie eng mit menschlichen Interaktionen verbunden sind.

Das **Hauptziel von CRAM** ist es, **führenden industriellen Unternehmen** einen Einblick in die potenziellen **Cybersicherheitsrisiken in ihren**

Die Cyber Risk Audit Matrix wird wichtige Risikoindikatoren skizzieren, die leicht auf Echtzeitdaten angewendet werden können

Systemen zu geben und sie bei der Annahme **einer effektiven Strategie zur Risikominderung** zu unterstützen. Da nur begrenzte Forschung im Bereich der Cybersicherheitsrisikobewertung in Fertigungssystemen verfügbar ist, wird das Encrypt 4.0 CRAM ein innovatives Werkzeug darstellen, das in die Risikomanagementpolitik der produzierenden Unternehmen integriert werden soll.

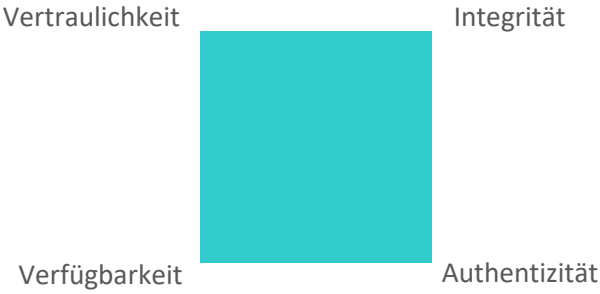


Das Hauptziel von CRAM ist es, führenden industriellen Unternehmen einen Einblick in die potenziellen Cybersicherheitsrisiken in ihren Systemen zu geben und sie bei der Annahme einer effektiven Strategie zur Risikominderung zu unterstützen.

Das CRAM wurde unter Berücksichtigung des CIAA-Quartetts entworfen

3. DIE METHODIK DER CYBER RISK AUDIT MATRIX

Das CRAM wurde entworfen unter Berücksichtigung des **CIAA** Quartett von **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Authentizität**. Zwei Hauptaspekte werden gemessen: **Risikowahrscheinlichkeit** und **Auswirkungen von Risiken**, zugeschnitten auf **Anforderungen** von produzierenden KMU mit dem Potenzial, leicht in die individuelle Organisationskultur eines bestimmten Unternehmens geformt und angepasst zu werden.



Die CRAM umfassen auch: i) Risikonummer, ii) Risikokategorie, iii) Risikoquelle, iv) Risikobeschreibung, v) potenzielle Kosten im Zusammenhang mit den Folgen des Risikos, vi) Organisationsabteilung, die betroffen sein könnte, vii) bereits gesetzte Maßnahmen, viii) Risikoauswirkungen, ix) Risikowahrscheinlichkeit, x) Gesamtrisikoniveau, xi) Auslöser, xii) durchzuführende Maßnahmen zur Risikominimierung, xiii) potenzielle Kosten der Maßnahmen, xiv) Frist, xv) für das Risikomanagement verantwortliche Person, xvi) für die Überwachung zuständige Aufsicht und xvii) Wirksamkeitsbewertung.

Im Folgenden finden Sie die Wichtigsten Konzepte, aus denen die Cyber Risk Audit Matrix besteht:

Verfügbarkeit: Gewährleistung eines zeitnahen und zuverlässigen Zugangs zu Informationen.

Authentizität: Sicherstellung der Dateneigenschaft, echt und originell zu sein, verifiziert werden zu können und Vertrauen in die Gültigkeit einer Übertragung, einer Nachricht oder eines Nachrichtenursprungsgebers zu haben. (Encrypt 4.0-Projekt, 2020).

Cybersicherheitsbewertung: Verbesserte Leitlinien und Bewertungsmechanismen für die Cybersicherheit, einschließlich gemeinsamer Grundsätze für Cybersicherheitsbewertungen, eines punktebasierten Bewertungsmechanismus und praktischer Verbesserungsschritte, die es Unternehmen ermöglichen, ihre

Cybersicherheitsbereitschaft zu bewerten und zu verbessern. (Weltwirtschaftsforum, 2017)

Vertraulichkeit: Aufrechterhaltung (kontrollierter) Beschränkungen des Zugriffs und der Offenlegung von Informationen, einschließlich Mitteln zum Schutz der Privatsphäre und proprietärer Informationen.

Auswirkung: Die bewerteten potenziellen Auswirkungen, die sich aus einer Gefährdung der Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationstyps ergeben, ausgedrückt als Wert von *niedrig, moderat, hoch.*

Integrität: Schutz vor unsachgemäßer Änderung oder Zerstörung von Informationen und einschließlich der Gewährleistung der Unleugbarkeit und Authentizität von Informationen.

Wahrscheinlichkeit: Ein gewichteter Faktor, der auf einer subjektiven Analyse der Wahrscheinlichkeit basiert, dass eine bestimmte Bedrohung in der Lage ist, eine bestimmte Schwachstelle oder eine Reihe von Schwachstellen auszunutzen.

Beschreibungen, die vom Leitfaden für die Durchführung von Risikobewertungen (National Institute of Standards and Technology, 2012) inspiriert sind.

4. CYBER RISK AUDIT MATRIX (CRAM)

Encrypt 4.0 CRAM stellt ein umfassendes Instrument dar, das Manager von produzierenden KMU dabei unterstützen soll, eine umfassende Analyse ihrer Prozesse unter Berücksichtigung des Einsatzes innovativer Industrie 4.0-basierter technologischer Lösungen durchzuführen und Cyberrisiken zu identifizieren und sie bei der Gestaltung und Einrichtung effektiver Kontrollen vor Ort zu unterstützen.

