CySeReS KMU

Herzlich willkommen zum Webinar

In 5 Schritten zu Supply Chain Cyber Security

Projektteam CySeReS-KMU

12.10.2023 16:00 - 17:00 Uhr Online

FH Oberösterreich, Logistikum, Universität Passau, Technische Hochschule Deggendorf, THD, universität innsbruck, FH Salzburg, Interreg Bayern-Österreich, Kofinanziert von der Europäischen Union

Webinarreihe - Zusammenarbeit

Unter diesem Link können Sie sich für alle zukünftigen Webinare im Projekt CySeReS-KMU anmelden:
https://www.eventbrite.com/cc/webinarreihe-cyber-security-fur-kmus-in-sc-2470389

Interesse an einer Zusammenarbeit im Projekt?

Gerne melden unter: office@cyseres-kmu.eu

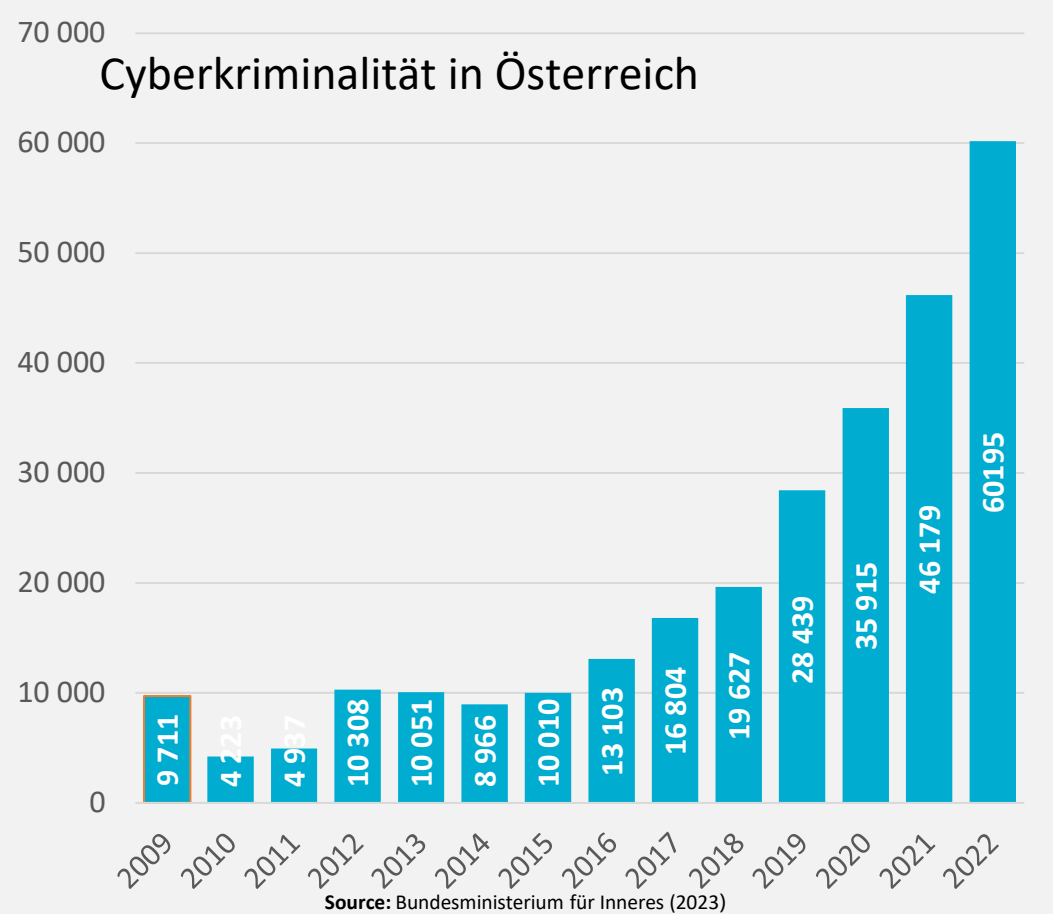
CySeReS KMU

In 5 Schritten zu Supply Chain Cyber Security

Mag. Michael Herburger BA MA PhD

FH OÖ, Logistikum, Universität Passau, Technische Hochschule Deggendorf, THD, universität innsbruck, FH Salzburg, Interreg Bayern-Österreich, Kofinanziert von der Europäischen Union

Der Aufstieg der Cyberkriminalität



Source: Bundesministerium für Inneres (2023)

"57% der KMU würden im Falle eines Sicherheitsvorfalles in Konkurs gehen"
[EU Agency for Cybersecurity (ENISA), 2021]

"90% sehen KMU als das schwächste Glied in der Lieferkette an - 40 % der Befragten wurden durch einen Vorfall im Bereich der Cybersicherheit in der Lieferkette negativ beeinflusst"
[World Economic Forum, 2022]

"Unternehmen benötigen im Durchschnitt 280 Tage, um einen Cyberangriff zu erkennen und darauf zu reagieren"
[World Economic Forum, 2022]

