www.nviso.eu

Cyberangriffe auf Ihre Lieferanten und Dienstleister sind auch Ihr Risiko

11.03.2025

Julian Obenland-Recker Geschäftsführer NVISO GmbH

In Zusammenarbeit mit

COMMERZBANK

Über NVISO

Unsere Firma

NVISO ist ein **Cyber Security** Beratungsunternehmen mit **über** 300 spezialisierten Sicherheitsexperten und wurde 2013 gegründet.

Ursprünglich in Belgien gegründet, sind wir seit 2019 auch in Deutschland und seit 2022 in Griechenland und Österreich vertreten.

Unsere Mission ist es, die **Grundwerte** der **europäischen Gesellschaft** vor Cyber-Angriffen zu **schützen**.

Unsere DNA

We are proud: wir sind stolz darauf, wer wir sind und was wir tun.

We care: wir kümmern uns um unsere Kunden und Menschen.

We break barriers: Wir fordern den Status quo durch kontinuierliche Innovation heraus..

No BS: Wir halten unsere Versprechen und erledigen unsere Aufgaben gewissenhaft.

Unsere Research

Wir investieren **10 %** unseres **Jahresumsatzes in** die **Erforschung** neuer **Sicherheitstechniken** und die **Entwicklung neuer Lösungen**.

Follow us on:

@NVISO_security and @NVISO_Labs

blog.nviso.eu/

Unsere Expertise

Wir übernehmen eine Vorreiterrolle und geben unser Wissen aktiv weiter. Ein Beweis dafür sind die SANS-Kurse, die wir (mit-)verfassen und unterrichten.

nviso.eu

SEC575

Mobile Pen. Testing

Seit 2019 sind NVISO-Experten die Hauptautoren des SANS SEC575 Kurses „Mobile Penetration Testing & Ethical Hacking“.

NVISO-Experten pflegen 6 Tage Kursmaterial für diesen 6-tägigen Kurs.

SEC598

Security Automation

Im Laufe der Jahre 2021 und 2022 hat NVISO einen neuen SANS-Kurs entwickelt, der sich auf Security Automation konzentriert. Veröffentlicht im Jahr 2023.

NVISO-Experten pflegen und entwickeln 6 Tage Kursmaterial für diesen Kurs.

SEC599

Purple Team Tactics

Im Jahr 2018 waren NVISO-Experten die Hauptautoren eines der ersten Purple Teaming Kurse, „SEC599 – Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses“.

NVISO-Experten pflegen 5 Tage Kursmaterial für diesen Kurs. Wir unterrichten ihn auch aktiv weltweit.

SEC699

Advanced Purple Team

Im Jahr 2020 entwickelten NVISO-Experten einen Folgekurs zu SEC599, genannt SEC699, der sich mehr auf die automatisierte Nachahmung von Bedrohungen mit CALDERA konzentriert.

NVISO-Experten pflegen 5 Tage Kursmaterial für diesen 6-tägigen Kurs. Wir unterrichten ihn auch aktiv weltweit.

Wir teilen unser Know-How mit der Community

Talks & Konferenzen

Wir präsentieren unsrer Forschungs-ergebnisse auf renommierten Sicherheitsveranstaltungen und Konferenzen präsentiert, darunter die RSA Conference, Black Hat, BruCON, OWASP, FIRST und viele weitere.

Frau Plattner als Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik eröffnet unsere Deutschen Hacking Meisterschaft.

Print media Handelsblatt – NVISO zeigt Expertise

Handelsblatt

KÜNSTLICHE INTELLIGENZ

Wie neuartige Cyberattacken mit KI die Banken bedrohen

von: Andreas Kröner • Elisabeth Atzler
Datum: 28.06.2023 04:00 Uhr

Geldhäuser geraten besonders häufig ins Visier von Hackern. Mit KI werden die Angriffe zunehmen und ausgefeilter werden. Aufsichtsbehörden sind alarmiert.

Frankfurte
Behörden
(Foto: dpa)

Frankfurt. Nico Leidecker greift Banken an – und der Einsatz von Künstlicher Intelligenz (KI) macht sein Leben leichter. Mit ChatGPT und ähnlichen Programmen kann er Schwachstellen bei Geldhäusern besser ausspähen und Bankmitarbeitern maßgeschneiderte Phishing-E-Mails schicken. Klickt nur ein Beschäftigter auf einen Link oder einen Anhang in einer solchen E-Mail, kann der Hacker in die Systeme der Institute eindringen.

„Für Banken und deren Kunden wird es deutlich schwieriger, solche Phishing-Mails zu erkennen", sagt Leidecker. „Gleichzeitig wird es für Angreifer auf der ganzen Welt einfacher, deutsche Banken zu attackieren." Dank ChatCPT müssen Cyberkriminelle schließlich keine Muttersprachler mehr sein, um fehlerfreie E-Mails zu schreiben.

Leidecker arbeitet für die IT-Sicherheitsfirma Nviso in Frankfurt. Finanzfirmen, Industriekonzerne und auch staatliche Stellen können sich von ihm attackieren lassen, um Schwachstellen in der eigenen Organisation zu erkennen und zu beheben.

Source:
https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/kuenstliche-intelligenz-wie-neuartige-cyberattacken-mit-ki-die-banken-bedrohen/29091744.html

BUNDESBANK-PROJEKT „TIBER"

„Wir greifen auf drei Wegen an": So lassen sich deutsche Banken fast immer hacken

Die Zahl von Cyberangriffen ist deutlich gestiegen. Um besser gerüstet zu sein, lassen sich Finanzkonzerne zu Testzwecken attackieren. Ein Angreifer erklärt, wie er dabei vorgeht.

19.10.2021 - 13:22 Uhr

Internetkriminalität

Die Zahl der Cyberattacken hat sich in der letzten Dekade
zählt dabei zu den am meisten attackierten Branchen.
(Foto: dpa)

Frankfurt. Pierre-Alain Mouy sitzt mit zwei Hacker-Kollegen im Besprechungsraum des Vorstands eines Versicherungskonzerns. Mit ihren Rechnern sind sie gerade ins Netzwerk des Unternehmens eingedrungen, als plötzlich die Tür aufgeht und ein Geschäftsführer vor ihnen steht. „Wer seid ihr denn?", fragt er die Eindringlinge. „Kommt ihr von SAP?" Als Mouy das bejaht, ist der Manager zufrieden. Er wünscht den Hackern noch viel Erfolg – und verschwindet wieder.