4.1 CYBER-RISIKEN AUDIT MATRIX KATEGORIEN

Diese Kategorien wurden aus einer durchgeführten Forschung und Analyse von über 20 Standards (Anhang A) im Bereich Informationssicherheit und Datenschutz sowie aus 12 durchgeführten Tiefeninterviews mit Cybersicherheitsexperten aus Österreich, Portugal, Rumänien, Bulgarien, Zypern und Spanien abgeleitet.

Tabelle 1. Kategorien der Cyber Risks Audit Matrix

Risikokategorie	Beschreibung der Risikokategorie
Personal	Identifizierung der Risiken, die mit den Personalressourcen des Unternehmens verbunden sind. Die Risiken, die mit den Rollen und Verantwortlichkeiten des Personals des Unternehmens, der Entscheidungsfindung, dem Management von Identitäten, der Kontrolle von Zugriffen, der Sensibilisierung ...
Geistiges Eigentum	Identifizierung der Risiken, die mit dem geistigen Eigentum des Unternehmens verbunden sind. Geistiges Eigentum umfasst gewerbliches Eigentum, Urheberrechte und verwandte Schutzrechte und verleiht das Recht zur ausschließlichen Nutzung der jeweiligen technischen, kommerziellen und industriellen Informationen. Das gewerbliche Eigentum zielt darauf ab, Erfindungen, Patente, Marken und Projekte zu schützen, die unter ausschließlichen Nutzungs-, Produktions- und Vermarktungsrechten fallen.
Industrial Control Systems (ICS) **Sicherheit**	ICS-Sicherheit umfasst die Sicherheit und Sicherung industrieller Steuerungssysteme sowie der notwendigen Soft- und Hardware, die vom System verwendet werden.
Produkte	Identifizierung der Risiken, die mit den Produkten verbunden sind. Das Auftreten dieser Art von Risiko kann die von der Organisation hergestellten Produkte gefährden.
Rechtliche Risiken für Cybersicherheit	Identifizierung der Risiken, die mit rechtlichen und regulatorischen Verantwortlichkeiten verbunden sind. Das Auftreten dieser Art von Risiko kann die rechtlichen und / oder regulatorischen Verantwortlichkeiten der Organisation gefährden.
Supply-Chain-Angriffe	Identifizierung von Schwachstellen in der Lieferkette. Die Organisation muss Risikomanagementprozesse der Liefer- und Logistikkette definieren, bewerten und verwalten. Identifizierung der Links zu Anbietern mit schlechter Sicherheitslage.
Technologie, IKT und Betriebssicherheit	Identifizierung der Risiken, die mit Technologie, IKT und Unternehmensbetrieb verbunden sind. Zur Bewältigung der Gefahren, die sich aus funktionsbedingten Unzulänglichkeiten der beabsichtigten Funktionalität, Betriebsstörungen oder durch vernünftigerweise vorhersehbaren Missbrauch/Fehler der Mitarbeiter im Zusammenhang mit Technologie, IKT und Betrieb ergeben.
Kundschaft	Das Auftreten eines bestimmten Risikos kann den Service für die Kunden des Unternehmens gefährden oder die Daten der Kunden gefährden.
Physische Cybersicherheit	Physische Cybersicherheit ist der Schutz von cyber-physischen Systemen, Internet-of-Things-Geräten, der Schutz von Menschen, Eigentum und physischen Vermögenswerten vor Handlungen und Ereignissen, die Schäden oder Verluste verursachen könnten.

5. CYBERSICHERHEITS-AUDITS

5.1 WAS IST EIN CYBERSECURITY AUDIT?

Die vierte industrielle Revolution oder Industrie 4.0 hat eine Reihe oder neue Technologien gebracht, die die physische und die digitale Welt der Geschäftsprozesse in integrierten intelligenten Systemen verbinden. Dies bringt viele Möglichkeiten zur Verbesserung von Prozessen und Gesamtleistung, aber auch viele neue Verantwortlichkeiten und Bedrohungen mit sich. Das höhere Maß an Konnektivität zwischen allen Systemen durch das Internet der Dinge, Cloud Computing und viele andere Technologien, neben vielen Vorteilen, stellt Unternehmen vor neue Herausforderungen in Bezug auf die Sicherheit der Informationen, Big Data usw., die von diesen integrierten Systemen verarbeitet werden. Aus diesem Grund benötigen Unternehmen und insbesondere KMU Werkzeuge, die sie dabei unterstützen, ihre Schwachstellen in Bezug auf die Sicherheit der Industrie 4.0-Technologien, die sie haben, zu überprüfen und zu analysieren. Ein wirksames Instrument zur Umsetzung dieser Überprüfung ist die Durchführung von Cybersicherheitsaudits.

Ein Cybersicherheitsaudit stellt eine Bewertung der Leistung anhand von Spezifikationen, Standards, Kontrollen oder Richtliniendar.

Ein Cybersicherheitsaudit stellt eine Bewertung der Leistung anhand von Spezifikationen, Standards, Kontrollen oder Richtlinien dar (CyLumena, 2020). Cybersicherheitsaudits werden in der Regel anhand einer Checkliste von Kontrollen (Kontrollbibliothek) durchgeführt, die auf der Grundlage bestimmter Standards für Cybersicherheit (national, international, unternehmensintern) und / oder Unternehmensverfahren und / oder -richtlinien definiert sind. Ziel eines Cybersicherheitsaudits ist es, Organisationen dabei zu unterstützen, zu beurteilen, ob sie über geeignete Sicherheitsmechanismen verfügen, indem sicherheitslücken identifiziert oder die angewandten Verfahren und Richtlinien überprüft werden. Cybersicherheitsaudits helfen Unternehmen zu überprüfen, was sich in ihrem Netzwerk befindet, was geschützt werden muss und welche Lücken in ihren bestehenden Schutzmaßnahmen bestehen, damit sie Verbesserungen vornehmen können (Dosal, 2020).