Cyber Risiko – ein Vergleich

Nr 1 der Unternehmensrisiken

Relevanz Supply Chain

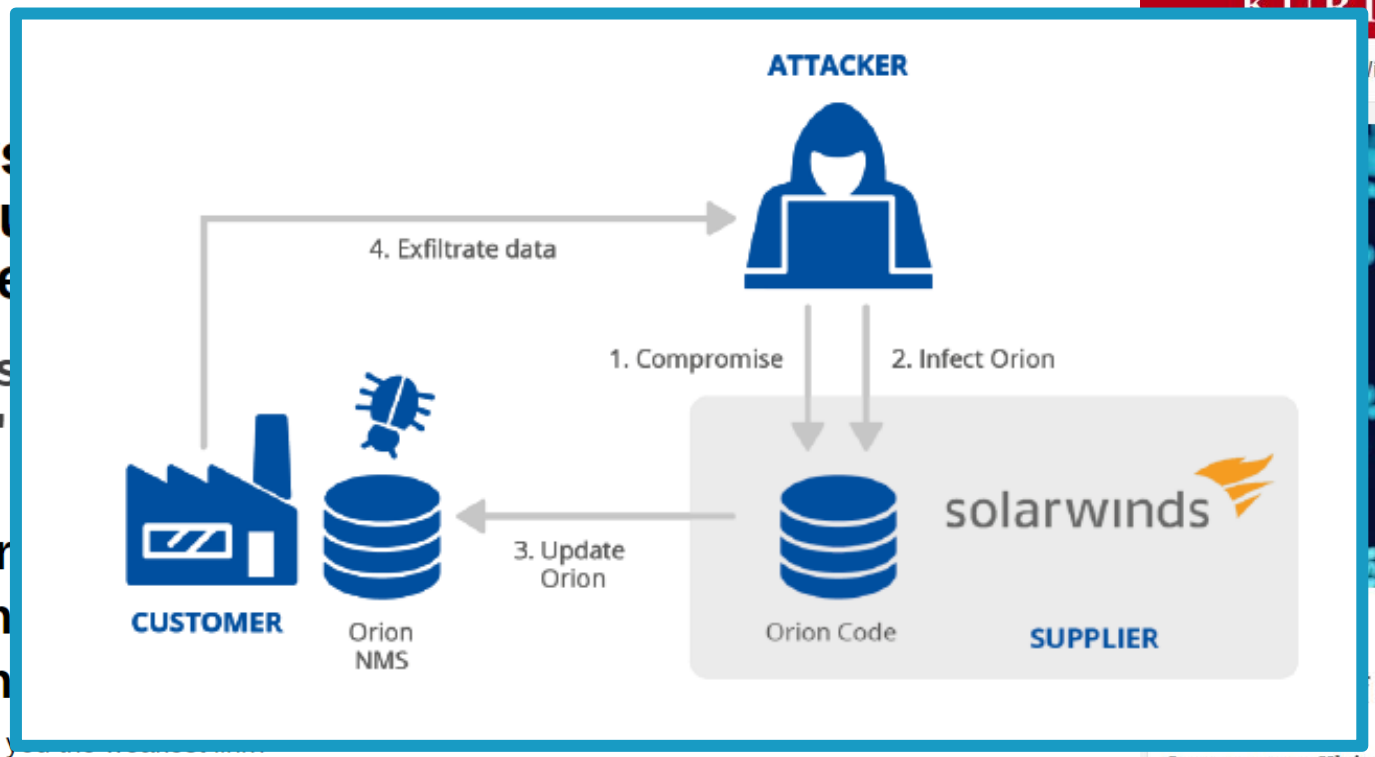
CySeReS KMU
www.cyseres-kmu.eu

Angreifer nutzen Schwachstellen in Lieferketten für deren Angriffe

U.S.

SolarWinds Says Customers, Inclu Government Age

SolarWinds hack was sophisticated attack'



Richard Speed Fri 15 Sep 2023 / 09:45 UTC

KURIER ABO ANMELDEN

Wissen Leben Kultur Stars Meinung MEHR

02.09.2021

auf 34 Firmen in Oberösterreich

Insgesamt 34 Klein- und Mittelbetriebe können nach der Attacke nicht mehr auf ihre Computer-Systeme zugreifen.

Cyber Security Awareness Supply Chain

CySeReS KMU

1. Niedrige Awareness **(Cyber-Angriff auf XYZ)**
   - Keine Erfahrung mit Cyber-Vorfall
   - Awareness aus Medien, etc.

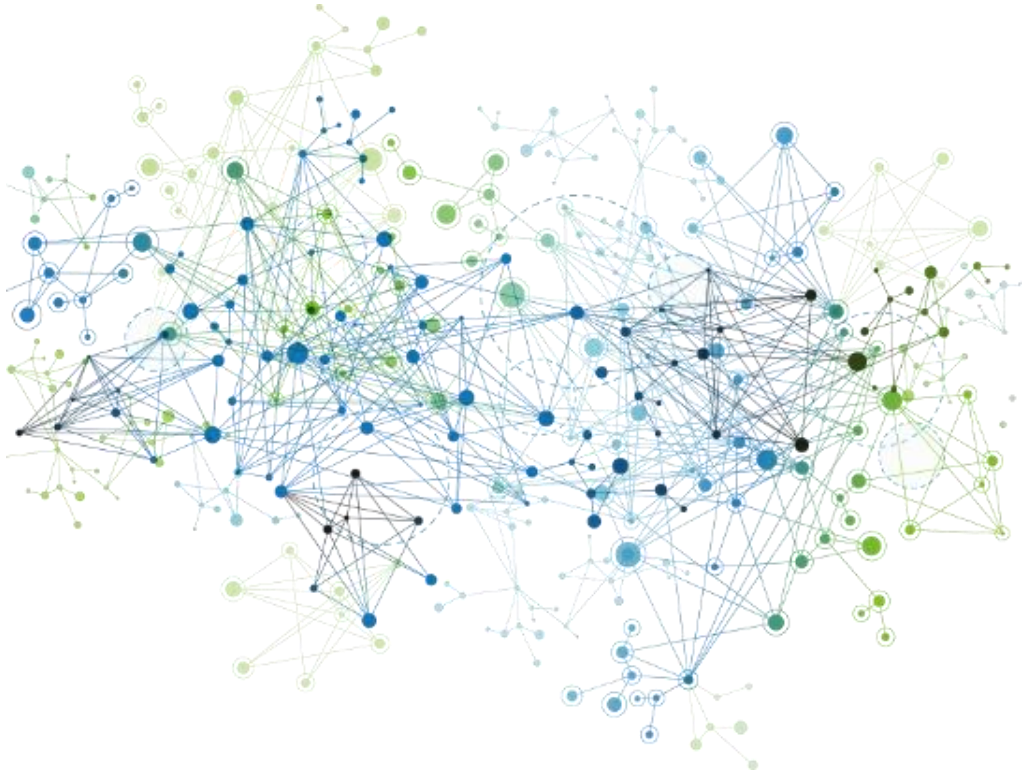
2. Höchste eigene Awareness **(Cyber-Angriff auf das eigene Unternehmen)**
   - Cyber-Vorfall selbst erlitten
   - Impact auf Supply Chain - Verfügbarkeit

3. Höchste Awareness Richtung Supply Chain **(Cyber-Angriff auf das eigene Unternehmen durch eine Schwachstelle beim Supply Chain Partner)**
   - Supply Chain Cyber-Vorfall erlitten
   - Impact auf Supply Chain – Verfügbarkeit, Integrität und Vertraulichkeit