Mouy ist Geschäftsführer der IT-Sicherheitsfirma Nviso in Frankfurt. Finanzfirmen, Industriekonzerne und auch staatliche Stellen können sich von ihm attackieren lassen, um Schwachstellen in der eigenen Organisation zu erkennen und zu beheben.

Source:
https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/bundesbank-projekt-tiber-wir-greifen-auf-drei-wegen-an-so-lassen-sich-deutsche-banken-fast-immer-hacken/27686376.html

Tagesschau – NVISO Experten informieren

tagesschau

Sendung verpasst?

Startseite ▸ Wirtschaft ▸ Finanzen ▸ "Virtueller Bankraub": Finanzaufsicht warnt vor Cyberangriffen

Cyberangriffe auf IT-Dienstleister

Finanzaufsicht warnt vor "virtuellem Bankraub"

Manchmal 100 Aufgaben ausgelagert

Allein bei der ING waren nach Angaben der Bank Zehntausende Kunden betroffen. Deren persönliche Daten seien im Darknet veröffentlicht worden, deren Vorname, Nachname und Kontonummer, heißt es in einer Stellungnahme: "Die betroffenen Kunden wurden umgehend informiert und über vorsorglich getroffene Sicherheitsmaßnahmen aufgeklärt." Die Bank will den Vorfall nun gründlich aufarbeiten und steht weiter in engem Kontakt mit dem IT-Dienstleister.

Hintergrund war eine Sicherheitslücke bei dem Softwareprogramm MOVEit. Laut BaFin waren davon weltweit Tausende Unternehmen betroffen, darunter zahlreiche deutsche Finanzinstitute und Versicherer. Deshalb will die Finanzaufsicht künftig noch genauer überprüfen, mit welchen Prozessen Dienstleister beauftragt werden. Im Schnitt werden laut BaFin pro Unternehmen zehn Aufgaben ausgelagert, bei manchen Unternehmen seien es allerdings auch über hundert.

Es gibt auch private Unternehmen, die die Banken in deren eigenem Auftrag angreifen, um Schwachstellen aufzudecken, etwa die Frankfurter Firma Nviso. Auch da könnten Kooperationspartner eine Rolle spielen, sagt Abteilungsleiter Nico Leidecker: "Wenn ich weiß, dass für diese Bank ein Dienstleister tätig ist, könnte ich mich als dieser ausgeben und Emails an einen Mitarbeiter der Bank schicken." Damit könne man ihn womöglich dazu bekommen, einen Anhang zu öffnen, eine Datei mit einer Schadsoftware herunterzuladen und auszuführen.

Leidecker zufolge ist das eine Möglichkeit, wie Kriminelle Zugriff zu einem Bankennetzwerk bekommen und langfristig zu den Kontobewegungen. Die könnten sie manipulieren, Geld von einem Konto zum anderen überweisen. Am Ende könnten sie es an einem Geldautomaten abheben - so ließen sich die Spuren der Verbrecher verwischen. Die kämen häufig aus dem Ausland, meint der IT-Sicherheitsexperte: "Aber dank Künstlicher Intelligenz können sie trotzdem Emails in fehlerfreiem Deutsch verfassen."

Source:
https://www.tagesschau.de/wirtschaft/finanzen/bafin-cyberangriffe-warnung-100.html

Körber AG

nVISO.eu

Customer Success Story

Read the story

KÖRBER

Our time-to-response and mean time-to-response have dropped enormously thanks to Microsoft Sentinel. This makes our IT infrastructure and us as a company much more resistant to cyberattacks.

Andreas Gaetje, Chief Information Security Officer, Körber

Source: https://www.microsoft.com/en/customers/story/20130-korber-microsoft-sentinel

100%

More **Detection**

50%

Fewer **Incidents**

240%

Increase in

Security Coverage

Unsere Kunden

Warum gerade Lieferanten und Dienstleister?

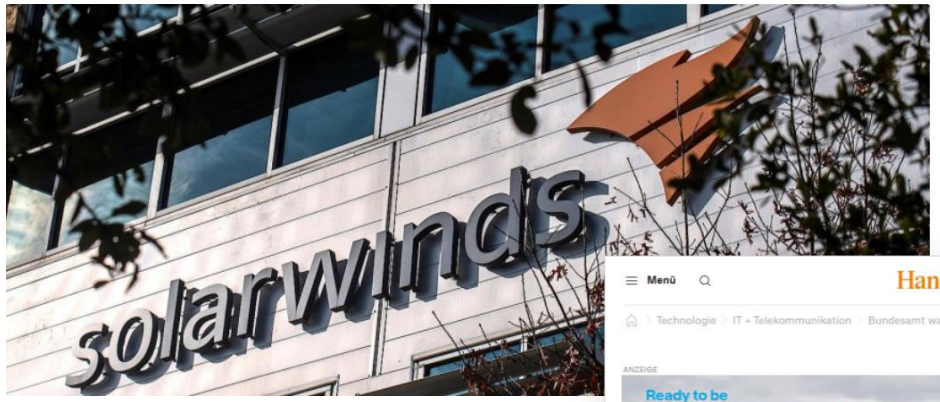
Warum gerade Lieferanten und Dienstleister?

Wir haben hohe Abhängigkeiten mit unseren Lieferanten & Dienstleister

SOLARWINDS-HACK

Massiver Cyberangriff gefährdet deutsche Behörden

VON BASTIAN BENRATH - AKTUALISIERT AM 07.01.2021 - 16:46



Kaseya VSA: Wie die Lieferketten-Angriffe abliefen und was sie für uns bedeuten

Auch wer nicht davon betroffen ist, sollte sich klarmachen, was da gerade geschieht. Denn Angriffe wie der aktuelle REvil-Coup werden die IT-Welt verändern.

