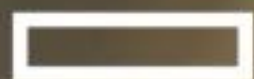


15. BECHTLE IT-FORUM THÜRINGEN

BECHTLE

2024

15. Mai 2024 • STEIGERWALD Stadion ^{Erfurt}



Hewlett Packard
Enterprise



HUAWEI

intel.

ONLY FOR CLOSED GROUP USE - Foto: Armin Frieling



Die unsexy Digital- „Streetbuilder“

ONLY FOR CLOSED GROUP USE - Foto: Armin Frieling



Wir sind die IT Forscher und Entwickler Nr.1



GLOBAL

207.000

Mitarbeiter
Weltweit

Nr. 96

der Fortune
Global 500

170+

Ländervertretungen
& Regionen

100+

Milliarden
Revenue/USD

Privat

Unternehmen



NIS 2 – KI – Up-Time-Anforderungen. Ansätze und Beispiele für mehr Sicherheit und Verfügbarkeit im IT-Betrieb

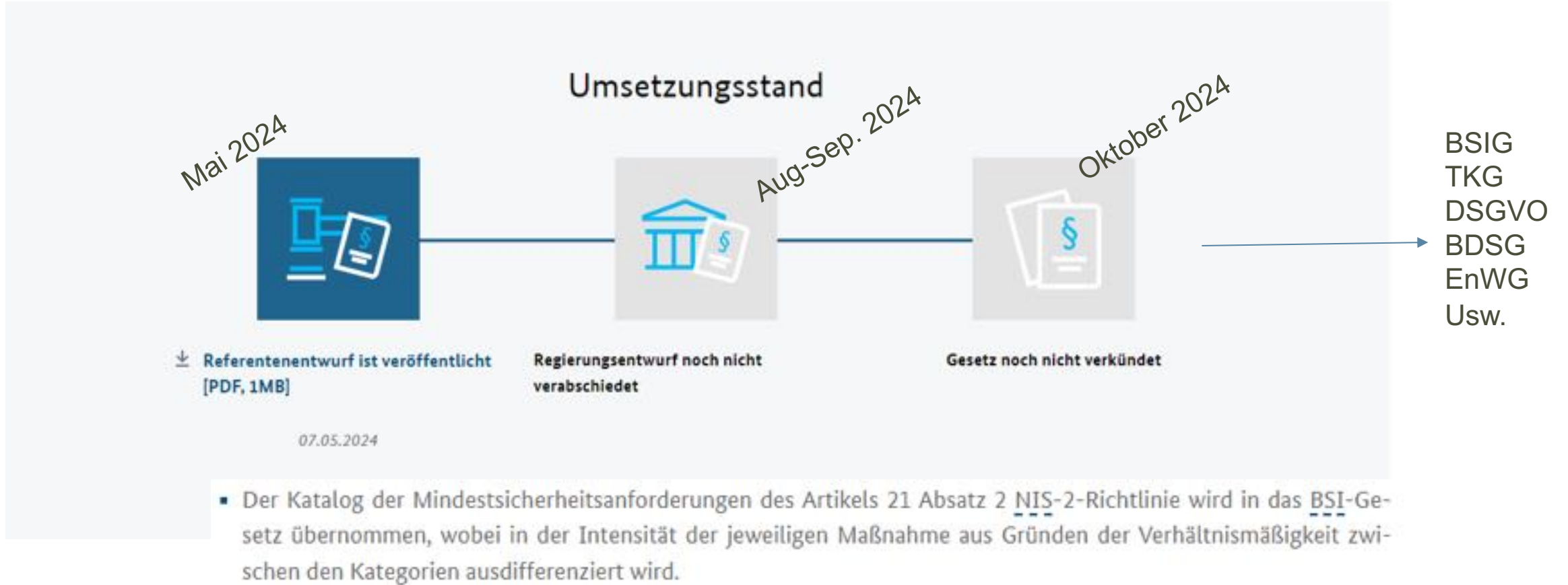
Alexios Grammatikopoulos
Huawei Technologies Deutschland GmbH

Rückblick

Rückblick



Rückblick – Aktueller Stand



Quelle: [BMI - Gesetzgebungsverfahren - Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes \(bund.de\)](https://www.bund.de)

Wie ist es aufgebaut?