Interreg Bayern-Österreich
Kofinanziert von der Europäischen Union

Analyse Supply Chains

Kunden ⟷ Unternehmen ⟷ Lieferanten



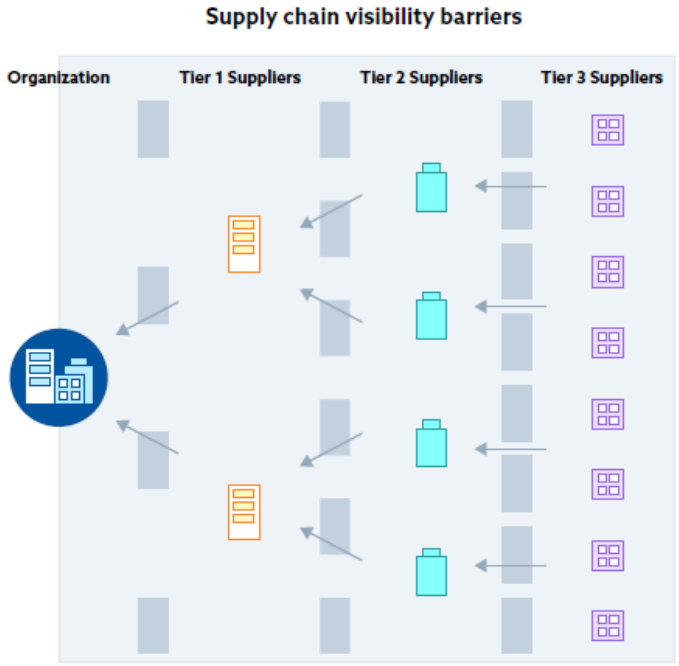


Figure 2: A typical organization's visibility of its suppliers at successive degrees of separation.[11]

11 National cybersecurity Center NZ, 2021. Supply Chain Cyber Security: In Safe Hands, Retrieved from https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

Relevante Supply Chain?

Zur Bestimmung der Kritikalität von Supply Chain Partnern und Komponenten müssen mehrere Kriterien herangezogen werden:

- Ist der Umsatzanteil des SC-Partner signifikant für Ihr Unternehmen?
- Hat der SC-Partner Zugriff auf geistiges Eigentum Ihres Unternehmens?
- Hat der SC-Partner Zugriff auf Daten Ihres Unternehmens?
- Hat der SC-Partner Zugriff auf die System- und Netzwerkinfrastruktur Ihres Unternehmens?
- Hat der SC-Partner Zugriff auf Kundendaten?
- Gibt es eine EDI-Schnittstelle (oder ähnliche) zum SC-Partner?
- Ist der SC-Partner ein Single Source?
- Ist der SC-Partner in den Entwicklungs- und/oder Innovationsprozess Ihres Unternehmens eingebunden?
- Führt ein Ausfall beim SC-Partner zum Produktionsstop bzw. zu einer Produktionseinschränkung?
- Liefert der SC-Partner ein smartes Produkt?
- Liefert der SC-Partner Schnelldreher oder beliefern Sie den SC-Partner mit Schnelldreher?
- Ist der SC-Partner in den Produktionsprozess hoch integriert?
- Ist der SC-Partner und dessen Produkte/Services schnell durch Alternativen ersetzbar?
- Hat der SC-Partner einen Fernwartungszugang zu Ihren Systemen?
- Bezieht Ihr Unternehmen Software as a Service beim SC-Partner?

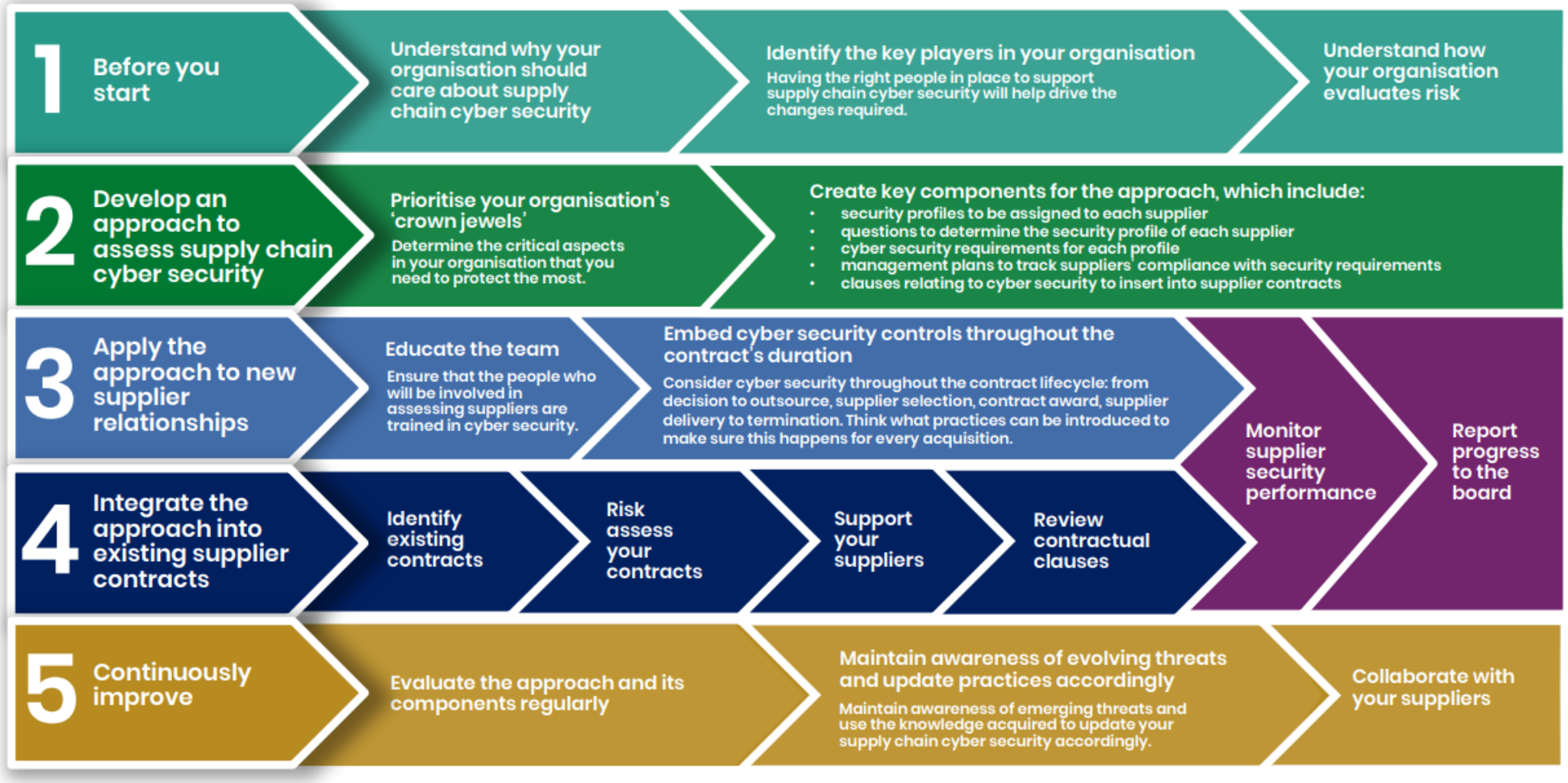
Grundlage für weiteres Risikomanagement in der Lieferkette (zB auf der Grundlage von ISO31000), IT/OT, Hardware, Software, Rohmaterial, End-to-End-SC