Handelsblatt

Menü Anmelden Abo

Technologie > IT + Telekommunikation > Bundesamt warnt vor großer Bedrohung durch Software-Sicherheitslücke

Java-Bibliothek Log4j

Warnstufe Rot: Sicherheitslücke gefährdet die IT zahlreicher Unternehmen

TLP:CLEAR

Bundesamt für Sicherheit in der Informationstechnik

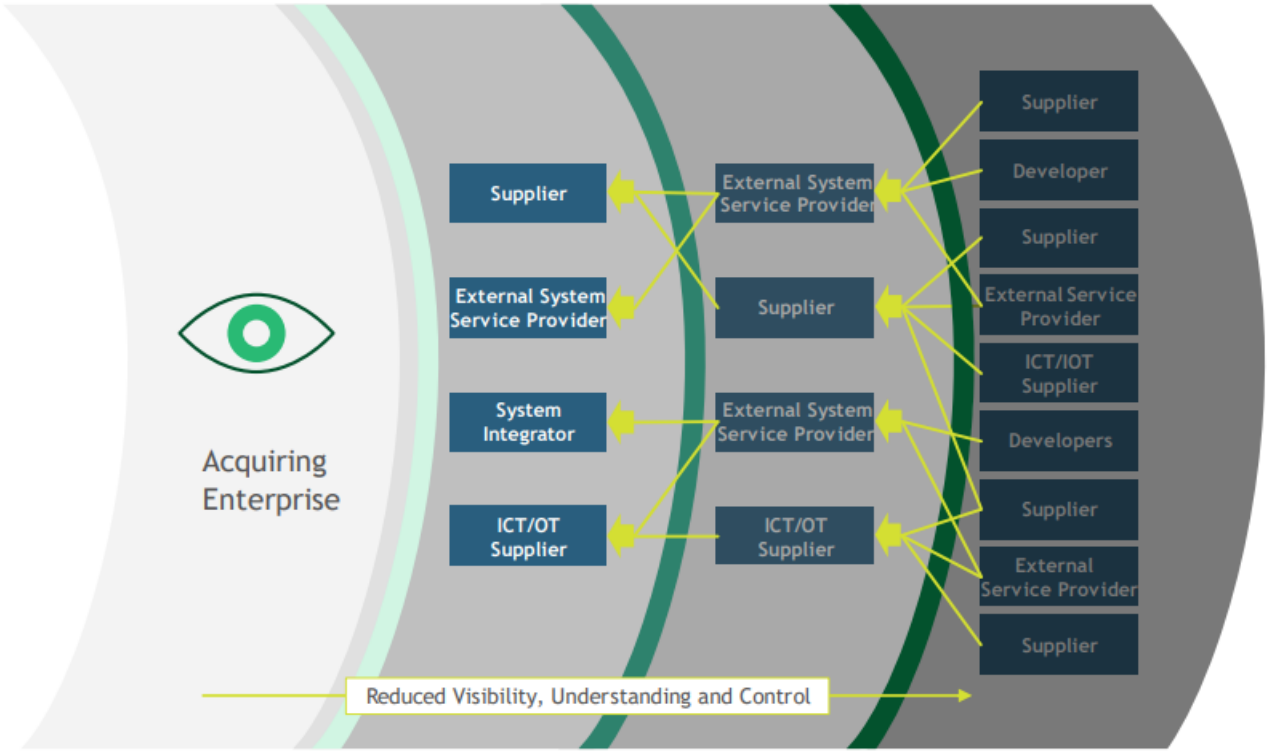
Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zero-Day Schwachstellen bei Cyber-Angriffen auf verschiedene Ivanti-Produkte genutzt

Warum gerade Lieferanten und Dienstleister?

Wir haben hohe Abhängigkeiten mit unseren Lieferanten & Dienstleister



Source:
NIST.SP.800-161r1

nviso

Viele Organisationen fehlt es an Visibilität und Verständnis, wie das eingesetzte Produkt oder Dienstleistung entwickelt und eingesetzt wird.

In unserer digitalen Welt ist die enge Verflechtung von Lieferketten Realität und nicht wegdenkbar – dies schafft Abhängigkeiten sowie “unvorhersehbare” Risiken.

Warum gerade Lieferanten und Dienstleister?

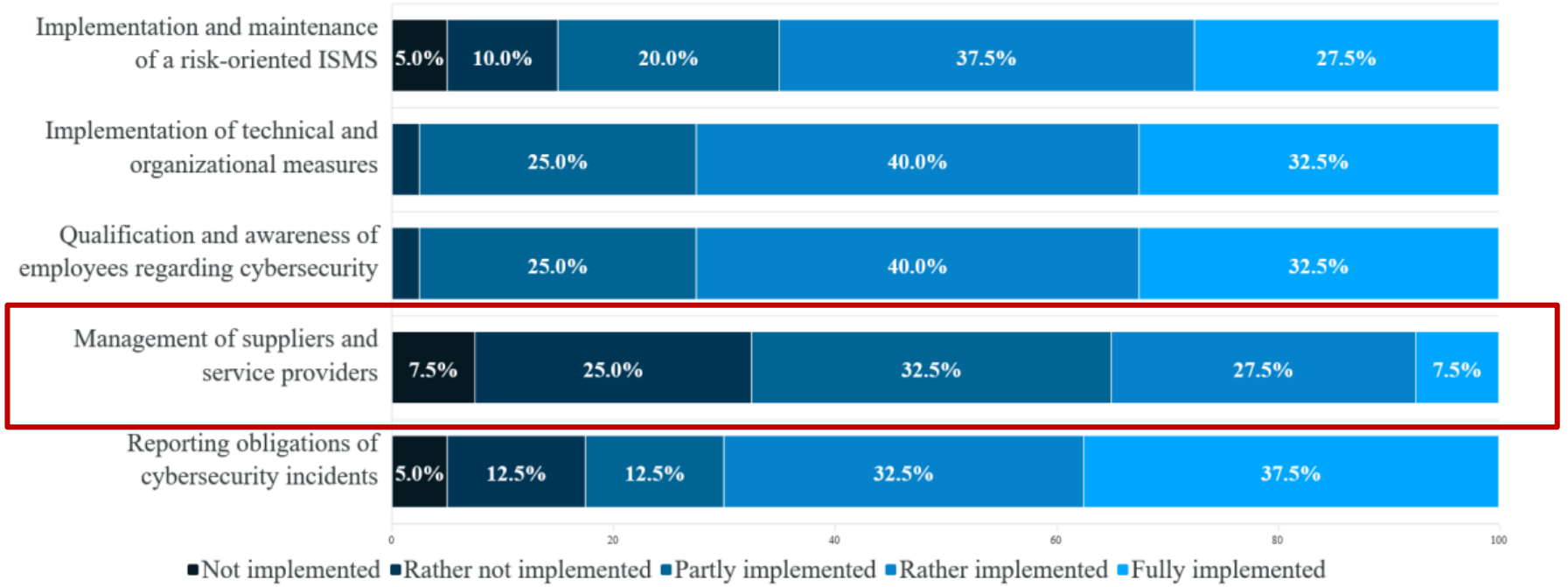
Wir haben hohe Abhängigkeiten mit unseren Lieferanten & Dienstleister

