
Spam!
CLOUD
BERLIN
heinlein
shutdown -h now
PHP OR PYTHON
RUHE!
ANMELDUNG
EINGANG
EIN ROOT FÜR ALLE FÄLLE
heinlein
PEST
ccc
Code of conduct
Bar

heinlein

NIS2:
Sind wir nicht alle ein bisschen KRITIS?

Darf ich mich noch kurz vorstellen…

Wir sind Experten für freie und sichere Kommunikation.

Seit über 30 Jahren.

- Die Heinlein-Gruppe
- Linux Consulting und Linux Akademie in Berlin
- Wir betreiben eigene ISPs und Datacenter in Berlin

- Betreiber des Testsiegers „mailbox.org“
- Gründer des Videokonferenz-Systems „OpenTalk“

- Unsere DNA: Datenschutz & Digitale Souveränität
- Expertise mit über 85 Mitarbeitern
- Open Source und Server-Experten durch und durch

- https://www.heinlein-support.de
- https://opentalk.eu

Ein Hallo auch von mir!

Das Suppenkoma überwinden wir ;)

Torsten Hallmann

- Head of Public Affairs
- Historie: Einzelhandel, Support, PreSales

SUSE

- Weltweit führender Anbieter innovativer, zuverlässiger und sicherer Open Source-Lösungen
- Auf geschäftskritische Lösungen im Bereich Linux, Enterprise Container-Management- und Edge spezialisiert
- Breite und aktive Zusammenarbeit mit Partnern und Communities

Was bisher geschah…

- Seit 2015 gibt es Regelung zum Schutz von „Kritischen Infrastrukturen“: KRITIS.
- Für Infrastrukturen, die nicht ausfallen dürfen.
  - Besondere Anforderungen
  - Besondere Dokumentationen
  - Besondere Absicherungen
- Bislang rund 2.700 Unternehmen in Deutschland
  - Vorzugsweise Energie-Sektor/-versorgung etc. etc.
- Wurde 2021 nochmal überarbeitet.
- Hat sich soweit etabliert und ist „da“.

Die Resilienz der Daseinsvorsorge

- Der Staat muss die Versorgung seiner Bevölkerung sicherstellen
- Aber immer mehr hoheitliche Versorgungsaufgaben wurden privatisiert
- Gleichzeitig hängt immer mehr von der IT ab
  - Systeme und Gesellschaft brechen ohne IT zusammen.
- Also muß der Staat regulieren und Vorschriften machen, um das sicherzustellen
- Schaden durch Cybercrime derzeit pro Jahr: > 200 Mrd €.

NIS 2 Richtlinie (EU 2022/2555)

In Kraft auf EU Ebene – Nationale Umsetzung in Arbeit

- Löst Vorgängerregelung aus 2016 ab (EU 2016/1148)
- Konkreterer und erweiterter Geltungsbereich
- Schreibt Anwendung von Maßnahmen für das Cyber Risk Management vor
- Fordert strikte Meldepflicht von Vorfällen
- Beinhaltet hohe Sanktionen bei Nichteinhaltung
- Umsetzung in nationales Recht bis spätestens 17. Oktober 2024

heinlein

Gebt mir ein…

NIS2UmsuCG

Darf ich präsentieren? Das NIS2UmsuCG!

- Anfang Januar auf EU-Ebene mit NIS2 beschlossen:

Das NIS2 Umsetzung- und Cybersicherheitsgesetz (NIS2UmsCG)

- Soll die allgemeine Versorgungssicherheit verbessern und die Gesellschaft resilienter machen.
  - Da kann man ja erstmal nix dagegen haben.

- Wer ist betroffen?
  - Unternehmen in besonderen Bereichen „Sektoren“
  - Ab einer gewissen Größe
  - Ggf. für bestimmte Dienste

Wer ist von NIS2 betroffen?
(1) Das kommt auf den Bereich an.

- Unternehmen aus 18 definierten Bereichen („Sektoren“)
  - Mehr als beim bisherigen KRITIS – neue Bereiche! Unwissenheit!

- 11 wesentliche Sektoren („essential“):
  - Energie, Transport, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser
  - Öffentliche Verwaltung, Raumfahrt
  - Digitale Infrastruktur

- 7 wichtige Sektoren:
  - Post und Kurier, Abfallwirtschaft, Chemikalien, Ernährung, Industrie, Forschung
  - Digitale Dienste

Wer ist von NIS2 betroffen?
(2) Das kommt auf die Größe an

- NIS2 unterscheiden zwei große Bereiche

- Ab 250 Mitarbeitern oder 50 M€ Jahresumsatz
  - Sind „besonders wichtige Einrichtungen"
  - Aktive Nachweispflicht der Maßnahmen

- Ab 50 Mitarbeitern oder 10 M€ Jahresumsatz
  - Sind „wichtige Einrichtungen“
  - Keine aktive Nachweispflicht – aber trotzdem Umsetzung!

