secuvera:
Cybersicherheit. Nachhaltig.

Wie Sie Ihr Unternehmen strategisch wappnen – Regulatorik wie NIS2 oder CRA?

COMMERZBANK

Tobias Glemser

(c) secuvera GmbH

Geschäftsbereiche

secuvera:
Cybersicherheit. Nachhaltig.

BSI-Prüfstelle

CRA-Beratung & Prüfung
Common Criteria, BSZ
TR-Prüfungen, Industrial
Security (IEC 62443)

Penetrationstests

u. a. Webanwendungen,
Ransomware-Simulation,
Red-Teaming, AD-Analysen

Sicherheitsberatung

NIS2-Beratung, BSI-GS/ISO27001/TISAX

CISO as a Service (CaaS)

Schulung und Herstellerberatung

OWASP® Top 10, SSDL, 27001, Cyber für KMU

Zertifizierungen und CRA

(c) secuvera GmbH

secuvera:
Cybersicherheit. Nachhaltig.

- 50 Mitarbeitende
- IT-Sicherheit seit 1988

- BSI-Grundschutz Auditoren,
  -Berater & -Praktiker
- ISO 27001 Lead Auditoren
- BCM Praktiker
- BSI-zertifizierte Pentester
- Common Criteria Evaluatoren
- Cyber Security Practitioner
- KRITIS-Prüfer
- TR-Prüfer
- ..

(c) secuvera GmbH

whoami

secuvera:
Cybersicherheit. Nachhaltig.

- Tobias Glemser, Geschäftsführer und Gesellschafter
- 25 Jahre in der Branche
- BSI-zertifizierter Penetrationstester
- OWASP German Chapter Lead

(c) secuvera GmbH

Bilderrätsel

(c) secuvera GmbH

Ausgangslage

CHRONIK

Hackerangriff: Mil

Nach dem Cyberangriff auf Salzburg
Produktion am Standort in Salzburg
stehe noch bis mindestens Montag

Salatknappheit: Produktionsausfall in den USA bei Dole nach Ransomware-Attacke

e und Schnittblumen Dole wurde Opfer
e temporär

Traditionsfirma mit über 400 Angestellten in der Insolvenz – nach Cyberattacke

14.10.2024, 16:24 Uhr

Nach Cyb
Tischlere

als 70 Kommunen lahm

Auch gut einen Monat nach dem Cyberangriff auf die Industrie- und Handelskammern (IHK) in Deutschland gibt es dort noch Einschränkungen.

Die Folgen ei
IT-Netzwerk von Tegut. Für Kunden habe dies allerdings

IT des irischen

kenfm.de: Anonymous hackt Website des Aktivisten Ken Jebsen

Nacht von einer
– mit Folgen für das

Das Hackerkollektiv hat Zugriff auf kenfm.de erlangt und von dort nach eigenen Angaben 3 GByte Daten kopiert.

VERSICHERUNG

Asiatische Axa-Partner von Ransomware getroffen

Teile des Versicherungskonzerns Axa in Asien wurden von einem Ransomware-Angriff getroffen, es soll um 3 Terabyte Daten gehen.

(c) secuvera GmbH

secuvera:
Cybersicherheit. Nachhaltig.

Größter Hack aller Zeiten

(c) secuvera GmbH

Ausgangslage

Ort Bonn
Datum 19.09.2024

Quelle: BSI/bitkom

Gestrichene Flüge, ausgefallene Server und PCs, Unternehmen, die ihre Beschäftigten nach Hause schicken mussten – vor zwei Monaten, am 19. Juli 2024, ging vielerorts nichts mehr. Ein fehlerhaftes Update einer Cybersicherheitslösung des Unternehmens CrowdStrike hatte weltweit zu zahlreichen IT-Ausfällen geführt. Welche Folgen die Panne für Unternehmen in Deutschland hatte, haben jetzt das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Digitalverband Bitkom in einer gemeinsamen Befragung von 331 von den Ausfällen betroffenen Unternehmen ermittelt.