- Aus den Erfahrungen der Vergangenheit kann nicht unbedingt immer auf die Zukunft geschlossen warden.
- Wie können wir auf der Grundlange von [endlichen] bekannten Eigenschaften auf das [unendliche] Unbekannte schließen?

#dontbetheturkey

Warum gerade Lieferanten und Dienstleister?

Ganzheitlicher Ansatz von Cyber Risiken im Supply Chain

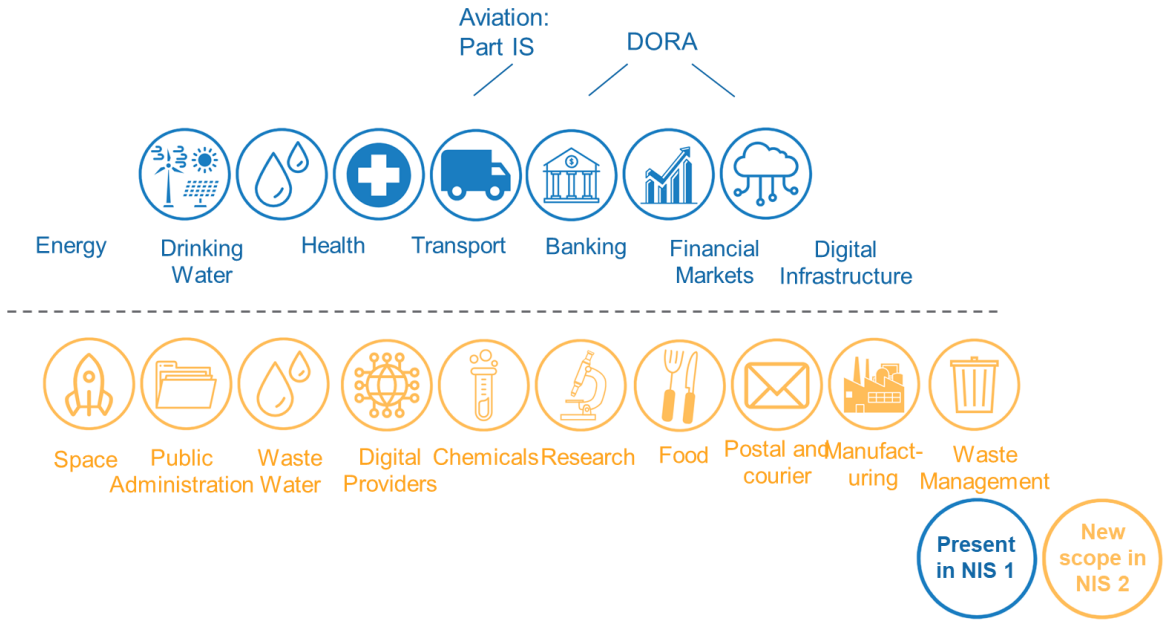


Source:
Fellerer, 2023; Universität Regensburg

- Eine empirische Studie der Universität Regensburg aus dem Jahr 2023 zeigt auf, dass eine geringe Anzahl von Unternehmen einen ganzheitlichen Ansatz von Cyber Risiken im Supply Chain besitzen.

Warum gerade Lieferanten und Dienstleister?

Gesetzliche Lage für Organisationen NIS2



- NIS2 betrifft in Deutschland circa 30.000 Unternehmen direkt und mehr als 300.000 Unternehmen indirect über Lieferketten.
- Verpflichtungen bzgl. Lieferanten & Dienstleistern findet sich insbes. **Artikel 21 Abs. 2d+e, Abs. 3**

Warum gerade Lieferanten und Dienstleister?

Gesetzliche Lage für Produkte EU Cyber Resilience Act

- Hersteller von Produkten mit digitalin Elementen müssen künftig die Sicherheitsmaßnahmen nachweislich umsetzen – Security by Design
- **EU Cyber Resilience Act, inbes. Annex I, II, V**

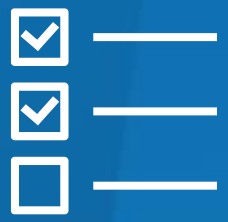
Warum gerade Lieferanten und Dienstleister?