CYBERSICHERHEITSAUDITS VS. CYBERSICHERHEITSBEWERTUNG

Cybersicherheitsaudits unterscheiden sich von Cybersicherheitsbewertungen. Während es bei der Cybersicherheitsaudit darum geht, ob bestimmte Kontrollen eingerichtet wurden, zielt die Cybersicherheitsbewertung darauf ab, die Wirksamkeit dieser Kontrollen zu bewerten (Aldorisio, 2020). Bewertungen können ein gewisses Maß an Audit beinhalten, aber nicht immer. Cybersicherheitsaudits können je nach Ziel auch angewendet werden, wenn eine Organisation ihre Einhaltung bestimmter Gesetze oder Standards bewerten möchte, in diesem Fall wird das Audit in der Regel von einem Dritten mit der erforderlichen Kompetenz durchgeführt. Die Cybersicherheitsbewertungen hingegen könnten intern von Personen innerhalb der Organisation durchgeführt werden, die über gute Kenntnisse der Cybersicherheitsinfrastruktur verfügen.

EXTERNE VS. INTERNE CYBERSICHERHEITSAUDITS

Externe Audits werden von Fachleuten durchgeführt, insbesondere wenn das Ziel des Audits darin besteht, die Zertifizierung nach bestimmten Cybersicherheitsstandards und die Konformitätsbewertung anhand offizieller Standards, Gesetze usw. zu ermöglichen. Interne Cybersicherheitsaudits (First-Party-Audits) können von internen Experten durchgeführt werden, die einen guten Überblick über Unternehmensprozesse, sowie der Cybersicherheitsarchitektur besitzen. Gemäß DSGVO (GDPR.EU N.d.) ist jedes Unternehmen gesetzlich verpflichtet, einen benannten Datenschutzbeauftragten zu haben, der sich mit dem Datenmanagement bewusst ist - welche Informationen in und aus dem Unternehmen kommen, in welchen Prozessen es verwendet wird und wie es verwaltet wird. Daher könnte eine natürliche Wahl für die Durchführung eines internen Cybersicherheitsaudits der

benannte Datenschutzbeauftragte oder ein Unternehmensteam sein, abhängig vom Umfang des Audits. In den nächsten Abschnitten dieses Dokuments werden wir einen kombinierten Ansatz zur Durchführung eines internen Cybersicherheitsaudits und einer Bewertung auf der Grundlage mehrerer zuvor genannter Kategorien vorstellen, die im Auditierungsprozess berücksichtigt werden müssen.

5.2 WIE FÜHRE ICH EIN INTERNES CYBERSICHERHEITSAUDIT DURCH?

Das Ziel dieses Abschnitts ist es, eine leicht verständliche Anleitung für die Durchführung von Selbst-Cybersicherheits-Audits (internes Cybersicherheitsaudit) bereitzustellen, die als effektives Instrument zur Bewertung der Cyber- und Datensicherheit in Ihrer Organisation und / oder als Vorbereitung für externe (Drittanbieter-) Cybersicherheitsaudits dienen können.

SCHRITT 1: Definieren Sie die Sicherheitsprioritäten Ihrer Organisation und den Umfang des Audits

In diesem Stadium muss die Person oder das Team, das mit der Durchführung des Audits beauftragt wurde, den Umfang des Auditierungsprozesses ermitteln. Ein guter Ausgangspunkt ist die Auflistung aller Cyber-Assets des Unternehmens, z. B. Cyber-Assets, die mit kritischen Assets verbunden sind, wie zum Beispiel: Kontrollsysteme; Datenerfassungssysteme; Netzwerkausrüstung; Hardwareplattformen für virtuelle Maschinen oder Speicher; Sekundäre oder unterstützende Systeme wie Virenscanner, HLK-Systeme und unterbrechungsfreie Stromversorgungen (USV) (n.d., Versify Solutions);

Als nächstes müssen Sie bewerten, welche die kritischen Cyber-Assets (CCA) sind. Gemäß dem Critical Infrastructure Protection (CIP) -Standard, Version 4 der North American Electric Reliability Corporation (NERC), ist ein CCA "jedes Gerät, das ein routingfähiges Protokoll verwendet, um außerhalb des elektronischen Sicherheitsperimeters (ESP) zu kommunizieren, ein routingfähiges Protokoll innerhalb eines Kontrollzentrums verwendet oder auf die Einwahl zugegriffen werden kann". (2011, Flick & Morehouse).

Einfacher ausgedrückt, können Die Vermögenswerte von Computerausrüstung bis hin zu verschiedenen Systemen und sensiblen Kunden- und Unternehmensinformationen, internen Dokumentationen und Kommunikationssystemen variieren.

Sobald die kritischen Cyber-Assets identifiziert wurden, müssen Sie identifizieren, wo die kritischen Sicherheitsparameter liegen und somit segmentieren, was in den Audit-Umfang aufgenommen wird (2019, LeCount). Sicherheitsparameter und -vermögenswerte werden von Unternehmen zu Unternehmen stark variieren, daher sind dieser erste Schritt und die richtige Definition des Prüfungsumfangs von entscheidender Bedeutung für die Effektivität des Prüfungsprozesses. Sobald der Überwachungsumfang definiert ist, können Sie mit dem nächsten Schritt fortfahren – der Identifizierung potenzieller Bedrohungen.