- Fast die Hälfte der betroffenen Unternehmen musste zeitweise Betrieb einstellen
- Mehrheit bessert Notfallpläne nach – und hält IT-Ausfälle für unvermeidbar
- BSI und Bitkom legen Ergebnisse einer gemeinsamen Unternehmens-Befragung vor

Die Untersuchung ist nicht repräsentativ, gibt aber ein aussagekräftiges Stimmungsbild. 62 Prozent der damals betroffenen Unternehmen litten unter direkten Folgen, wie dem Ausfall der eigenen PCs oder Server. 48 Prozent spürten indirekte Auswirkungen, weil zum Beispiel Zulieferer, Kunden oder Geschäftspartner betroffen waren. Knapp die Hälfte der direkt oder indirekt betroffenen Unternehmen (48 Prozent) musste daraufhin vorübergehend den Betrieb einstellen – im Schnitt für 10 Stunden. Rund drei Viertel (73 Prozent) bezeichnen rückblickend die entstandenen Probleme und Störungen als gravierend für die deutsche Wirtschaft. Zugleich sind zwei Drittel (64 Prozent) mit Blick auf das eigene Unternehmen aber auch sicher: Ein solcher Vorfall lässt sich nicht vollständig verhindern.

(c) secuvera GmbH

Ausgangslage

11.10.24 18:22
Börse Global

Die CrowdStrike-Aktie setzt ihren beeindruckenden Aufwärtstrend fort und verzeichnete am 11. Oktober 2024 einen weiteren Kursgewinn. Mit einem Plus von 1,56% schloss die Aktie bei 292,40 EUR und liegt damit 15,31% über dem Kurs des Vormonats. Besonders bemerkenswert ist der Jahresvergleich: In den letzten zwölf Monaten konnte der Aktienkurs um satte 67,86% zulegen, was das starke Interesse der Investoren an dem Cybersecurity-Unternehmen unterstreicht.

Wachstum trotz hoher Bewertung

Trotz der hohen Bewertung mit einem KUV von 22,27 für das laufende Jahr zeigt sich die CrowdStrike-Aktie weiterhin in Topform. Das Unternehmen profitiert von der steigenden Nachfrage nach Cloud-basierten Sicherheitslösungen und seiner führenden Position im Markt für Endgeräteschutz und Bedrohungsabwehr. Anleger sollten jedoch die hohe Bewertung im Auge behalten und mögliche Kursschwankungen einkalkulieren.

(c) secuvera GmbH

Ausgangslage

(c) secuvera GmbH

Jetzt neu: Regulierung für IT-Kram

secuvera:
Cybersicherheit. Nachhaltig.

- Heutiger Fokus
  - NIS2 (Network and Information Security)
  - CRA (Cyber Resilience Act)
  - Praxis