Unsere Herausforderungen

nviso

Es gibt im Bereich von Lieferantenmanagement einige Herausforderungen:

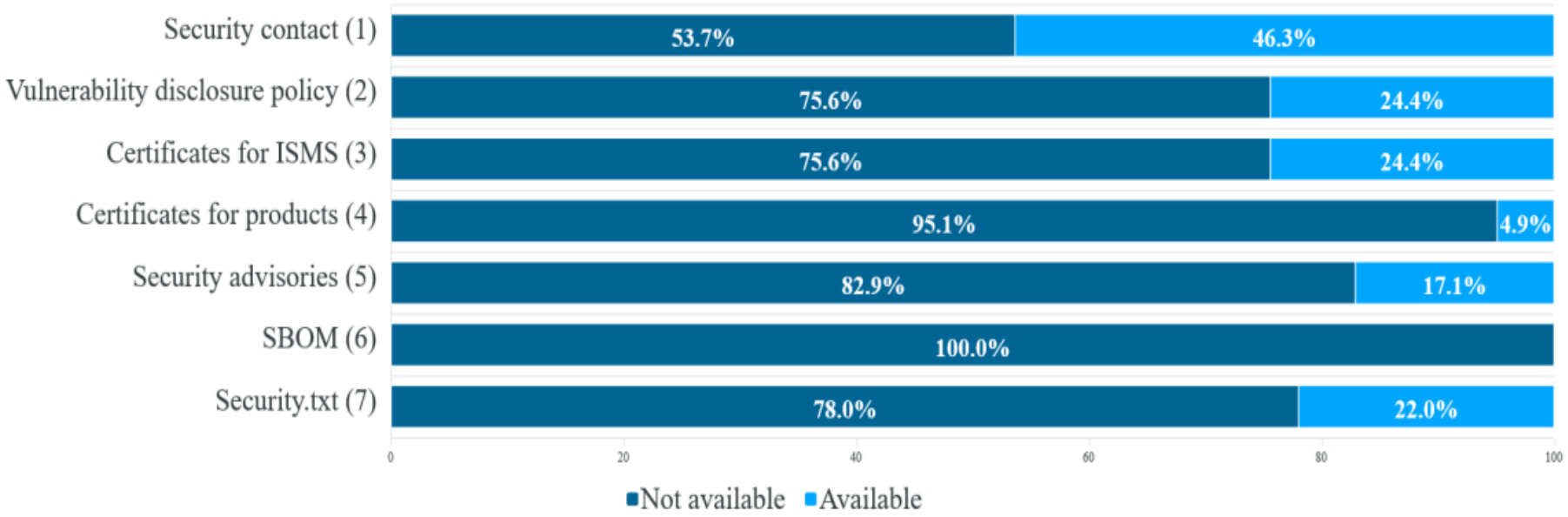
- Starke Abhängigkeit in einer digital-vernetzten Welt
- Steigende gesetzliche Anforderungen
- Fehlender ganzheitlicher Ansatz
- Mangelnde Sichtbarkeit & „es ist ja immer schon gut gegangen“



Was können Sie tun?

Was können Sie tun?

Effizienz und Transparenz helfen dabei

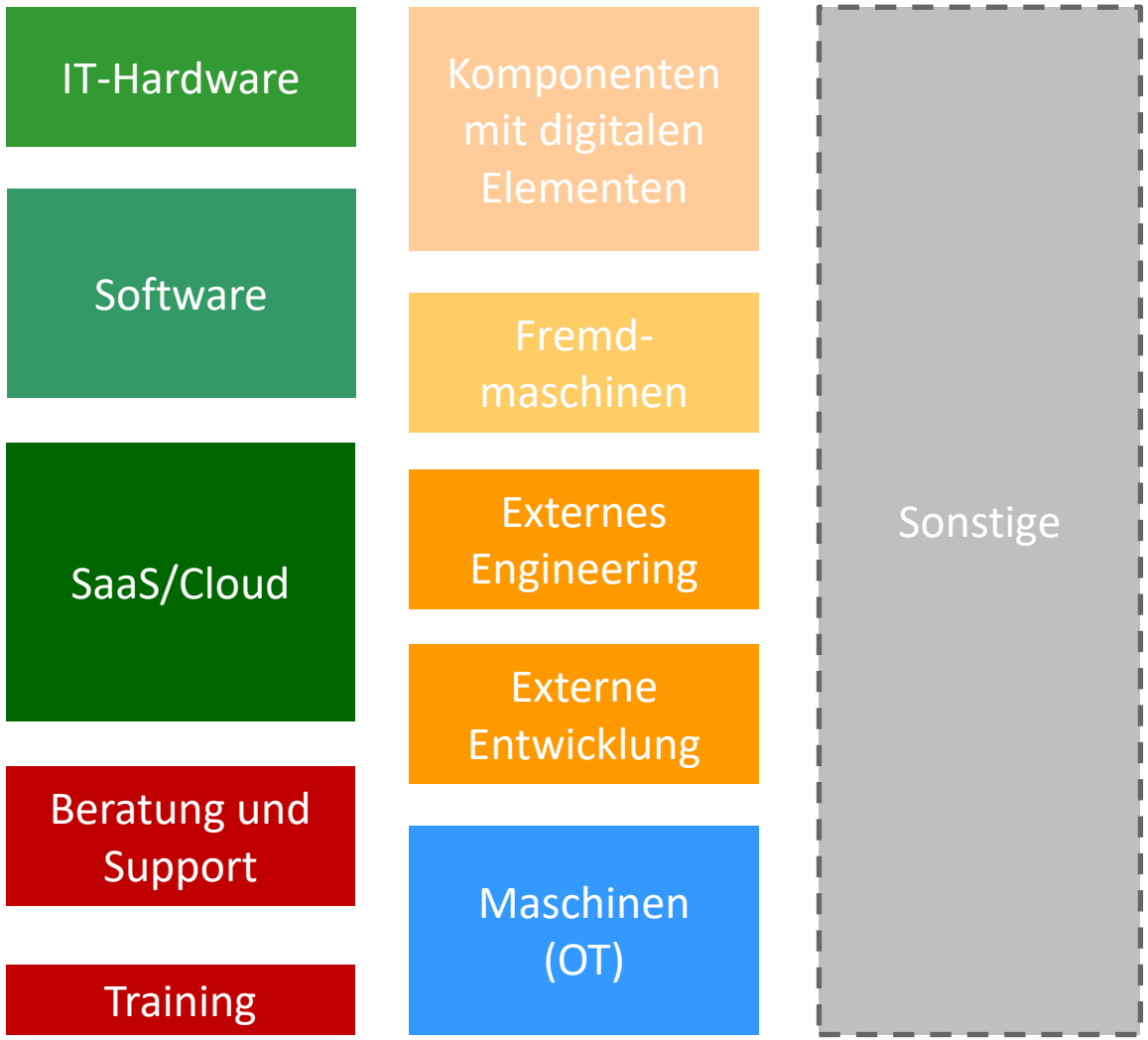


Source:
Fellerer, 2023; Universität Regensburg

- Transparenz durch “einfache” Security Maßnahmen schaffen.
- Von den befragten Unternehmen hatten, die wenigstens Maßnahmen umgesetzt, um Transparenz zu schaffen.