Richtlinie zur Netz- und Informationssicherheit (NIS2)

Geltungsbereich (Artikel 2 & 3)

Mittlere Unternehmen:
50 bis 250 Beschäftigte,
10 bis 50 Mio. € Umsatz,
‹ 43 Mio. € Bilanzsumme

Große Unternehmen:
› 250 Beschäftigte,
› 50 Mio. € Umsatz,
› 43 Mio. € Bilanzsumme

Aber:
Je nach Kritikalität und Position des Unternehmens sind Ausnahmen nach unten möglich!

Wer ist von NIS2 betroffen?
War's das? NEIN!

- Achtung: Klein- und Kleinstunternehmen auch bei „Digitale Infrastruktur“, „Öffentliche Verwaltung“ und einigen Sonderfällen!
  - DNS und TLD-Registry
  - Qualifizierte Vertrauensdienste
  - Öffentliche Kommunikationsnetze/Dienste

- Zulieferer/Dienstleister eines NIS2-Unternehmens sind durch die Sicherstellung der Lieferkette ebenfalls verpflichtet, NIS2-Standards einzuhalten!
  - Hallo wach? Das sind wir hier!

Was müssen NIS2-Unternehmen tun?

- Diese Unternehmen müssen umfangreich Vorsorge zur Cybersicherheit treffen
  - Risikoanalyse
  - Risikomanagement
  - Krisenmanagement
- KRITIS für Arme!

Richtlinie zur Netz- und Informationssicherheit (NIS2)

Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21)

a) Information Security Management

b) Incident Response / Incident Management

c) Business Continuity Management

d) Third Party Risk Management

e) Vulnerability Management

f) Pentesting/Auditing

g) Sensitization & Training

h) Cryptography & Encryption

i) Access Management

j) Authentication Management

Welche Aufgaben entstehen bei einer NIS2-Umsetzung?

- Konzepte: Risikoanalyse und IT-Sicherheit
- Incident Management: Prävention, Detektion und Bewältigung
- Business Continuity: Backup-Management, Data Recovery, Krisenmanagement
- Sicherheit der Lieferkette: Garantieren, nicht nur dokumentieren!
- Schwachstellenmanagement
- Schulung und Training: Awarness und Wissen bei Mitarbeiter
- Einsatz von Kryptographie und Verschlüsselung

Welche Aufgaben entstehen bei einer NIS2-Umsetzung?

- Personal/Human Resources Security
- Zugangskontrollen
- Asset-Management
- Supply Chain: Sicherheit in der Lieferkette & sicheren Entwicklung bei Zulieferern
- Authentifizierung: Einsatz von Multi-Factor-Authentisierung und SSO
- Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- Notfall-Kommunikation: Einsatz gesicherter Notfall-Kommunikations-Systeme

Was, wenn doch?

- Knackige Meldepflichten bei einem Ausfall einer kritischen Dienstleistung
  - Binnen 24 Stunden eine „vorläufige Meldung“
  - Binnen 72 Stunden eine „qualifizierte Meldung“
- => Aufbau von Prozessen für eine entsprechende Meldung/Meldekette.

heinlein

Die Haftung (des Geschäftsführers!)

Und was ist, wenn nicht?

- Harter Bußgeldkatalog mit existenziellen Bußgeldern möglich
  - 10 MEUR oder 2% des weltweiten Umsatzes (besonders wichtige Unternehmen)
  - 7 MEUR oder 1,4% des weltweiten Umsatzes (wichtige Unternehmen)

- DSGVO lässt grüßen

Und was ist, wenn nicht?

- Persönliche Haftung und Verantwortung der Unternehmensleitung in Art. 20
  - Hihihi… heißt auch: Sie müssen selbst an Cybersicherheitsschulungen teilzunehmen und sie nicht nur allen Mitarbeitern regelmässig anbieten.
- Wer gegen die NIS2-Vorgaben handelt, handelt i.d.R. grob fahrlässig
  - Grob fahrlässigem Handeln löst eine Haftung des Geschäftsführers aus
  - Aus seinem privaten Vermögen!
- Übrigens springt dann auch keine Management-Haftpflicht-Versicherung mehr ein..