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Wie ist es aufgebaut?

- KAPITEL I - ALLGEMEINE BESTIMMUNGEN
- KAPITEL II - KOORDINIERTER RAHMEN FÜR DIE CYBERSICHERHEIT
- KAPITEL III - ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE
- KAPITEL IV - RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT
- KAPITEL V - ZUSTÄNDIGKEIT UND REGISTRIERUNG
- KAPITEL VI - INFORMATIONSAUSTAUSCH
- KAPITEL VII - AUFSICHT UND DURCHSETZUNG
- KAPITEL VIII - DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE
- KAPITEL IX - SCHLUSSBESTIMMUNGEN
- ANHANG I
- ANHANG II
- ANHANG III



- Artikel 20 - Governance
- Artikel 21 - Risikomanagementmaßnahmen im Bereich der Cybersicherheit**
- Artikel 22 - Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union**
- Artikel 23 - Berichtspflichten**
- Artikel 24 - Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung
- Artikel 25 - Normung

Anwendungsbereiche

- Anwendungsbereich 1 - Sektorenzugehörigkeit
- Anwendungsbereich 2 - Größe
- Anwendungsbereich 3 - Kritikalität

Muss ich mich damit beschäftigen?

Anwendungsbereich 1 - Sektorenzugehörigkeit

Anhang 1

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitales Infrastruktur
- Verwaltung von IKT-Diensten (Business-to-Business)
- öffentliche Verwaltung
- Weltraum

Anhang 2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Muss ich mich damit beschäftigen?

Anwendungsbereich 1 - Sektorenzugehörigkeit

Anhang 1

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- **Digitales Infrastruktur**
 - **Cloud Anbieter – RZ-Anbieter**
- Verwaltung von IKT-Diensten (Business-to-Business)
- **öffentliche Verwaltung**
 - **öffentlichen Verwaltung von Zentralregierungen**
 - **öffentlichen Verwaltung auf regionaler Ebene**
- Weltraum

Anhang 2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Muss ich mich damit beschäftigen?

Anwendungsbereich 1 - Sektorenzugehörigkeit

Anhang 1

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitales Infrastruktur
- Verwaltung von IKT-Diensten (Business-to-Business)
- öffentliche Verwaltung
- Weltraum

Anhang 2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- **Forschung**
 - **Forschungseinrichtungen**

Muss ich mich damit beschäftigen?

Anwendungsbereich 2 - Größe

GROSSE UNTERNEHMEN



- Mehr als 250 Mitarbeiter
- Mehr als 50 Mio. EUR Jahresumsatz oder
- Mehr als 43 Mio. EUR Jahresbilanz

MITTEL(GROSSE) UNTERNEHMEN



- Mehr als 50 Mitarbeiter
- Mehr als 10 Mio. EUR Jahresumsatz/Bilanz

Muss ich mich damit beschäftigen?

Anwendungsbereich 3 - Kritikalität

WESENTLICHE EINRICHTUNGEN



- Nach Anhang 1
- Bereits Kritis Unternehmen
- Eingestuft durch Behörde

WICHTIGE EINRICHTUNGEN



- Nach Anhang 1 und 2
- Mittelgroße Unternehmen / Große Unternehmen
- Eingestuft durch die Behörde