Supply Chain Assets

SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Pre-existing Software	e.g. software used by the supplier, web servers, applications, databases, monitoring systems, cloud applications, firmware. It does not include software libraries.
Software Libraries	e.g. third party libraries, software packages installed from third parties such as npm, ruby, etc.
Code	e.g. source code or software produced by the supplier.
Configurations	e.g. passwords, API keys, firewall rules, URLs.
Data	e.g. information about the supplier, values from sensors, certificates, personal data of customers or suppliers themselves, personal data.
Processes	e.g. updates, backups or validation processes, signing certificates processes.
Hardware	e.g. hardware produced by the supplier, chips, valves, USBs.
People	e.g. targeted individuals with access to data, infrastructure, or to other people.

CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK	
Data	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
Personal data	e.g. customer data, employee records, credentials.
Software	e.g. access to the customer product source code, modification of the software of the customer.
Processes	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
Bandwidth	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
Financial	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
People	e.g. individuals targeted due their position or knowledge.

NCSC – Supply Chain Cyber Security



CySeReS KMU

Kenntnisse über den Ansatz Ihrer eigenen Organisation beim Management von Cyberrisiken zu erlangen

Erwartete Ergebnisse aus Phase 1:

- Besseres Verständnis der Bedrohungen für Ihre Supply Chain auf der Grundlage der Art der Beziehungen, die Sie mit Ihren Lieferanten unterhalten (und der Zugänge, die diese zu Ihren Systemen und Dienstleistungen haben).
- Besseres Verständnis der bestehenden Risikobereitschaft und der Prozesse innerhalb Ihrer eigenen Organisation.
- Einbindung der Führungskräfte in die Umsetzung von Änderungen zur Einführung oder Verbesserung der Cybersicherheit in der Lieferkette.
- Einrichtung eines Teams zur Entwicklung eines neuen Ansatzes für die Bewertung der Cybersicherheit in der Lieferkette.

CySeReS KMU

Schritt 1:
Verstehen Sie, warum sich Ihr Unternehmen um die Cybersicherheit der Lieferkette kümmern sollte

Mögliche Fragestellungen:

- Warum könnte jemand an einem Angriff auf Ihre Supply Chain interessiert sein?
- Wer steckt hinter den Angriffen auf Supply Chains, und was sind ihre Beweggründe?

- Welche potenziellen Cyber-Bedrohungen könnten Ihrem Unternehmen Schaden zufügen?
- Welche Schwachstellen könnten innerhalb Ihrer Lieferkette durch einen Cyberangriff ausgenutzt werden?
- Welche Auswirkungen hat es auf Ihr Unternehmen, wenn diese Schwachstellen ausgenutzt werden?
- Welche Arten von Lieferantenbeziehungen gibt es und warum sind ihre Risikoprofile unterschiedlich?

CySeReS KMU

Schritt 2:
Identifizieren Sie die Hauptakteure in Ihrer Organisation

Mögliche Fragestellungen :

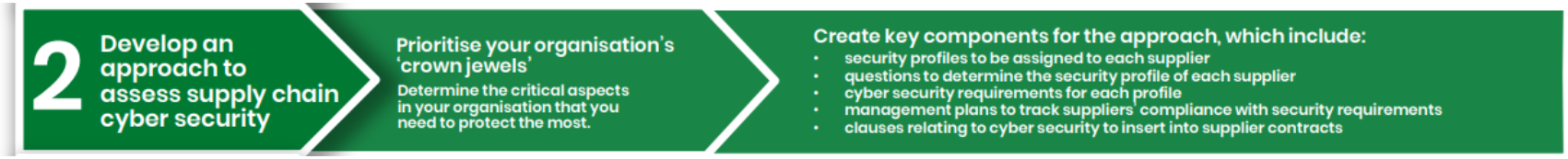
- Wen müssen Sie überzeugen, um die Bewertung der Cybersicherheit in der Lieferkette einzuführen oder zu verbessern?
- Wer ist für die Entwicklung eines neuen Ansatzes zur Bewertung der Cybersicherheit in der Lieferkette verantwortlich?
- Wer sollte bei der Entwicklung dieses neuen Ansatzes konsultiert werden? interdisziplinärer Ansatz

- Wer sollte über die Aktivitäten informiert werden?
- Wer sollte an den Aktivitäten zur Cybersicherheit in der Lieferkette beteiligt sein? Definition eines Prozesses mit klaren Rollen, Verantwortlichkeiten und Kriterien (wahrscheinliche Rollen - IT/Cybersicherheit, Beschaffung, Risikomanagement, Softwareentwicklung, IT-Engineering, Recht, HR, Geschäfts-/Prozesseigentümer, Top-Management)

CySeReS KMU

Schritt 3:
Verstehen, wie Ihre Organisation Risiken bewertet

- Verstehen des organisatorischen Risikomanagement-ansatzes einschließlich der Risikobereitschaft.
- Aufbau auf bestehenden Ansätzen.



Schritt 1:
Setzen Sie Prioritäten bei den "Kronjuwelen" Ihrer Organisation

- Bestimmen Sie die kritischen Aspekte in Ihrem Unternehmen, die Sie am meisten schützen müssen (Ihre "Kronjuwelen"), und berücksichtigen Sie dabei potenzielle Bedrohungen, Schwachstellen, Auswirkungen und die Risikobereitschaft Ihres Unternehmens.
- Ein klares Verständnis der kritischsten Aspekte Ihres Unternehmens mit Kriterien für die Bestimmung der Zusicherungen, die Sie von Ihren Lieferanten benötigen, um diese zu schützen.