Oooops.

heinlein

Die Supply-Chain

Die Haftung für die Supply-Chain

- NIS2 verpflichtet die Unternehmen, die Sicherheit der Lieferkette sicherzustellen
  - Sicherstellen. Nicht nur überprüfen.
  - Sicherstellen!

- Eine einfache ISO 27001 des Vorlieferers reicht nicht aus.
  - Ein IT-Risiko in der ISO 27001 kann erkannt und nach wirtschaftlichen Erwägungen auch schlichtweg akzeptiert werden.
  - Das geht für NIS2 nicht – die Sicherheit muß gewährleistet sein.

  - Unklar wäre bei einer ISO 27001 auch, was mit dem Vor-Vorlieferer oder Vor-Vor-Vorlieferer ist.

Common Criteria EAL 4+ vs ISO 27001

Selected Aspects

Common Criteria EAL 4 + Flaw Remediation	ISO 27001
– **Product specific** including organization	– Organizational, **excluding product features**
– Demanding **full control** and description over all security aspects	– Delegation possible so delegated areas are **blind spots**
– No compromise approach **transparent to the customer**	– Balancing risk with investment **unknown to customer**
– Suitable to **highest security standards**	– **Good enough security** for unknown level
– **Fully comparable**	– **Not comparable** depending on risk analysis

Die Haftung für die Supply-Chain

- Notwendig ist eine vollständige Evaluierung der Supply-Chain-Kette
  - In allen Bereichen – Quelle des Codes, Review des Codes, Paketierung und Softwarebereitstellung, Vulnerability-Management
  - Fortlaufend
  - Nach dem aktuellen Stand der Technik (der Cyber-Abwehr!)

- Eine umfassende eigene Überprüfung der eigenen IT-Vorlieferer kaum möglich
  - Wenn jetzt jedes Unternehmen jedes Unternehmen validiert… Gute Nacht.

- Das entspricht einer Zertifizierung nach nach CC-EAL4+ des BSI
  - 4+ heisst: Inkl. Vulnerability-Management
  - Vorteil: BSI ist staatlicher Akteur => kein grob fahrlässig/falsch möglich

Richtlinie zur Netz- und Informationssicherheit (NIS2)

Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21)

a) Information Security Management

b) Incident Response / Incident Management

c) Business Continuity Management

d) **Third Party Risk Management**

e) Vulnerability Management

f) Pentesting/Auditing

g) Sensitization & Training

h) Cryptography & Encryption

i) Access Management

j) Authentication Management

"Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern"

Richtlinie zur Netz- und Informationssicherheit (NIS2)

Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21)