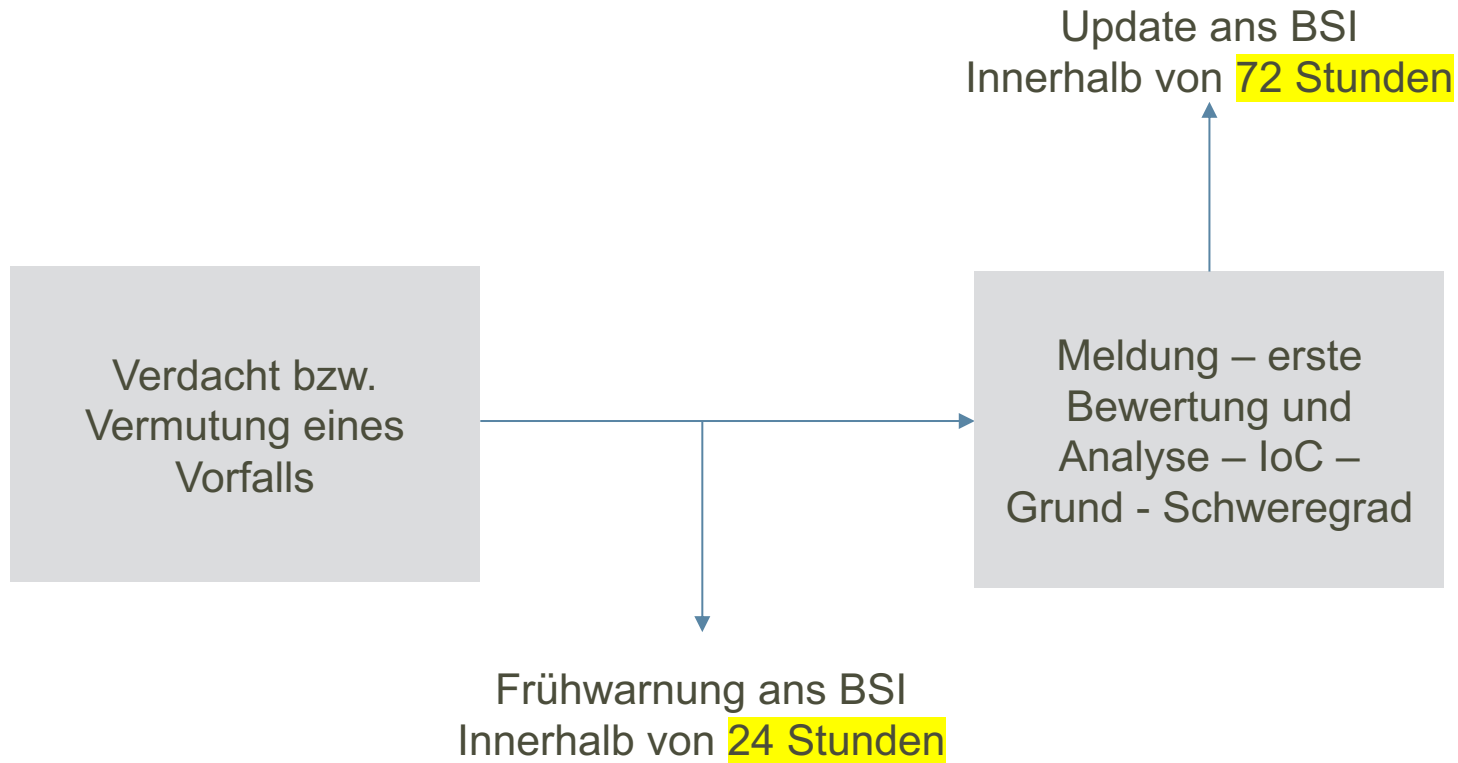
Meldepflichten

Wohin und wann melden, wenn etwas passiert?