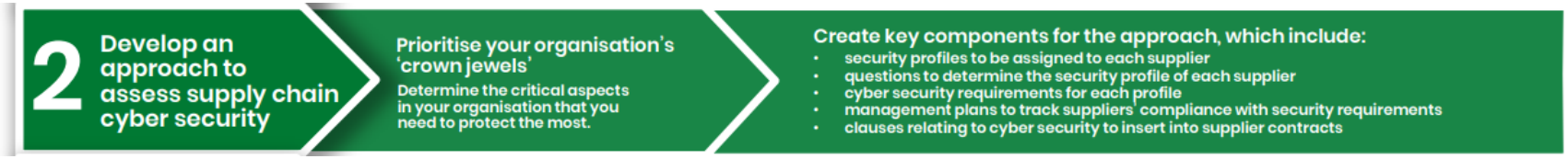
Dazu ist es sinnvoll, die Ressourcen zu berücksichtigen, zu denen jeder Anbieter Zugang hat. Zum Beispiel:

- Hat der Lieferant Zugang zu persönlich identifizierbaren/kommerziell sensiblen Daten?
- Wo wird der Lieferant die Daten und Informationen der Organisation verarbeiten und speichern?
- Hat der Auftragnehmer Zugang zu wichtigen oder geschäftskritischen Anlagen?
- Hat der Lieferant Zugang zu und/oder Verbindung zum Netzwerk der Organisation mit zusätzlichen Privilegien?
- Hat der Lieferant Verbindungen zu Regierungen oder Organisationen, die Ihrem Sektor feindlich gegenüberstehen könnten?

Sie können auch die Auswirkungen eines möglichen Verstoßes berücksichtigen:

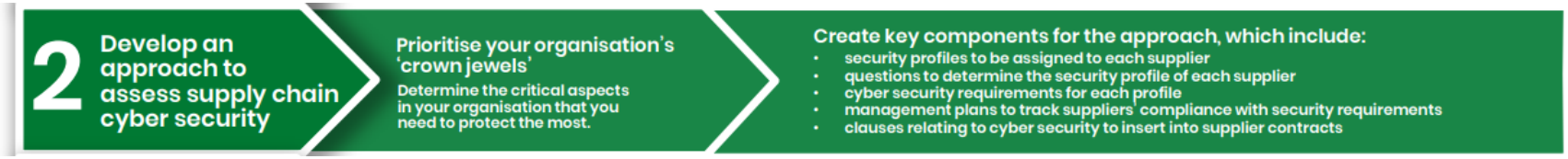
- Ist der Lieferant eine einzige Anlaufstelle für Störungen? Was tut der Anbieter für Sie?
- Würde sich eine Sicherheitsverletzung durch den Lieferanten nachteilig auf den Geschäftsbetrieb und/oder die Prozesse der Organisation auswirken?
- Würde ein Verstoß durch den Lieferanten den Ruf des Unternehmens beeinträchtigen?
- Würde ein Verstoß durch den Lieferanten erhebliche finanzielle und/oder rechtliche, regulatorische oder vertragliche Konsequenzen nach sich ziehen?
- Würde ein Verstoß die Sicherheit Ihrer Mitarbeiter oder Kunden beeinträchtigen?

Relevante Supply Chain und Supply Chain Assets



Schritt 2:
Erstellen Sie Schlüsselkomponenten für Ihren Ansatz

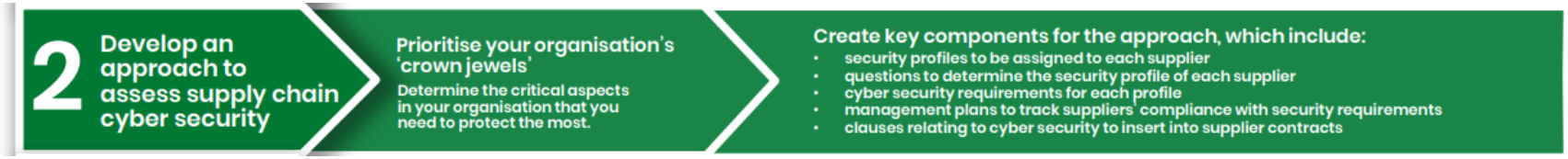
- Aktion 1: Erstellung einer Reihe von Sicherheitsprofilen (einschließlich Beschreibung)
  Geringe Auswirkungen - Mäßige Auswirkungen - Hohe Auswirkungen
- Aktion 2: Bestimmung des Sicherheitsprofils für jeden Lieferanten
- Aktion 3: Definition der Mindestanforderungen an die Cybersicherheit für jedes Sicherheitsprofil
  - Welche Verhaltensweisen und Praktiken im Bereich der Cybersicherheit sollte ich von meinen Lieferanten erwarten?
  - Welche Industriestandards für die Sicherheit der Lieferkette sollte ich von meinen Lieferanten einfordern?
- Aktion 4: Entscheiden Sie, wie Sie Ihre Lieferanten bewerten wollen
  Fragebogengestützte Erhebung, Interviews, Besuch vor Ort, unabhängige Bewertung/Zertifizierung, automatische Bewertungen (Häufigkeit)
  - Wie häufig sollte ich die Sicherheit meiner Lieferanten bewerten?
  - Wie kann ich sicherstellen, dass meine Lieferanten die geforderten Cybersicherheitsanforderungen einhalten?
    - Kommunizieren Sie die Anforderungen so früh wie möglich.
    - Verpflichten Sie Ihre Lieferanten in ihren Verträgen zur Einhaltung von Mindestanforderungen an die Cybersicherheit.
    - Verlangen Sie Nachweise von Ihren Lieferanten.



Schritt 2:
Erstellen Sie Schlüsselkomponenten für Ihren Ansatz

- Aktion 5: Plan für den Fall der Nichteinhaltung

  Erstellen Sie einen Plan für das Sicherheitsmanagement, in dem die Kontrollen festgelegt sind, die der Lieferant innerhalb eines bestimmten Zeitplans einrichten muss. Er kann Folgendes umfassen:
  - erfüllte und nicht erfüllte Anforderungen
  - erforderliche Maßnahmen zur Behebung
  - Zeitrahmen
  - Datum der letzten Bewertung
  - Datum der nächsten Bewertung
  - Art der Beurteilung (zB Besuch vor Ort, Fragebogen, Pen-Test)
  - Ergebnis der Bewertung

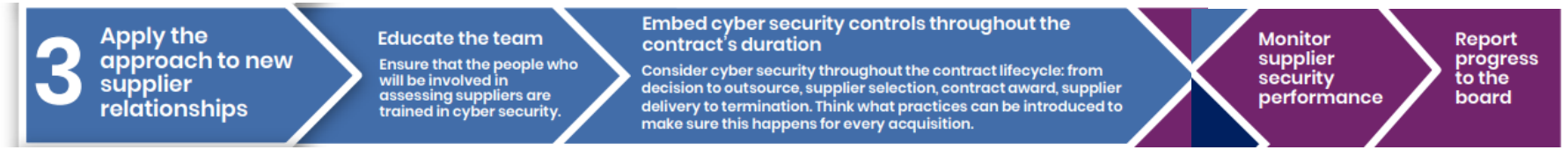


Schritt 2:

Erstellen Sie Schlüsselkomponenten für Ihren Ansatz

- Aktion 6: Vertragsklauseln erstellen
  - Sicherstellung, dass alle vom Anbieter beauftragten Unterauftragnehmer das gleiche Maß an Cybersicherheitsmaßnahmen durchführen wie der Anbieter selbst. Dies kann Beschränkungen in Bezug auf Organisationen oder Regionen beinhalten, an die Unteraufträge vergeben werden können, oder wo Daten gespeichert werden, sowie die Benachrichtigung im Falle eines Wechsels des Unterauftragnehmers.
  - Reaktions- und Benachrichtigungsfristen für die Reaktion auf eine Sicherheitsverletzung sowie Unterstützung der Organisation bei der Suche nach der Ursache.
  - Erwartete Personalfreigaben und durchzuführende Due-Diligence-Prüfungen, möglicherweise organisatorische Genehmigung, welche Mitarbeiter des Lieferanten Zugang zu den Systemen haben.
  - Fähigkeit, den Lieferanten zu überprüfen und erwartete Häufigkeit der Prüfungen.

    - Ob eine Versicherung für Cybersicherheitsvorfälle erforderlich ist.
    - Offenlegung früherer Schwachstellen von Komponenten, Cyber-Vorfälle oder Datenschutzverletzungen.
    - Allgemeine Cybersicherheitskontrollen, die eingehalten werden müssen (erforderliche Verschlüsselungsstufen, zulässige Endnutzergeräte, Datenvernichtung, Identitäts- und Auditkontrollen).
    - Vereinbarung darüber, wie lange die Geräte unterstützt und gewartet werden, um zu vermeiden, dass die Geräte nicht mehr unterstützt werden.
    - Datenmanagement, einschließlich der Frage, welche Informationen an einen Drittanbieter weitergegeben werden dürfen. Nur notwendige Daten dürfen aus dem Organisationsnetz heraus übertragen werden und müssen durch Authentifizierung und Verschlüsselung geschützt werden. Werden die Daten getrennt, wenn sie auf einer Lieferantenplattform gespeichert sind?
    - Möglichkeit, im Vertrag eine Ausstiegsklausel geltend zu machen, wenn die Sicherheit des Lieferanten nicht den erwarteten Standards entspricht.
    - Alle anderen Bestimmungen, die die Verantwortlichkeiten der Organisation und des Lieferanten bei Cyber-Assurance-Aktivitäten klar definieren.

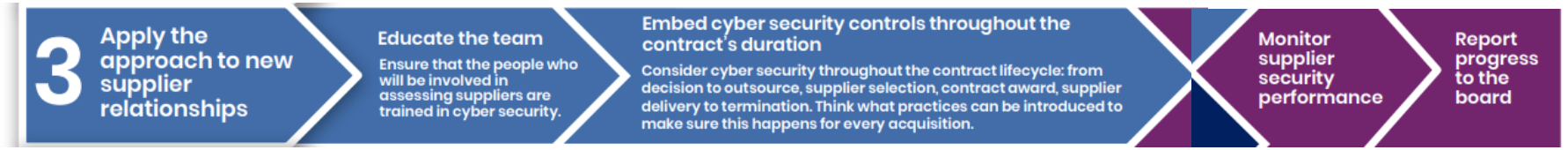


CySeReS KMU

Schritt 1:
Das Team schulen

Sicherstellen, dass die Personen, die an der Bewertung von Lieferanten beteiligt sind:

- sich der Bedrohungen bewusst sind, die von der Cybersicherheit der Lieferanten ausgehen
- ihre Rolle bei der Verringerung des Risikos verstehen
- den Prozess verstehen, den Sie für Ihr Unternehmen festgelegt haben



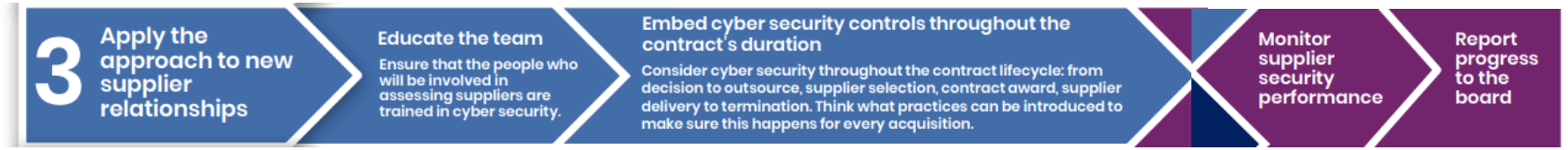
CySeReS KMU

Schritt 2:
Verankerung von Kontrollen der Cybersicherheit während der gesamten Vertragslaufzeit

Berücksichtigen Sie die Cybersicherheit in jedem Schritt des Vertragslebenszyklus:

- Outsourcing-Entscheidungen
- Bei der Auswahl von Lieferanten
- Bei der Auftragsvergabe
- Während der Vertragslaufzeit
- Bei der Beendigung eines Vertrags

Kofinanziert von der Europäischen Union



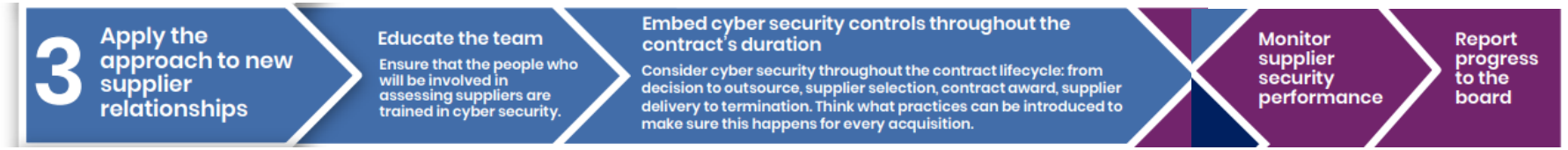
CySeReS KMU

Schritt 3:
Lieferantenmonitoring

Wie kann ich die Sicherheit meiner Lieferanten laufend gewährleisten?