Was können Sie tun?

Lieferanten Kategorisieren und Priorisierung



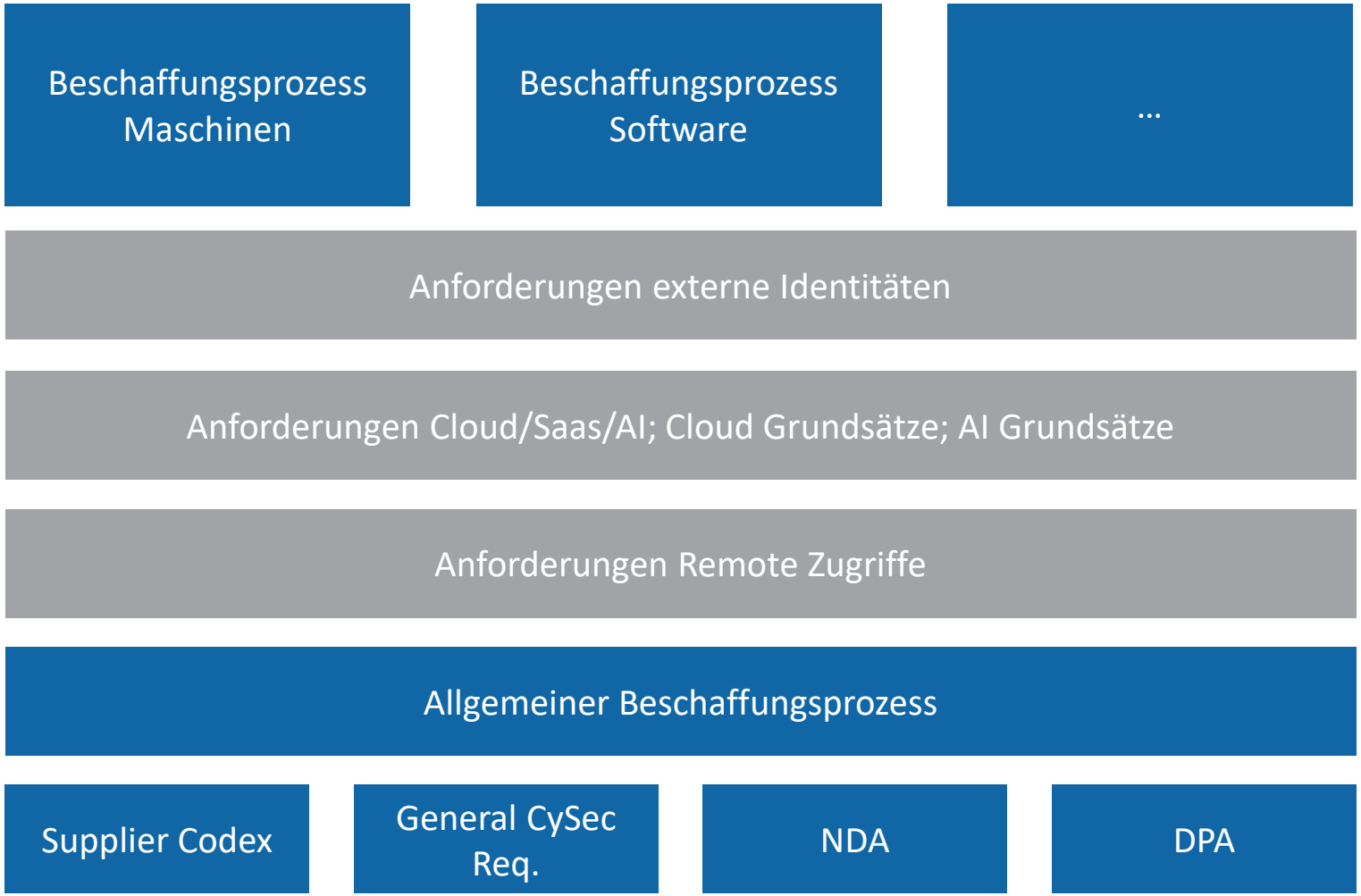
Source:
Nowey, 2023; Krones AG

nviso

- Die Kategorisierung von Lieferanten & Dienstleistern kann beispielsweise nach Anwendungsgebiet erfolgen.
- Die Priorisierung von Lieferanten kann mittels Auswertungen von BIA-Analysen erfolgen, um die Kritikialität des Lieferantens zu bestimmen.

Was können Sie tun?