SCHRITT 2: Identifizieren Sie die potenziellen Risiken und Bedrohungen

Basierend auf ausführlichen Interviews mit 12 Experten auf dem Gebiet der Cybersicherheit hat das ENCRYPT 4.0-Konsortium neun mögliche Risikokategorien identifiziert und eine Liste potenzieller Bedrohungen zusammengestellt, die jede dieser Kategorien für kritische Cyber-Assets darstellen kann. Das ENCRYPT-Modell umfasst die folgenden neun Risikokategorien, die berücksichtigt werden müssen: (1) Humanressourcen; (2) Geistiges Eigentum; (3) Sicherheit industrieller Kontrollsysteme (ICS); (4) Produkte; (5) Rechtliche Risiken im Bereich der Cybersicherheit; (6) Angriffe auf die Lieferkette; (7) Technologie, IKT und Betriebssicherheit; (8) Kunden; (9) Cybersicherheit physisch. Denken Sie daran, dass abhängig von den Geschäftsaktivitäten, dem Geschäftsmodell

und dem Betriebssektor Ihres Unternehmens möglicherweise nicht alle Kategorien auf Sie zutreffen, oder Sie entscheiden, dass Sie keine kritischen Cyber-Assets haben, die mit diesen Kategorien verbunden sind. Um diese zu bewerten, überprüfen Sie Anhang 1 und wählen Sie die für Ihr Unternehmen zutreffenden Kategorien und die Bedrohungen aus, die Sie für relevant halten, abhängig von den identifizierten entscheidenden Cyber-Assets in Ihrem Unternehmen.

SCHRITT 3: Priorisieren Sie die Risiken

In diesem entscheidenden Schritt müssen Sie die Liste der potenziellen Bedrohungen überprüfen, die Sie für Ihr Unternehmen für anwendbar halten, und nach einer Reihe von Kriterien entscheiden, welche Risiken sehr wahrscheinlich und mit potenziell schwerwiegenderen nachteiligen Auswirkungen sind. Aus diesem Grund hat das ENCRYPT 4.0-Konsortium eine Risikobewertungsmethodik entwickelt, die die folgenden Komponenten berücksichtigt:

- Potenzielle Kosten im Zusammenhang mit den Folgen des Risikos;
- Abteilung(en) der Organisation, die möglicherweise betroffen sind;
- Mögliche Auswirkungen;
- Wahrscheinlichkeit – berücksichtigen Sie bei der Bewertung der Wahrscheinlichkeit Branchentrends, frühere Sicherheitsverletzungen;
- Risikostufe.

Sie können das entwickelte TOOL ENCRYPT 4.0 Cybersecurity Risk Assessment Matrix (CRAM) direkt verwenden, um die potenziellen Risiken einfach zu priorisieren.

SCHRITT 4: Überprüfen der aktuellen Sicherheitsmaßnahmen

Nachdem Sie die anwendbaren Risikokategorien und Bedrohungen für Ihr Unternehmen identifiziert haben, besteht der nächste Schritt darin, zu bewerten, ob Ihre kritischen Cyber-Assets und -Infrastrukturen für eine dieser Bedrohungen anfällig sind. Zu diesem Zweck müssen Sie die Sicherheitsprotokolle/-verfahren/-maßnahmen bewerten, die im Hinblick auf die Identifizierung potenzieller Sicherheitslücken, die geschlossen werden müssen, eingerichtet wurden. In Tabelle 2 finden Sie einige Leitfragen und Tipps, wie Sie beurteilen können, ob die bestehenden Sicherheitsmaßnahmen angemessen sind, dies hängt jedoch auch von den Bedrohungen ab, die Sie in jeder Kategorie für anwendbar halten.

Tabelle 2. Tipps zur Identifizierung von Sicherheitsmaßnahmen

Nein.	Kategorie	Tipps zur Überprüfung vorhandener Sicherheitsmaßnahmen
1	**Personalabteilung**	Überprüfung der Verteilung der Rollen und Verantwortlichkeiten im Zusammenhang mit Datenmanagement und -sicherheit; Cybersicherheit; Systemsteuerung usw. Sprechen Sie mit ernannten verantwortlichen Mitarbeitern in diesen Bereichen - fragen Sie sie, wie sie in bestimmten Situationen reagieren würden, welche Sicherheitsprotokolle sie implementieren würden, so dass Sie beurteilen können, ob die Mitarbeiter im Falle der Realisierung bestimmter Cybersicherheitsrisiken bewusst und vorbereitet sind; ob sie eine Schulung benötigen oder nicht. Analysieren Sie Unfälle und Sicherheitsverletzungen aufgrund von Fehlern der Mitarbeiter und wie sie gehandhabt wurden. Denken Sie, dass es noch etwas mehr geben könnte, um das Auftreten dieser Bedrohung in Zukunft weiter zu minimieren.
2	**Geistiges Eigentum**	Überprüfen Sie die Verteilung der Rollen und Verantwortlichkeiten im Zusammenhang mit der Verwaltung von geistigem Eigentum sowie Geschäftsgeheimnissen usw. Befragen Sie die verantwortlichen Mitarbeiter, lesen Sie relevante Dokumentationen zum Vermögensschutz wie Patente, Markenrechte. Wie wird diese Dokumentation aufbewahrt und verwaltet, wer hat Zugriff darauf? Gab es in der Vergangenheit Vorfälle im Zusammenhang mit Informationsverletzungen, fehlenden Informationen in diesem Bereich? Wie sie gehandhabt wurden, wird das Sicherheitsprotokoll aktualisiert?
3	**Sicherheit industrieller Steuerungssysteme (ICS)**	Wer hat Remote- und/oder physischen Zugriff auf das ICS? Wie wird der Fernzugriff auf ICS verwaltet? Gibt es Sicherheitskontrollen wie starke Authentifizierung, Zugriffskontrolle und Verschlüsselung, um vor unbefugtem Zugriff auf und Ausnutzung dieser Systeme zu schützen? Was sind physische Zutrittskontrollmaßnahmen? Verwenden Sie ICS-protokollfähige Firewalls, um Zugriffskontrollen für den ICS-Netzwerkverkehr zu erzwingen? Haben Sie ein Intrusion Prevention-System eingerichtet?
4	**Produkte**	Abhängig vom Produktionsprozess der Produkte müssen Sie identifizieren, in welchen Prozessen sensible Informationen behandelt werden und auf welche Weise sie verwaltet und verwaltet werden.