- Regelmäßiger Dialog mit Ihren Lieferanten
- Regelmäßige Überprüfung der Cybersicherheit einschließlich
  - Liste der von Ihrer Organisation genutzten Vermögenswerte der Anbieter.
  - Angriffe oder Sicherheitsverletzungen, die sie erlitten haben.
  - Bestätigung, dass sie alle System- oder Dienstkonten, die sie für den Zugang zu Ihren Systemen, Diensten und Informationen nutzen, aktiv verwalten, überwachen und regelmäßig überprüfen.
  - KPIs mit Metriken zur Sicherheitsleistung, einschließlich Software, die gepatcht wird, Sicherheitsverletzungen, Intrusion Detection Systems Output, Firewall Output.
  - Ergebnisse der jüngsten Überprüfungsaktivitäten der eigenen Lieferanten.
  - Wie oft wird der Reaktionsplan des Lieferanten auf Zwischenfälle überprüft?
  - Wann wurde der Zulieferer zuletzt besucht?

Kofinanziert von der Europäischen Union

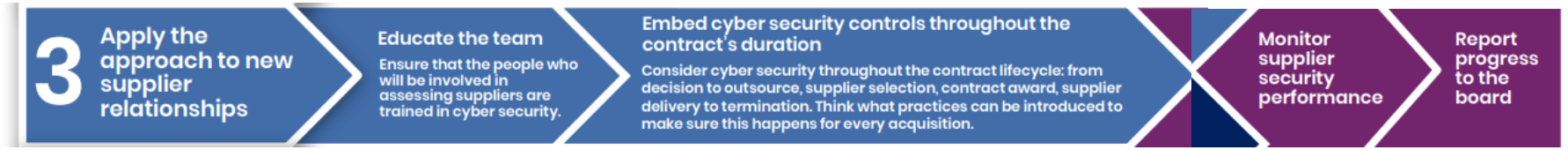


CySeReS KMU

Schritt 3:
Lieferantenmonitoring

Wie kann ich die Sicherheit meiner Lieferanten laufend gewährleisten?

- Regelmäßiger Dialog mit Ihren Lieferanten
- Regelmäßige Überprüfung der Cybersicherheit
- Prüfung des Vermögens Ihrer eigenen Organisation, einschließlich
  - Überprüfung, ob die privilegierten Zugänge der Lieferanten wie erwartet genutzt werden.
  - Überwachung von Systemen und Diensten, um unbefugte Zugriffe, externe Verbindungen, Fernzugriff und Datenexfiltration zu erkennen.
  - Führen einer Liste genehmigter Netzwerkverbindungen (z. B. Site-to-Site-VPNs) zwischen Ihrem Unternehmensnetzwerk und Dritten und Überwachung der Netzwerkverbindungen, um sicherzustellen, dass nur genehmigte Verbindungen bestehen.
  - Durchführung von Penetrationstests der gemeinsam genutzten Infrastruktur des Unternehmens/Lieferanten.

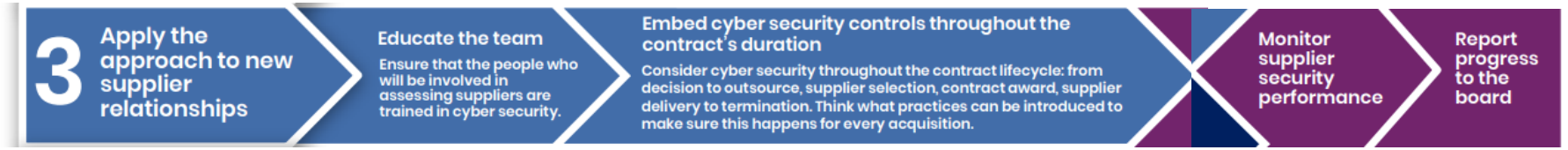


CySeReS KMU

Schritt 3:
Lieferantenmonitoring

Wie kann ich die Sicherheit meiner Lieferanten laufend gewährleisten?

- Regelmäßiger Dialog mit Ihren Lieferanten
- Regelmäßige Überprüfung der Cybersicherheit
- Prüfung des Vermögens Ihrer eigenen Organisation
- Erwägen Sie den Einsatz von Drittanbieter-Tools zur kontinuierlichen Überwachung Ihrer Lieferanten.
  - Überwachung von außen
  - Service Level Agreement einschließlich
    - den Umfang der Überwachung, die durchgeführt werden soll
    - erwartete(r) zu erfassende(r) Datensatz(e)
    - Mechanismen für die Weitergabe oder den Versand von Protokollen/Daten
    - Garantien für die Integrität und Sicherheit der erfassten Daten
    - wie die Informationen verwendet werden sollen
    - Reaktionen auf Feststellungen außerhalb der festgelegten Schwellenwerte
    - Einzelheiten zum Management von Vorfällen und zur Berichterstattung



CySeReS KMU

Schritt 4:
Berichterstattung über die Fortschritte an den Vorstand

Das Top-Management ist für den Erfolg entscheidend.

Bereitstellung regelmäßiger Berichte einschließlich

- Wie viel Prozent der Lieferanten / Unterauftragnehmer wurden bewertet?
- Wie viel Prozent davon erfüllen die Anforderungen?
- Wann wurden die Zulieferer zuletzt bewertet?
- Gibt es bei einigen Zulieferern erhebliche Probleme, die gelöst werden müssen?
- Haben wir einen Überblick über die kritischen Lieferanten innerhalb der Lieferkette?
- Welche schwerwiegenden Probleme sind seit der letzten Aktualisierung aufgetreten?

CySeReS KMU

Nach der Einführung eines neuen Konzepts sollten Sie Ihre bestehenden Verträge entweder bei der Erneuerung oder, wenn es sich um kritische Lieferanten handelt, früher überprüfen.

Erwartete Ergebnisse von Phase 4:

- Ein Register, in dem alle Ihre Lieferanten verzeichnet sind.
- Lieferanten mit "hoher Priorität" werden anhand definierter Sicherheitskontrollen einer Risikobewertung unterzogen.
- Lieferanten mit Sicherheitsmängeln werden identifiziert, und es wird ein Plan zur Verbesserung ihrer Sicherheit vereinbart.
- Verbesserter Ansatz auf der Grundlage der aus den Aktivitäten gezogenen Lehren.
- Die Leistung wird regelmäßig anhand festgelegter Kennzahlen gemessen, die für die Vorstandsmitglieder sichtbar sind.