Unterschiedliche Maßnahmen für unterschiedliche Arten von Lieferanten



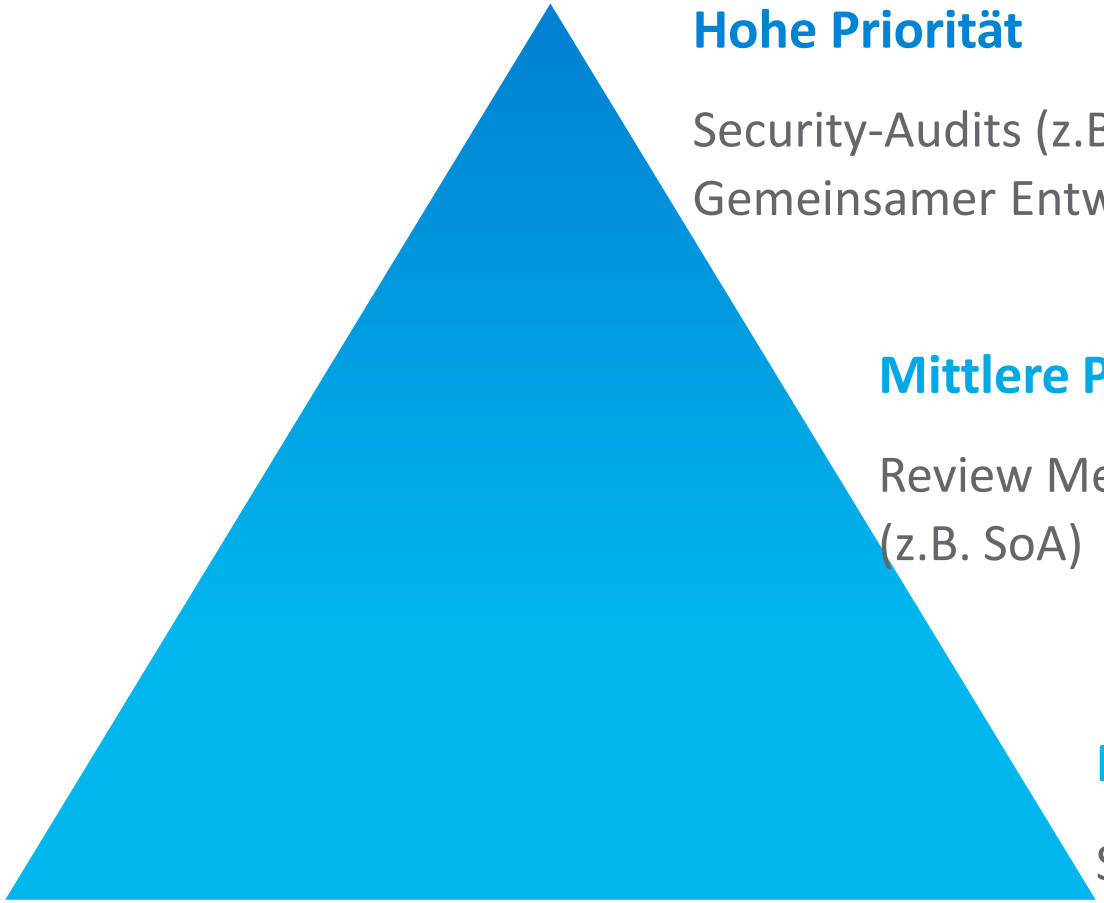
Source:
Nowey, 2023; Krones AG

Toolbox

- Direkte Abstimmung
- Richtlinien
- Vertragsvorlagen
- Cloud&AI Grundsätze
- External Attack Surface Assessment
- Checklisten & Self-Assessments
- Dokumentationen
- Zertifikate/Nachweise
- Lastenhefte/Spezifikationen
- Audits
- Review Meetings
- Anbindung Due Diligence Tools

Was können Sie tun?

Unterschiedliche Maßnahmen für unterschiedliche Arten von Lieferanten



Hohe Priorität

Security-Audits (z.B. Penetrationstests); Gemeinsamer Entwicklungsprozess

Mittlere Priorität

Review Meetings; Zertifikate/Nachweise (z.B. SoA)

Niedrige Priorität

Self-Assessment; Vertragliche Vereinbarungen

nviso

Je nach Kritikalität des Lieferanten und Dienstleister hat dieser eine höhere bzw. Niedrigere Auswirkung auf Ihr Unternehmen. Aus diesem Grund sollten Sie dementsprechend unterschiedliche Maßnahmen walten lassen. Eine allgemeine Due Diligence ist jedoch immer empfehlenswert.

Was können Sie tun?

Unterschiedliche Maßnahmen für unterschiedliche Arten von Lieferanten

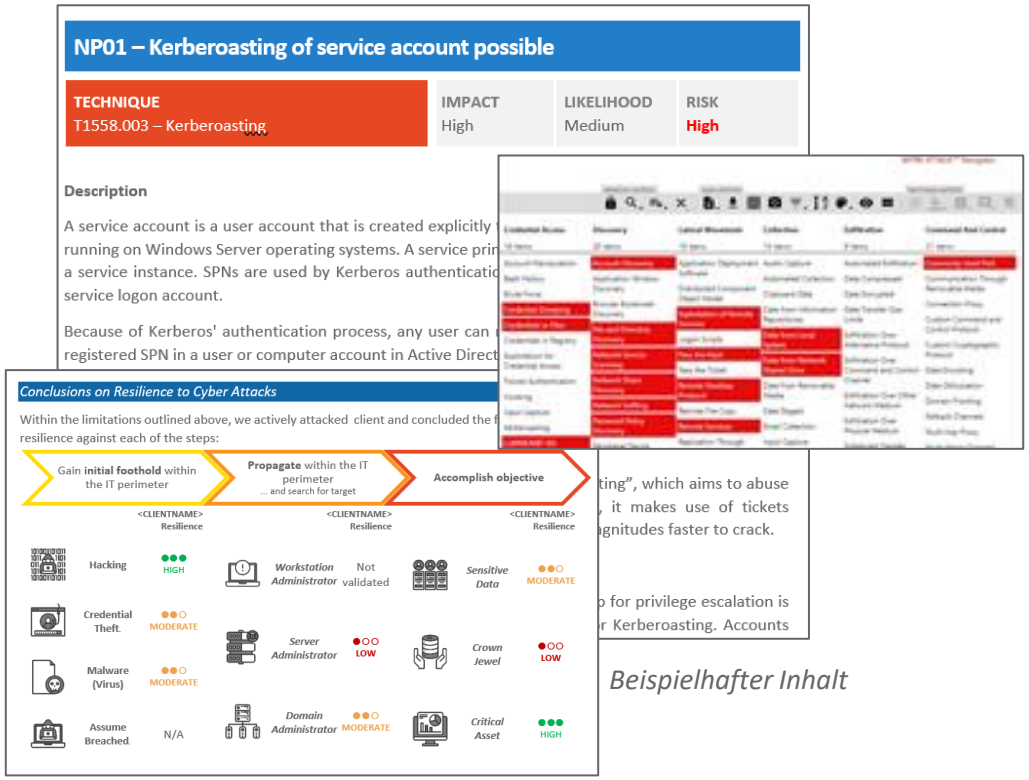
Je nach Bedarf kann der komplette Lebenszyklus auditiert werden, um die Einhaltung entsprechender Sicherheitsmaßnahmen zu gewährleisten!

nviso

- Unsere Erfahrung zeigt, dass bis zu 90 % aller Software-Schwachstellen hätten vermieden werden können, wenn bereits zu Beginn des Softwareentwicklungszyklus (SDLC) sichere Programmierung mit Quality Gates angewandt worden wären.