Verdacht bzw.
Vermutung eines
Vorfalls

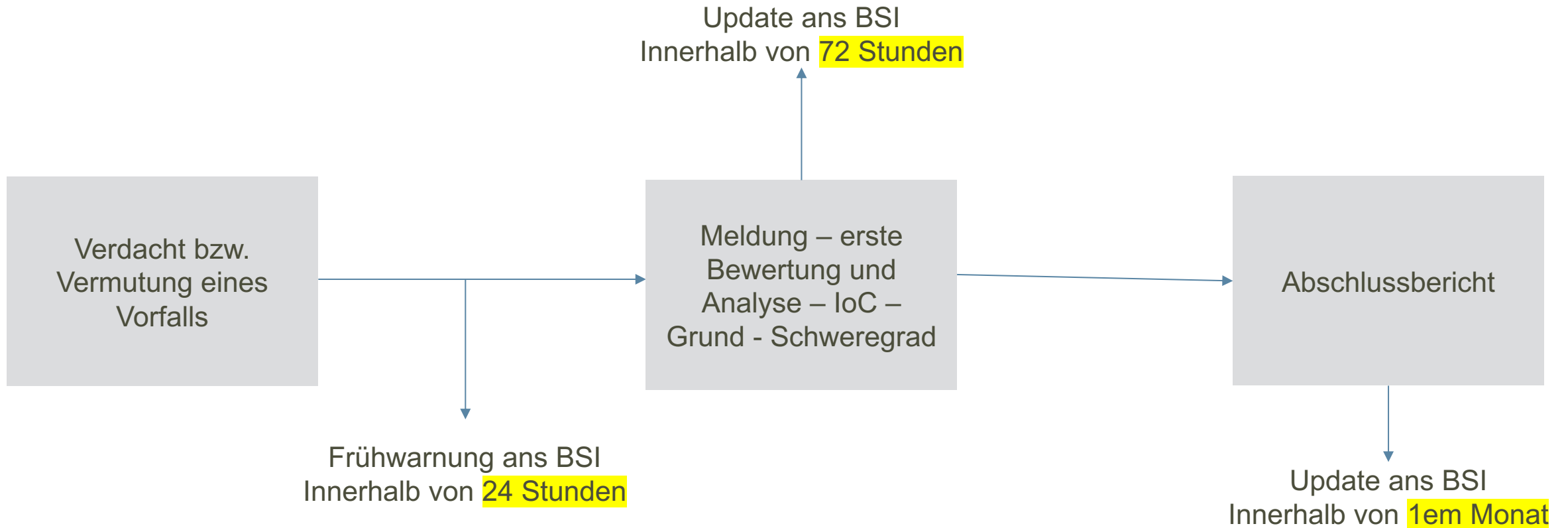
Meldepflichten

Wohin und wann melden, wenn etwas passiert?



Meldepflichten

Wohin und wann melden, wenn etwas passiert?



Konkrete Maßnahmen nach Artikel 21.

Risikoanalyse und Sicherheit für Informationssysteme

Bewältigung von Sicherheitsvorfällen

Aufrechterhaltung des Betriebs
Backup-Management und Wiederherstellung

Sicherheit der Lieferkette

Sicherheitsmaßnahmen bei Erwerb

Konzepte von Risikomanagementmaßnahmen

Cyberhygiene und Schulungen

Einsatz von Kryptografie und Verschlüsselung

Sicherheit des Personals, Konzepte für die Zugriffskontrolle und
Lösungen zur Multi-Faktor-Authentifizierung

Meldepflicht

Konkrete Maßnahmen nach Artikel 21.

Risikoanalyse und Sicherheit für Informationssysteme



Bewältigung von Sicherheitsvorfällen



Aufrechterhaltung des Betriebs
Backup-Management und
Wiederherstellung



Sicherheit der Lieferkette

Sicherheitsmaßnahmen bei Erwerb



Konzepte von Risikomanagementmaßnahmen

Cyberhygiene und Schulungen



Einsatz von Kryptografie und
Verschlüsselung



Sicherheit des Personals, Konzepte für die
Zugriffskontrolle und Lösungen zur
Multi-Faktor-Authentifizierung



Meldepficht

Konkrete Maßnahmen nach Artikel 21.

Sicherheit der Lieferkette

Konzepte von
Risikomanagementmaßnahmen

Einsatz von Kryptografie
und Verschlüsselung

Meldepflicht

Security WorkShop - Beratungsunternehmen

Einführung eines ISMS - Systems

Implementierung eines SOC's – intern oder extern

Incident Response - Notfallhandbuch

Die Core Strategie Elemente in Deutschland

Architektur

(Nachhaltig & flexibel)

KI (L4)