CySeReS KMU

Schritt 1:
Identifizierung bestehender Verträge

- Erstellen Sie ein Verzeichnis aller Lieferanten, mit denen Ihre Organisation zusammenarbeitet.
- Zumindest sollten Ihre wichtigsten Lieferanten identifiziert werden.

Schritt 2:
Risikobewertung und Prioritätensetzung für Ihre Verträge

- Risikobewertung und Priorisierung bestehender Verträge, mit Schwerpunkt auf kritischen Geschäftsfunktionen und Bereichen mit hohem Cyber-Risiko
- Identifizieren Sie Ihre unmittelbaren Lieferanten und was sie für Sie tun
- Arbeiten Sie mit Ihren Lieferanten zusammen, um ein Gesamtbild zu erstellen
- Führen Sie eine Risikoanalyse für die identifizierten Lieferanten durch.
- Festlegung von Aktivitäten zur Abbildung der Lieferkette in Lieferantenverträgen

Kofinanziert von der Europäischen Union

CySeReS KMU

Schritt 3:
Unterstützen Sie Ihre Lieferanten (und Kunden - Wettbewerbsvorteil)

Schritt 4:
Überprüfung der Vertragsklauseln

- Die meisten Verträge enthalten die in Schritt 2 genannten Klauseln nicht.

Schritte 5 and 6 (Monitoring und Vorstandsberichte)

CySeReS KMU

Schritt 1:
Regelmäßige Evaluierung des Konzepts und seiner Komponenten

Schritt 2:
Aufrechterhaltung des Bewusstseins für sich entwickelnde Bedrohungen und entsprechende Aktualisierung der Praktiken

Wege, um mit der sich schnell entwickelnden Bedrohungslandschaft Schritt zu halten:

- Abonnieren Sie Dienste, die Sie über Schwachstellen in den von Ihnen genutzten Geräten und Diensten informieren, und vergewissern Sie sich, dass Ihre Zulieferer ähnlich vorgehen und regelmäßige Tests nachweisen.
- Informieren Sie sich über alle lieferkettenspezifischen Vorfälle und untersuchen Sie die Ursache, um sicherzustellen, dass Ihre Lieferanten nicht für dieselbe Art von Schwachstelle anfällig sind.
- Sammeln von Geschäftsinformationen über die Aktivitäten in der Lieferkette, um zu verstehen, was gut läuft und wo möglicherweise Lücken bestehen.
- Gespräche mit wichtigen Mitarbeitern, die an der Sicherung der Lieferkette beteiligt sind. Ist der Schwerpunkt der Aktivitäten auf die beste Wirkung ausgerichtet? Was kann optimiert und verändert werden, um bessere Ergebnisse zu erzielen?

CySeReS KMU

Schritt 3:
Arbeiten Sie mit Ihren Lieferanten zusammen

Möglichkeiten zur Sensibilisierung und Aufklärung der eigenen Mitarbeiter und Lieferanten über die Bedeutung der Cybersicherheit in der Lieferkette:

- Verpflichtende Cybersicherheitsschulungen bei der Einstellung von Mitarbeitern, einschließlich der Mitarbeiter von Zulieferern. Stellen Sie sicher, dass diejenigen, die an der Bewertung der Cybersicherheit in der Lieferkette beteiligt sind, eine spezielle Schulung erhalten, die sie in die Lage versetzt, ihrer Verantwortung gerecht zu werden.
- Stellen Sie sicher, dass die Cybersicherheitsschulung aktualisiert und regelmäßig wiederholt wird.
- Fördern Sie eine positive Sicherheitskultur, indem Sie Diskussionen anregen, Umfragen durchführen, Sicherheitsvorfälle und Berichte über Beinaheunfälle überprüfen.
- Schaffen Sie ein Gefühl der gemeinsamen Verantwortung, denn sowohl das Unternehmen als auch der Lieferant sollten ihren Teil dazu beitragen, dass die Cyberrisiken in der Lieferkette minimiert werden.
- Teilen Sie Ihr Wissen über potenzielle Bedrohungen mit Ihren Lieferanten, z. B. wenn Ihr Unternehmen in Informationen eingeweiht ist, die für sie von Interesse sein könnten, oder umgekehrt.
- Austausch von Wissen und Erfahrungen mit einer Gruppe von Unternehmen, die ähnlichen Bedrohungen ausgesetzt sind. Dies kann über etablierte Plattformen geschehen.

CySeReS KMU

Schritt 3:
Arbeiten Sie mit Ihren Lieferanten zusammen

Wege, um Vertrauen zu den Lieferanten aufzubauen und sie zu kontinuierlichen Verbesserungen zu ermutigen:

- Transparent sein
- Unterstützen Sie Ihre Lieferanten bei der Verbesserung ihrer Cybersicherheitsstandards
- Lernen Sie Ihre Lieferanten kennen

Trust but verify – Vertraue, aber überprüfe

Fazit

- Komplexe, interdisziplinäre und langfristige Aufgaben
- Nutzung bestehender Standards und Richtlinien
- Reifegrad und Bewusstsein entlang der SC völlig unterschiedlich
- Mangelnde SC Sichtbarkeit
- Sie brauchen die Unterstützung des Top-Managements
- Sie brauchen die jeweiligen Prozessverantwortlichen

Resilienz Ihrer SC Prozesse, nicht der IT/OT, von der sie abhängen.

Weiterführende Referenzen

- NCSC - How to assess and gain confidence in your supply chain cyber security. https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
- NCSC - Mapping your supply chain Mapping your supply chain - NCSC.GOV.UK
- NIST - Cybersecurity Supply Chain Risk Management https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications
- NIST - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
- Supply Chain Cyber Resilience (Michael Herburger) https://research.cbs.dk/en/publications/supply-chain-resilience-a-concept-for-coping-with-cyber-risks

Webinarreihe - Zusammenarbeit

Unter diesem Link können Sie sich für alle zukünftigen Webinare im Projekt CySeReS-KMU anmelden:
https://www.eventbrite.com/cc/webinarreihe-cyber-security-fur-kmus-in-sc-2470389

Interesse an einer Zusammenarbeit im Projekt?

Gerne melden unter: office@cyseres-kmu.eu

Vielen Dank für Ihr Interesse!

CySeReS KMU

Folgen Sie uns schon auf LinkedIn?

Nein? Na dann gleich mal reinschauen!

Oder unter: https://www.linkedin.com/company/cyseres-kmu-cyber-security-und-resilienz-in-supply-chains-mit-fokus-auf-kmus/

Weitere Infos finden Sie auch auf unserer Projektwebsite:

Oder unter: https://cyseres-kmu.eu/