		Gibt es Geschäftsgeheimnisse im Zusammenhang mit der Produktherstellung usw. Wie stellt das Unternehmen sicher, dass diese Informationen sicher verwaltet werden? Was ist das Protokoll – Rollen und Verantwortlichkeiten, Verfahren usw.? Gibt es eine Kontrolle des physischen und Remote-Zugriffs auf Computer und Netzwerke? Produktionsanlagen etc.? Wie werden diese gesichert und kontrolliert?
5	**Rechtliche Risiken im Bereich Cybersicherheit**	Gibt es eine Kontrolle des physischen und Remote-Zugriffs auf Unternehmenscomputer und -netzwerke? Wie werden diese gesichert und kontrolliert? Wie werden rechtliche Daten verwaltet und verwaltet? Ist der Server gesichert? Wer hat Zugriff auf diese Informationen? Gab es in der Vergangenheit Sicherheitslücken? Wie wurden sie gehandhabt? Gibt es eine Möglichkeit, die Sicherheitsprotokolle basierend auf den neuesten Trends/ Ereignissen / Technologieentwicklungen zu verbessern?
6	**Supply-Chain-Angriffe**	Wer hat Zugang zu Supply Management Systemen? Gibt es Privileged Access Management? Wer hat Zugriff auf sensible Daten? Wie ist dieser Zugang gesichert? Haben Sie Honeytokens implementiert? Wie hoch ist der Grad der Zugriffskontrollen durch Serviceanbieter? Wie viele Anbieter haben Zugriff auf Software? Wird das Netzwerk des Anbieters auf Schwachstellen überwacht?
7	**Technologie, IKT und Betriebssicherheit**	Haben Sie strenge Richtlinien für mobile Sicherheit und Datenschutz? Sind alle Softwareanwendungen und Betriebssysteme auf dem neuesten Stand? Gibt es Zugriffskontrollen für kritische Cybersicherheitsressourcen? Überwachen Sie die Aktivität von Benutzerkonten, die Protokollierung und den Zugriff auf Ihr Netzwerk? Überprüfen Sie, ob Firewalls ordnungsgemäß konfiguriert sind, und stellen Sie sicher, dass Sie über eine Ende-zu-Ende-Verschlüsselung für vertrauliche Daten verfügen. Haben Sie Mechanismen eingerichtet, um Angriffe wie Phishing und Pharming zu erkennen und zu vermeiden?

8	**Kundschaft**	Wer hat Zugriff auf wichtige Kundendaten? Haben Sie backup von wichtigen Geschäftsdaten und Informationen?
9	**Physische Cybersicherheit**	Wie wird die Wartung von Geräten und kritischen Cybersicherheitsanlagen verwaltet? Wer hat physischen Zugriff auf Geräte und kritische Cybersicherheitsressourcen? Wie ist der Zugang gesichert?

SCHRITT 5: Festlegen/ Aktualisieren der Sicherheitsprotokolle basierend auf dem Audit

Nach Abschluss von SCHRITT 4 müssen Sie Ihre Liste der identifizierten Bedrohungen für Ihr Unternehmen anwendbar haben, um zu wissen, was Sie bereits tun und was möglicherweise fehlt, und angemessene Informationssicherheitskontrollen zu identifizieren, um das Bedrohungsrisiko zu neutralisieren oder zu beseitigen (2020, LeCount).

Informationssicherheitskontrollen sind Maßnahmen, die ergriffen werden, um Informationssicherheitsrisiken wie Verletzungen von Informationssystemen, Datendiebstahl und unbefugte Änderungen an digitalen Informationen oder Systemen zu reduzieren (Garcia, 2019). Das Hauptziel von Sicherheitskontrollen ist es, die Verfügbarkeit, Vertraulichkeit und Integrität von Daten und Netzwerken innerhalb eines Unternehmens zu schützen. Wie bereits erwähnt, werden Sicherheitskontrollen in der Regel nach einer Informations- oder Cybersicherheits-Risiko Bewertung implementiert und stellen ein gewünschtes Ergebnis von Cybersicherheitsbewertungen und -audits in Bezug auf die Behebung identifizierter tatsächlicher oder potenzieller Sicherheitslücken dar.

In Tabelle 3 wurden im Einklang mit dem Encrypt 4.0-Modell zur Risikobewertung der Cybersicherheit auf der Grundlage von Interviews mit Cybersicherheitsexperten aus 6 EU-Ländern zwei Arten von Kontrollen identifiziert – präventive und korrigierende Kontrollen in jeder der neun Risikokategorien. Basierend auf dem in SCHRITT 4 durchgeführten Audit kennen Sie bereits die Cybersicherheitsverfahren in Ihrer Organisation. In Tabelle 3 finden Sie einige Vorschläge für präventive und korrigierende Kontrollen für jede der Kategorien, die Sie in Ihrer Organisation möglicherweise vermissen.