a) Information Security Management

b) Incident Response / Incident Management

c) Business Continuity Management

d) Third Party Risk Management

e) Vulnerability Management

f) Pentesting/Auditing

g) Sensitization & Training

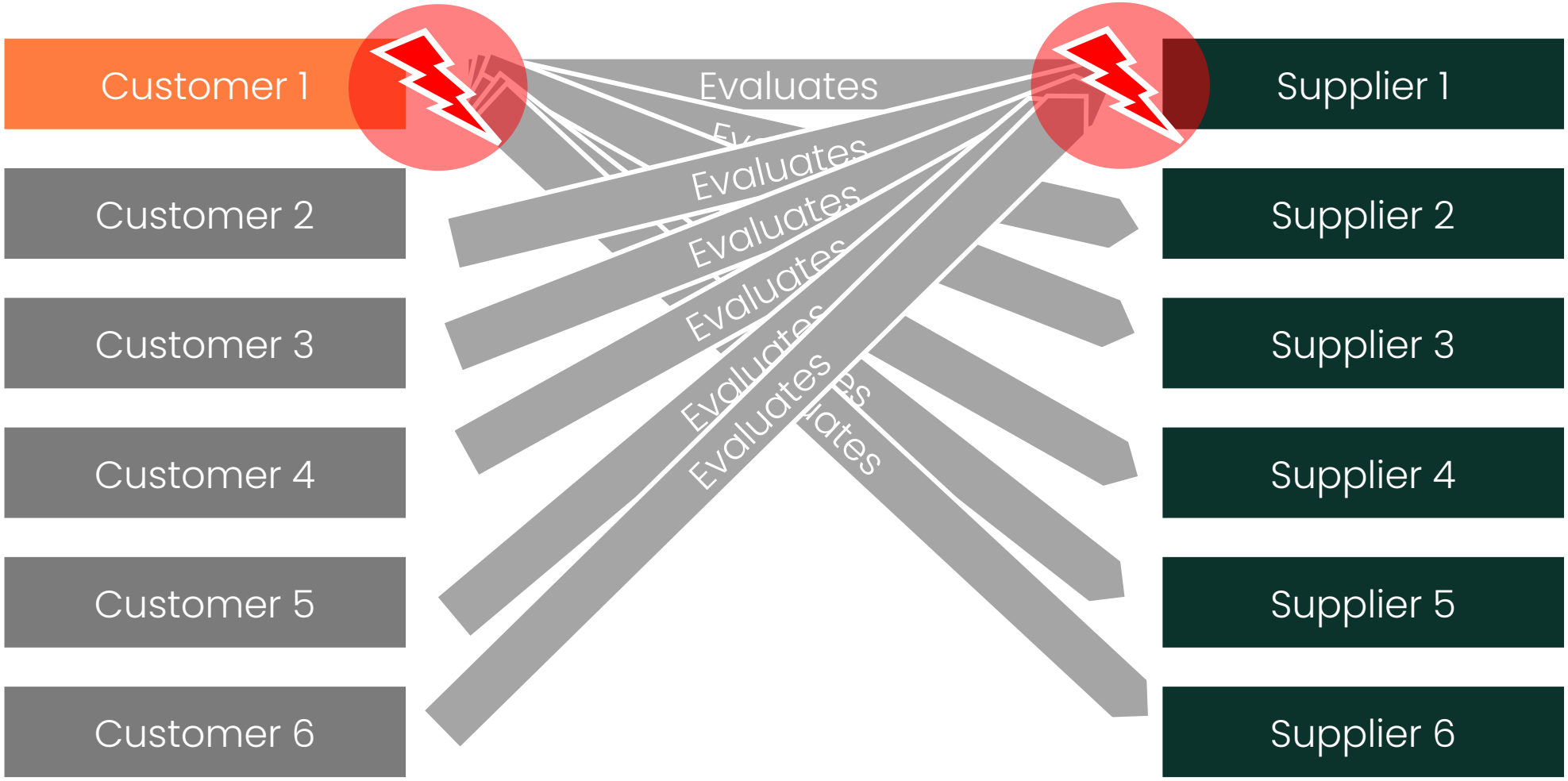
h) Cryptography & Encryption

i) Access Management

j) Authentication Management

"Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen"

Selbst ist der Mann/die Frau?



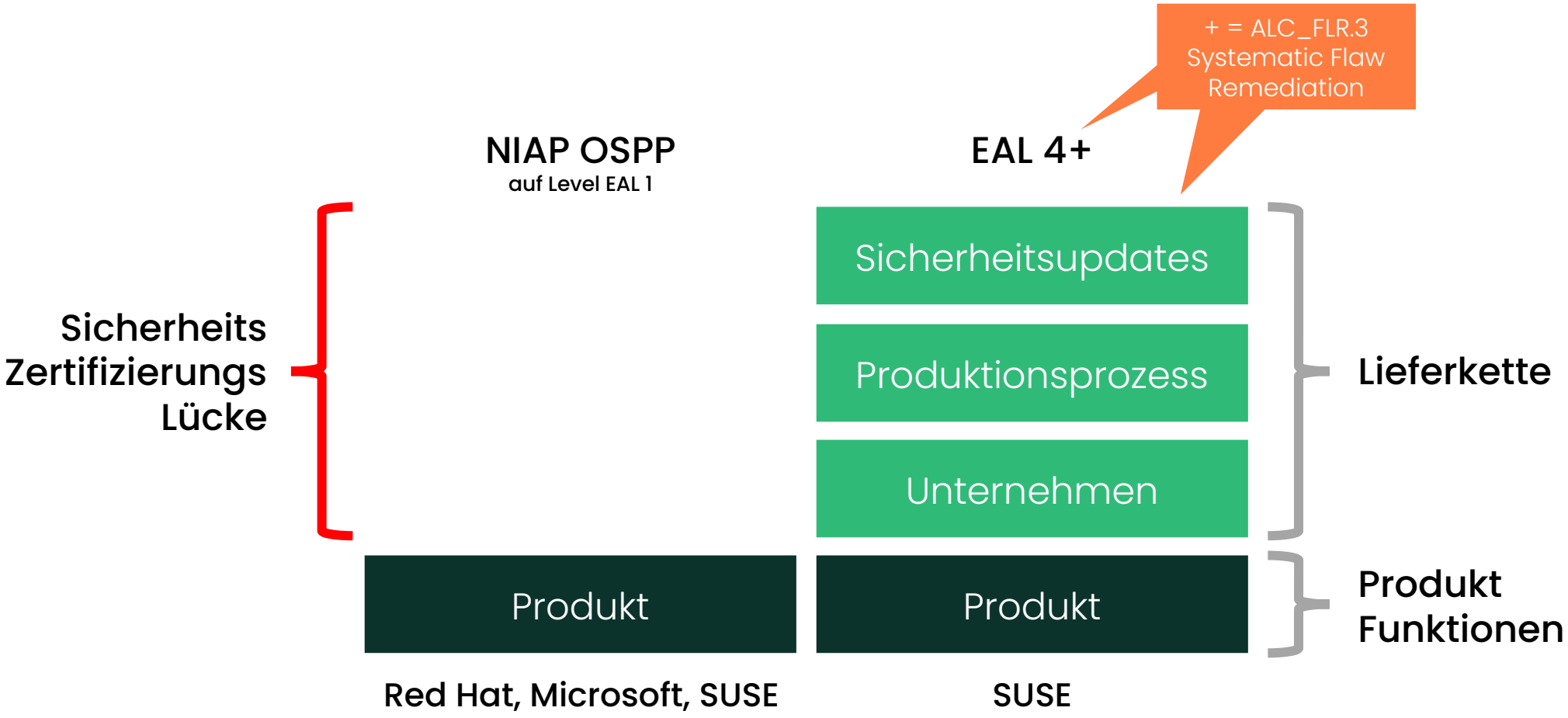
Und will ich das wirklich?