(c) secuvera GmbH

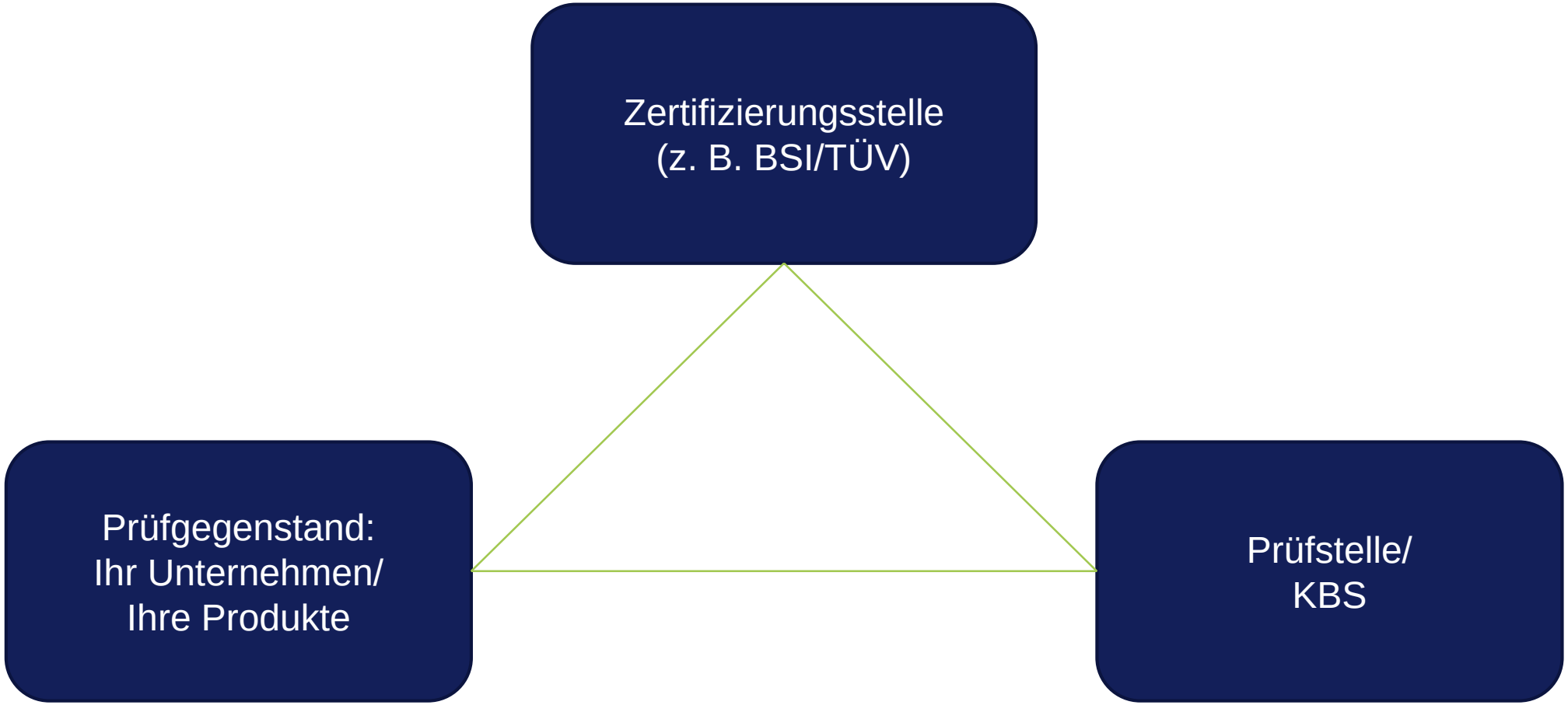
Grundsätzlich

secuvera:
Cybersicherheit. Nachhaltig.

- Gesetze erfüllen = Normen und Standards umsetzen (+ bisschen Extras, meist Meldepflichten)
- Normen und Standards **rechtssicher** umsetzen = Zertifizierung

(c) secuvera GmbH

Zertifizierung?



(c) secuvera GmbH

NIS2 und CRA im Vergleich: Anwendungsbereich

secuvera:
Cybersicherheit. Nachhaltig.

Merkmal	NIS2	CRA
Ziel	Stärkung der Cybersicherheit für Betreiber kritischer Dienste und wesentliche Einrichtungen.	Erhöhung der Cybersicherheitsstandards für Produkte mit digitalen Elementen (Hard- & Software).
Adressaten	Kritischen Sektoren (z. B. Energie, Transport, Finanzen, Gesundheit, digitale Infrastruktur).	Hersteller, Importeure und Händler von Produkten mit digitalen Elementen in der EU.
Pflichten	Sicherheitsmaßnahmen und Meldepflichten für Betreiber wesentlicher Dienste.	Sicherheitsanforderungen für Produkte mit dig. Elementen über den gesamten Lebenszyklus.

(c) secuvera GmbH

NIS2 und CRA im Vergleich: Umsetzung

secuvera:
Cybersicherheit. Nachhaltig.