Tabelle 3. Präventive und korrigierende Cybersicherheitskontrollen

Risikokategorie	Präventivmaßnahmen	Korrekturmaßnahmen
Personalabteilung	Einrichtung eines Schulungs- und Sensibilisierungsprogramms Identifizieren Sie eindeutig die Verwaltung von Identitäten, Authentifizierung und Kontrolle von Zugriffen Das Unternehmen hat eine Richtlinie, die Folgendes umfasst: ● Liste der autorisierten Software. ● Autorisiertes Software-Repository und Lizenzregistrierung.	Steuerung von Benutzerberechtigungen Implementieren Sie das Intrusion Detection System (IDS), um nicht autorisierten Zugriff auf einen PC oder ein Netzwerk zu erkennen Ändern Sie alle Passwörter nach einer möglichen Datenschutzverletzung Sperren von Konten, bei denen der Verdacht auf unbefugten Zugriff besteht

Risikokategorie	Präventivmaßnahmen	Korrekturmaßnahmen
	• Disziplinarische Sanktionen im Zusammenhang mit der Nichteinhaltung dieser Vorschriften. Vierteljährliche Drehung der Kennwörter ("Richtlinie für starke Kennwörter") Entwicklung von Disaster Recovery-Lösungen und Business Continuity-Plänen	Richten Sie nach Möglichkeit eine Zwei-Faktor-Authentifizierung ein.
Geistiges Eigentum	Angemessene Richtlinien und Verantwortlichkeiten für die Verwaltung von geistigem Eigentum Alle anwendbaren Vermögenswerte sollten durch eingetragene Patente, Urheberrechte und Marken geschützt werden. Relevante Vermögenswerte sollten überwacht und durch Versicherungen geschützt werden. Entwicklung von Maßnahmen, Richtlinien und Verantwortlichkeiten für das Reputationsmanagement	Regelmäßige Bewertung und Aktualisierung von Richtlinien und Verantwortlichkeiten Wenn ein eingetragenes Patent fehlt, müssen ein vorläufiges Patent, eine Marke und Urheberrechte eingeholt werden Regelmäßige Bewertung und Aktualisierung von Richtlinien und Verantwortlichkeiten
Industrielle Steuerungssysteme (ICS) Sicherheit	Entwicklung von Maßnahmen, Policies, Verantwortlichkeiten und schneller Reaktion im Falle eines Vorfalls	Regelmäßige Bewertung und Aktualisierung von Richtlinien und Verantwortlichkeiten.
Produkte	Bewertung von Workflow-Prozessen Standardisierung und Evolution Steuern des physischen Zugriffs auf Computer und Netzwerkkomponenten	Implementieren Sie einen mehrschichtigen Ansatz für jedes Risiko oder zumindest für diejenigen, die im konkreten Fall ein hohes Potenzial haben, um zumindest ein paar Schichten Schutz zu haben, egal wenn es um Technologien, Mitarbeiter, Prozesse, Kunden usw. geht.
Rechtliche Risiken für Cybersicherheit	Behalten Sie nur das, was Sie brauchen. Inventarisieren Sie die Art und Menge der Informationen in Ihren Dateien und auf Ihren Computern Daten schützen Vor der Entsorgung vernichten Update-Verfahren Mitarbeiter schulen/schulen	Betroffene identifizieren Betroffene Personen benachrichtigen Rechtsbeistand suchen