Der Mehrwert einer Zertifizierung

	Self Evaluation	Common Criteria EAL 4+ Certified Vendor
Pros	+ Full control over all Aspects	+ Full legal recognition in the EU + Cost paid by supplier (economy of scale) + Implementation immediately + Low risk due to governmental attestation + Conformity with international standards + Comparable with other entities solution + Evaluator has full access to all relevant evidence + Supplier need to limit attack surface
Cons	- Full liability - Customer has high internal effort - Customer has high cost - Customer bares high risk - Long implementation time frame - Incomplete access to suppliers' evidence - Supplier might have a high attack surface - Supply chain intransparent	- Not all suppliers available

NIAP OSPP vs. EAL 4+ Certification Scope

Warum ein reiner Produktansatz nicht mehr ausreicht



Das ganze beginnt beim Betriebssystem

- OS/Distributionen mit CC-EAL4+:
  - SUSE / SLES

- OS/Ditributionen ohne CC-EAL4+:
  - Debian
  - Ubuntu
  - RedHat/RHEL
  - Quasi alle anderen

  - Microsoft Windows

Software Bill of Material (SBOM)

Ein weiterer Ansatz für mehr Sicherheit durch Transparenz

- Model einer **“Zutatenliste”** aus der fertigenden Industrie
- **Schnelle Identifikation** von betroffenen Produkten/Systemen
- **Automatisierung** durch zwei offene, formale Standards:
  - SPDX (Linux Foundation)
  - CycloneDX (OWASP Foundation)
- **Inhaltliche** Definitionen reifen noch
  - **Erster Aufschlag** durch das BSI in der TR-03183-2

Microsoft Windows. Too big to fail?

- Windows hatte alle paar Monate einen schweren Incident in der Supply-Chain
- Da man die Sicherheit der eigenen Supply-Chain gewährleisten muss fällt es schwer nicht zu dem Schluss zu kommen, dass beim Einsatz von MS Windows ein grob fahrlässiges Handeln vorliegt.
  - Grob fahrlässiges Handeln des Managers (=> Haftung!)
- Genau um sowas geht es doch bei NIS2
- Ist es nur eine Frage der Zeit, bis die ersten sehr empfindlichen Bußgelder verhängt werden?

heinlein

Watt mutt, datt mutt.

Tja. So im Großen und Ganzen…

- Cyber-Sicherheit und Resilienz finden wir super.
  - Nun wird es eingefordert.
  - In anderen Worten: Oh. Das wird ein bisschen weh tun.
- Das BMI schätzt den Umsetzungsaufwand von NIS2 auf 1,5 Mrd. €.
  - Nur die primär betroffenen ~27.000 Unternehmen
  - Vor-Zulieferer nicht erfasst.
- Aber watt mutt, datt mutt.

heinlein

Fragen und Diskussionen

Linux höchstpersönlich.

Bleiben wir im Kontakt

Peer Heinlein

Tel. +49 30 40 50 51-42
p.heinlein@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de