Merkmal	NIS2	CRA
Ziel	EU-Richtlinie → Muss von Mitgliedsstaaten in nationales Recht umgesetzt werden.	EU-Verordnung → Gilt direkt in allen Mitgliedsstaaten ohne zusätzliche Umsetzung.
Überwachung	Nationale Behörden überwachen und sanktionieren Verstöße.	Marktüberwachung (CE-Kennzeichen)
Meldepflicht	Cybervorfälle müssen innerhalb von 24 Stunden gemeldet werden.	Sicherheitslücken in Produkten müssen innerhalb von 24 Stunden an ENISA gemeldet werden.
Sanktionen	Strafen bis zu 10 Mio. € oder 2 % des globalen Umsatzes.	Strafen bis zu 15 Mio. € oder 2,5 % des globalen Umsatzes.

(c) secuvera GmbH

Zoom auf NIS2: Einordnung

secuvera:
Cybersicherheit. Nachhaltig.

- NIS2-Umsetzungsgesetz aufgrund „Regierungsumbildung“ nicht da (Frist war Oktober 24)
- Ca. 30.000 Unternehmen betroffen

11	Anwendung auf Bundesverwaltung	Art. 1 § 29, 44 BSIG	Keine Aufnahme wegen Kosten

- KRITIS Dachgesetz gilt weiterhin

(c) secuvera GmbH

Zoom auf NIS2: Einordnung

secuvera:
Cybersicherheit. Nachhaltig.

- 18 Sektoren wie Energie, IT und TK, Ernährung
- „Wichtige Einrichtungen“: >50 MA oder Umsatz >10 Mio
- „Besonders wichtige Einrichtungen“: >250 MA oder Umsatz >50 Mio
- Speziell: DNS, QTS, TLD, TK-Anbieter
- Betroffene Unternehmen müssen sich selbst registrieren
- https://nis2-check.de/#check

(c) secuvera GmbH

Zoom auf NIS2: Einordnung

secuvera:
Cybersicherheit. Nachhaltig.

- Audits: Nicht verpflichtend (außer wenn KRITIS-Unternehmen)
- Zertifizierung
- Persönliche Haftung für GF ist aktuell nicht mehr dabei

(c) secuvera GmbH

Zoom auf NIS2: Umsetzung

secuvera:
Cybersicherheit. Nachhaltig.

- Risikomanagement/Informationssicherheitsmanagementsystem (ISMS) einführen
  - ISO 27001 (einfacher)
  - BSI-Grundschutz (detaillierter, konkreter, aufwändiger)
- Business Continuity Management (BCM) einführen
  - ISO 22301
  - BSI Standard 200-4

(c) secuvera GmbH

Zoom auf NIS2: Umsetzung

secuvera:
Cybersicherheit. Nachhaltig.

- Schulungen (auch GF) verpflichtend (NIS2UmsuCG § 38 Absatz (3))
- Prozess für Meldepflichten/Krisenmanagement
- Registrierung

💡 Auch ohne NIS2-Zwang sinnvoll

(c) secuvera GmbH

Zoom auf CRA

secuvera:
Cybersicherheit. Nachhaltig.

- In Kraft seit 11. Dezember 2024
- Fokus: Produkte mit digitalen Elementen (salopp: Kann Verbindungen aufbauen/annehmen)
- Gilt nicht für:
  - Medizinprodukte
  - KFZ
  - Zivilluftfahr und Flugsicherheit
  - Verteidigung

(c) secuvera GmbH

Zoom auf CRA

secuvera:
Cybersicherheit. Nachhaltig.

- Meldepflicht von Schwachstellen ab 11. September 2026
- Einhaltung in Produkten ab 11. Dezember 2027, sonst kein CE-Kennzeichen

(c) secuvera GmbH

Praxis

(c) secuvera GmbH

Anfangen. Jetzt. Wirklich.

secuvera:
Cybersicherheit. Nachhaltig.

- Extrem unterschiedliche Reifegrade
- Meist ein längerer, denn ein kürzerer Weg
- GAP-Analyse bleibt der beste Einstieg
- Nähkästchen: DiGAs als „CRA-Prototyp“

(c) secuvera GmbH

Bilderrätsel

(c) secuvera GmbH

secuvera:
Cybersicherheit. Nachhaltig.

Danke sehr!

Weitere Fragen? Beratungsbedarf? Gerne melden.

tglemser@secuvera.de

www.secuvera.de