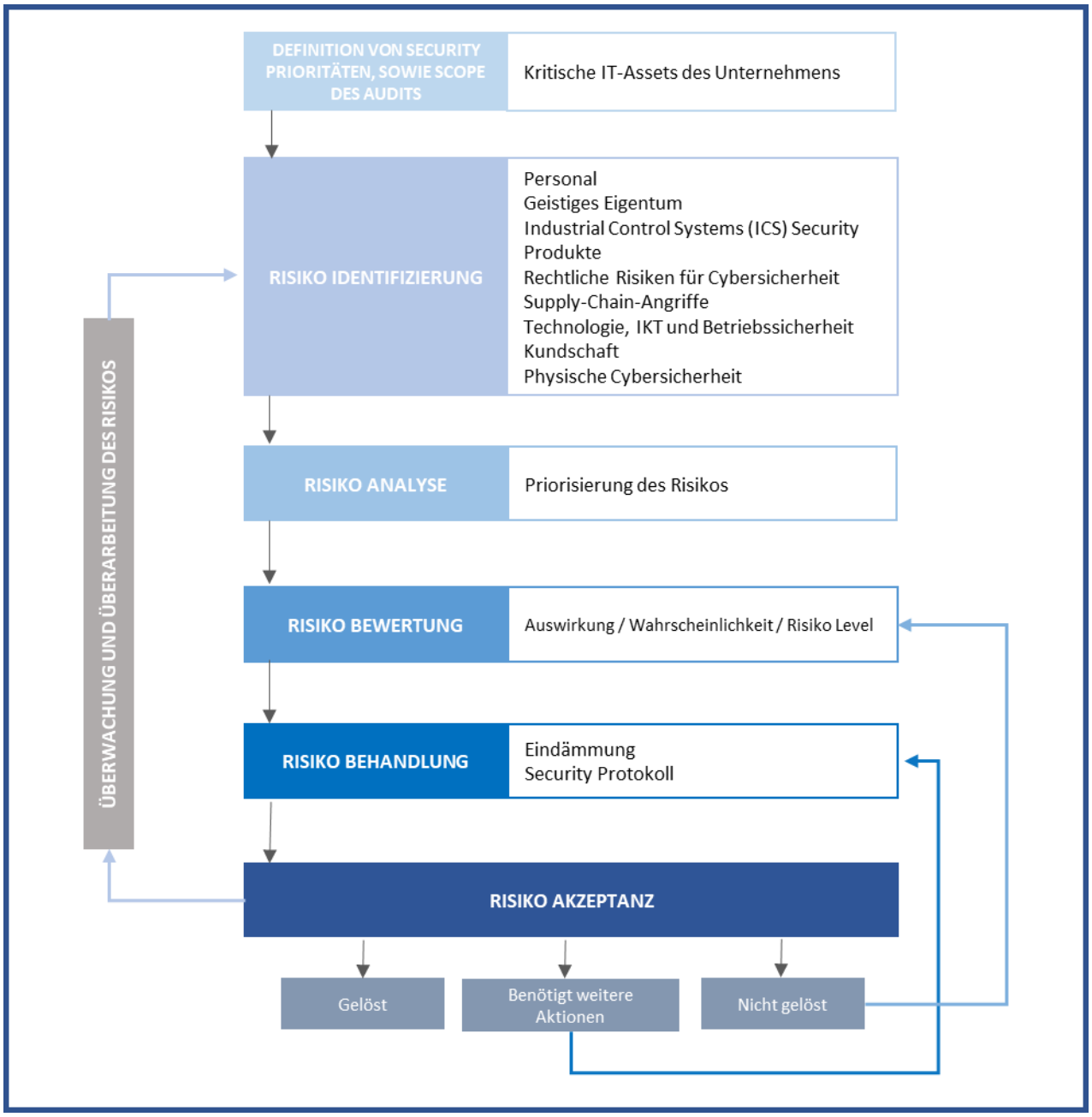
Risikokategorie	Präventivmaßnahmen	Korrekturmaßnahmen
	Steuern Sie die Computernutzung. Sichern Sie alle Computer.	
Supply-Chain-Angriffe	Honeytokens implementieren Sichere Verwaltung privilegierter Zugriffe Identifizieren Sie alle potenziellen Insider-Threads Identifizieren und Schützen anfälliger Ressourcen Minimieren Sie den Zugriff auf sensible Daten Regelmäßig Risikobewertungen von Drittanbietern anfordern Überwachen Des Anbieternetzwerks auf Schwachstellen Identifizieren Sie alle Datenlecks des Anbieters	Überprüfen Sie die Lizenzen in der gesamten Lieferkette der KMU Suchen Sie nach den Kontaktdaten Ihrer präventiven und korrektiven Wartung von KMU-Maschinen in der gesamten Lieferkette auf regionaler/lokaler Ebene
Technologie, IKT und Betriebssicherheit	Herunterladen und Installieren von Softwareupdates für Ihre Betriebssysteme und Anwendungen, sobald diese verfügbar sind Betriebssysteme und Firmware aktualisiert Installieren der Firewall zwischen dem Internet und dem LAN Identifizieren Kritischer Assets Sicherheitsbewusstsein, Backup und Recovery, Schwachstellen- und Patch-Management, Zugriffskontrollen anwenden, Verwenden Sie die Inhalts- und Whitelist-Filterung, Endpunkte richtig konfigurieren, Incident-Response-Prozesse einrichten, Verwenden Sie Threat-Intelligence-Lösungen und -Systeme.	Überprüfen Sie alle Betriebssystem- und Firmware-Fristen, die Sie in Ihren KMU haben, und überwachen Sie, ob alles aktualisiert wird Eine Firewall zwischen dem Internet und dem LAN installieren. Entfernen von Software, die illegal oder nicht im Software-Repository zulässig ist Standardinstallationen an allen Computergeräten Konfiguration von VPN, wenn eine Verbindung von außen hergestellt werden muss. Identifizierung und Korrektur des Problems. Überwachen und Aktualisieren der Sicherheitsrichtlinien und -regeln.

Risikokategorie	Präventivmaßnahmen	Korrekturmaßnahmen
	Ordnungsgemäß konfigurierte Firewalls, strenge mobile Sicherheitsrichtlinien, Ende-zu-Ende-Verschlüsselung, Audit-Protokollierung und die Autorisierung von Geräten für den Zugriff auf das Netzwerk sind einige der Praktiken, die die Bedrohungen durch die Verwendung mobiler Geräte in einem Unternehmensnetzwerk reduzieren. Bewerten Sie Software in Bezug auf Cybersicherheitsprinzipien. Sicherstellen, dass Betriebssysteme und alle Softwareanwendungen auf dem neuesten Stand sind, Sicherstellen, dass sensible Daten verschlüsselt sind, Datenschutzsoftware verwenden, Regelmäßige Überwachung der Aktivität von Benutzerkonten, Datenschutzeinstellungen für mobile Anwendungen verwalten, Strenge Gerätekontrollen für Wechselmedien durchsetzen, Etablieren Sie Mechanismen, um Angriffe wie Phishing und Pharming zu erkennen und zu vermeiden. Betrieb basierend auf Sicherheitsrichtlinien und -regeln.	
Kundschaft	Erstellen Sie Sicherungskopien wichtiger Geschäftsdaten und -informationen	Richten Sie nach Möglichkeit eine Zwei-Faktor-Authentifizierung ein Sperren von Konten, bei denen der Verdacht auf unbefugten Zugriff besteht Blockieren von IP-Adressen mutmaßlicher Bedrohungsakteure basierend auf erkannten Aktivitäten
Physische Cybersicherheit	Umsetzung eines Sicherheitsplans bei Bränden, Überschwemmungen, Diebstählen, Verlusten...	Seien Sie auf dem Gelände über die Gebäudesicherheit auf dem Laufenden und verfügen Sie über Brandschutzmaßnahmen.