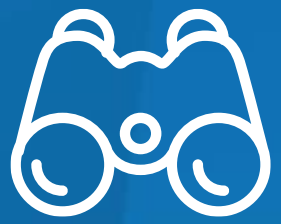
Was können Sie tun?

Unterschiedliche Maßnahmen für unterschiedliche Arten von Lieferanten



Beispielhafter Inhalt

- Gesamthafte externe Assessment von Lieferanten helfen die eigene Resilienz zu stärken und zu erhöhen – bei unseren Assessments von kritischen Dienstleistern oder Lieferanten verwenden wir allgemeingültige Frameworks, um potentielle Gefährdungen transparent aufzuzeigen.



Ausblick

Was können Sie tun?

Stärken Sie Ihre eigene Resilienz

1. Unternehmen müssen sich den kommenden gesetzlichen **Anforderungen schrittweise annähern**
2. Verbesserung der Lieferanten durch **klare, abgestimmte Vorgaben** und konstruktiven Austausch
3. Eigene **Resilienz stärken** durch regelmäßige Prüfung Ihrer Lieferanten
4. Zukünftige Herausforderungen z.B. im Schwachstellenmanagement lassen sich nur mit **Automatisierung** lösen
   → Automatisierung braucht standardisierte Daten und Formate
   → CPE/eindeutige Identifier, BSI CSAF, OWASP CycloneDX (SBOM)
5. Schaffen **Sie Transparenz und Verlangen Sie dies von Ihren Lieferanten**
   → Basisinformationen öffentlich/leicht zugänglich machen z.B. security.txt auf der Website

nviso

VDMA

VDMA-Lastenheft

Supply Chain Security

Praktische Ransomware Simulation

Testen Sie Ihre Resilienz gegen Ransomware-Angriffe durch eine ganz praktische Prüfung.

COMMERZBANK

Für Commerzbank-Kunden für nur 9.900 €

Gültig nur bis Ende Mai 2025

Unser Vorgehen:

Kick-Off
Wir einigen uns auf ein Szenario und die konkreten Rahmenbedingungen für die Simulation und halten diese in einem Simulationsplan fest.

Ausführung
Unsere sichere Ransomware wird auf den Zielsystemen ausgerollt. Je nach Szenario wird das IT Teamvon dem Angriff informiert oder nicht.

Entdeckung & Wiederherstellung
Ihr IT-Team entdeckt den Angriff und folgt den Playbooks zur Wiederherstellung der betroffenen Systeme.

Erkenntnis und Maßnahmenplan
Wir stellen die Lücken bei der Erkennung und Wiederherstellung fest und leiten die Maßnahmen zur Behebung ab.

nviso.eu

Codename „Cardinalis“

Von NVISO‘s Red Team speziell für Ransomware-Simulationen entwickelte Ransomware.

Hauptmerkmale:

- **Realismus:** Entwickelt basierend auf dem Vorgehen echter Ransomware
- **Sicherheit**: Verschlüsselt nur die für die Simulation konfigurierten Dateien und Ordner
- **Unsichtbar**: Bietet fortschrittliche Techniken zur Umgehung von AV und EDR
- **Modularität**: Kann mit verschiedenen Funktionen ausgeführt werden, z. B. C2-Kommunikation
- **Protokollierung**: Integrierte Protokollierung zur Unterstützung des Blue Teams bei Untersuchungen und Folgemaßnahmen.

Referenzen

Referenzen

- https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/kuenstliche-intelligenz-wie-neuartige-cyberattacken-mit-ki-die-banken-bedrohen/29091744.html
- https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/bundesbank-projekt-tiber-wir-greifen-auf-drei-wegen-an-so-lassen-sich-deutsche-banken-fast-immer-hacken/27686376.html
- https://www.faz.net/pro/d-economy/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html
- https://www.heise.de/hintergrund/Kaseya-VSA-Wie-die-Lieferketten-Angriffe-abliefen-und-was-sie-fuer-uns-bedeuten-6129656.html
- https://www.mandiant.de/resources/blog/accellion-fta-exploited-for-data-theft-and-extortion
- https://www.tagesschau.de/wirtschaft/finanzen/bafin-cyberangriffe-warnung-100.html

Referenzen

- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-205101-1032.pdf?__blob=publicationFile&v=2
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
- BaFin - Rundschreiben - Rundschreiben 11/2021 (BA) - Zahlungsdiensteaufsichtliche …
- https://securitytxt.org/
- https://datatracker.ietf.org/doc/html/rfc9116
- https://www.vdma.org/viewer/-/v2article/render/73448513
- https://www.vdma.org/viewer/-/v2article/render/82349740
- https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- https://eur-lex.europa.eu/eli/dir/2022/2555

Referenzen

- https://www.faz.net/pro/d-economy/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html
- https://www.heise.de/hintergrund/Kaseya-VSA-Wie-die-Lieferketten-Angriffe-abliefen-und-was-sie-fuer-uns-bedeuten-6129656.html
- https://www.mandiant.de/resources/blog/accellion-fta-exploited-for-data-theft-and-extortion
- BaFin - Rundschreiben - Rundschreiben 11/2021 (BA) - Zahlungsdiensteaufsichtliche …
- https://dsgvo-gesetz.de/art-33-dsgvo/
- https://dsgvo-gesetz.de/art-82-dsgvo/
- https://dsgvo-gesetz.de/art-58-dsgvo/
- https://dsgvo-gesetz.de/themen/bussgelder-strafen/
- https://www.openkritis.de/eu/eu-nis-2-direktive-kritis.html
- https://www.heise.de/news/Ivanti-VPN-Sicherheitsluecken-fuehren-zu-tausenden-kompromittierten-Geraeten-9599887.html
- https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html
- https://www.handelsblatt.com/technik/it-internet/java-bibliothek-log4j-warnstufe-rot-sicherheitsluecke-gefaehrdet-die-it-zahlreicher-unternehmen/27885628.html