Risikokategorie	Präventivmaßnahmen	Korrekturmaßnahmen
	Schalten Sie alle Werkzeuge oder Geräte aus, die nicht verwendet werden Um eine unterbrechungsfreie Backup-Stromversorgung zu haben oder eine zweite Notstromquelle zu erhalten Überprüfen Sie regelmäßig alle Geräte Backups durchführen Vorzugsweise alle Daten in der Cloud gehostet haben	Einsatz von Backup-Batterien für Ihre Computer, bzw. eine zweite Notfallenergiequelle beschaffen. "Sicherheitskopie" erstellen Integration eines Sicherheitsschalter Ersetzen oder Beheben beschädigter oder ausgefallener Geräte

GRAFISCHE ÜBERSICHT ÜBERDEN PROZESS MIT DEM CRAM

Hier wird der graphische Überblick über den Audit-Prozess dargestellt, indem das Encrypt 4.0 CRAM als Werkzeug verwendet wird. Es werden die entsprechenden Maßnahmen skizziert, die von der verantwortlichen Person in produzierenden KMU zu ergreifen sind, um eine umfassende Analyse ihrer Prozesse durchzuführen. Dabei werden die Cyberrisiken identifiziert und eine Unterstützung für wirksame Kontrollen entsprechend dem Fortschritt des Cyberangriffs geboten.



Der Encrypt 4.0 CRAM ist ein systematischer, kontinuierlicher Prozess. Es ist ein zyklischer Prozess, der, sobald er die Risiken identifiziert, analysiert, bewertet, bewertet, adressiert und akzeptiert hat, einen Risikoüberwachungs- und Überprüfungsprozess durchführen muss. Falls das Problem weiterhin besteht, müssen Sie weitere ergänzende Maßnahmen ergreifen, um das Problem zu lösen, und dazu müssen Sie zum vorherigen Schritt der Risikobehandlung zurückkehren. Und wenn das Problem ungelöst bleibt, müssen Sie das Risiko neu bewerten.

6. PROJEKT UND PARTNER

ENCRYPT 4.0

Eine Gemeinsame Cyber Personal-entwicklungsinitiative soll es der europäischen Industrie ermöglichen, den Mangel an Cybersicherheitsfachleuten zu überwinden

Das Projekt ENCRYPT4.0 (2020-1-RO01-KA202-079983) zielt darauf ab, das Management von KMU in der Fertigung zu einem proaktiven Ansatz für die Cybersicherheit zu bewegen, indem es sie bei der Analyse, Identifizierung und Bewältigung der Cyberrisiken und -bedrohungen unterstützt, die für ihre Organisation gelten. Durch die Förderunginteraktiven projektbasierten Lernens im Hinblick auf die Stärkung der Cybersicherheitsfähigkeiten und -kompetenzen der Mitarbeiter von KMU und/oder Cybersicherheitsfachleuten.

"George Emil Palade" Universität für Medizin, Pharmazie, Wissenschaften und Technologie von Târgu

Projektkoordinator

European Center for Quality Ltd., Consulting company - Bulgarien

Instituto de Soldadura e Qualidade, Technologische Einrichtung - Portugal

Avantalia, technologiebasiertes KMU - Spanien

FH Joanneum, Fachhochschule - Österreich

PCX Management, Computer & Information Systems Ltd. - Zypern

BIBLIOGRAPHISCHE HINWEISE

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

ANHANG A – SAMMLUNG BESTEHENDER STANDARDS FÜR CYBERSICHERHEITSRISIKEN

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Information Security (Cross-Industry)	ISO/IEC 27001:2018 Information security management systems – Requirements
	ISO/IEC 27002:2018 Code of practice for information security controls
	ISO/IEC 27003:2017 Information security management systems guidance
	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
	International Organisation for Standardisation and International Electrotechnical Commission
	ISO/IEC 27014:2013 Governance of information security
	ISO/IEC TR 27016:2014 Information security management - Organisational economics
	ISO/IEC 27032:2012 Guidelines for information security
	ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts
	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
	ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways
	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
	ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access
	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
	ISO/IEC 27040:2015 Storage security
	CSA Cloud Controls Matrix
	BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification
	PCI Data Security Standard
	ISF The Standard of Good Practice for Information Security
	UK Gov. Security policy framework
	UK Gov. Cyber essentials scheme
	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
	BSI 100-1 Information Security Management Systems (ISMS)
	BSI 100-2: IT- Grundschutz Methodology
	BSI 200-1 Information Security Management Systems (ISMS)
	BSI 200-2: IT- Grundschutz Methodology
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model

	ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components
	ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components
	ISO/IEC 19790:2012 Security requirements for cryptographic modules
	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC 27007:2017 Guidelines for information security management systems auditing
	ISO/IEC 27014:2020 Governance of information security
	ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	ISO/IEC 29147:2018: Vulnerability disclosure
	ISO/IEC 30111:2019: Vulnerability handling processes
	OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements
	ISO/IEC 27701:2019 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
	ISO/IEC TS 27100:2020 Information technology -Cybersecurity- Overview and concepts

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Risk Management	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
	ISO/IEC 27005:2016 Information security risk management
	ISO/IEC 31000 Risk management - Risk assessment techniques
	IEC 31010:2009 Risk management - Risk assessment techniques
	BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
	BSI 100-3: Risk Analysis based on IT-Grundschutz
	BSI 200-3: Risk Analysis based on IT-Grundschutz
	ISO/IEC 27005:2018 Information security risk management
	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Business Continuity Management	ISO 22301:2012 Business continuity management systems – Requirements
	ISO 22313:2012 Business continuity management systems – Guidance
	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
	100-4: Business Continuity Management
	OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Data Protection and Privacy	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29100:2011 Privacy framework
	ISO/IEC 29101:2013 Privacy architecture framework
	BSI BS 10012:2009 Data protection. Specification for a personal information management system
	CEN CWA 16113:2010 Personal Data Protection Good Practices
	OEVE/OENORM 17529:2020: Data protection and privacy by design and by default
	OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements
	ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29134:2017: Guidelines for privacy impact assessment
	ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping
	ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
	ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Incident Management	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management
	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
	ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
	ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Third-Party Management	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
	ISO/IEC 27035:2011 Information security incident management
	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Industrial security	OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
	OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
	OVE IEC TS 62351-100-1:2020 06 01