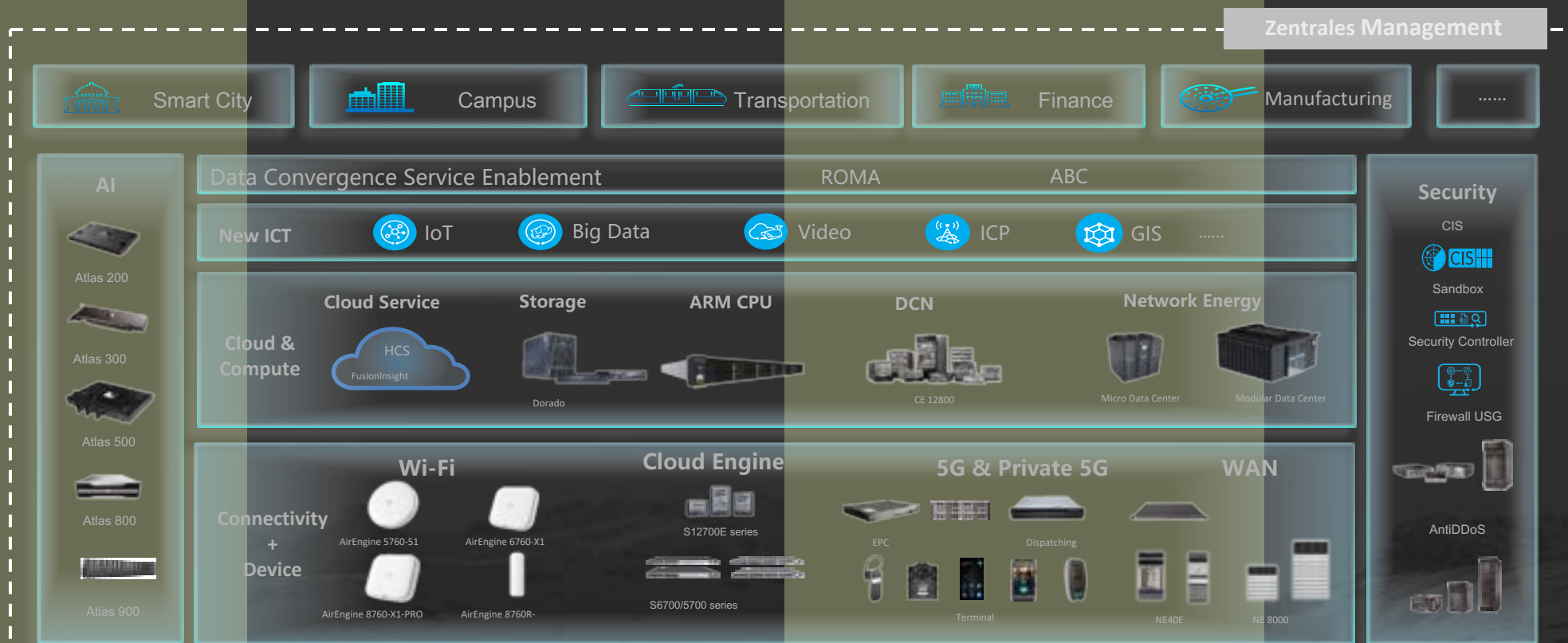
(Mehr Aufgaben & Weniger Menschen)

Energie


(Kosten & Verantwortung)

Cloud(like)

(Zentrale Steuerung & Sourcing & Betrieb)

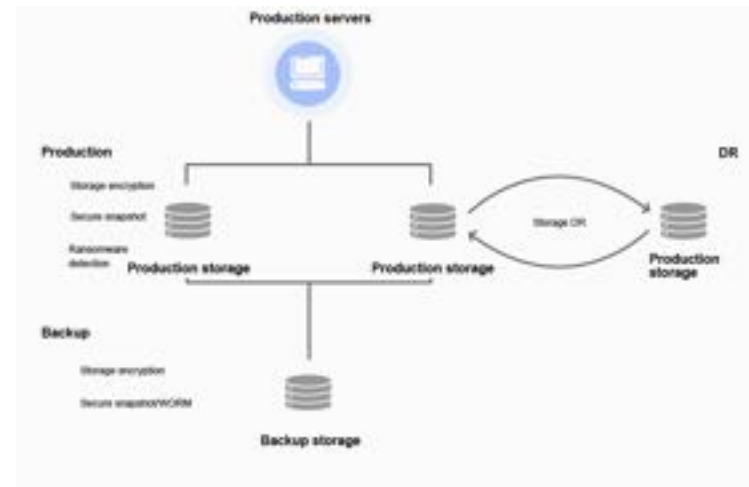
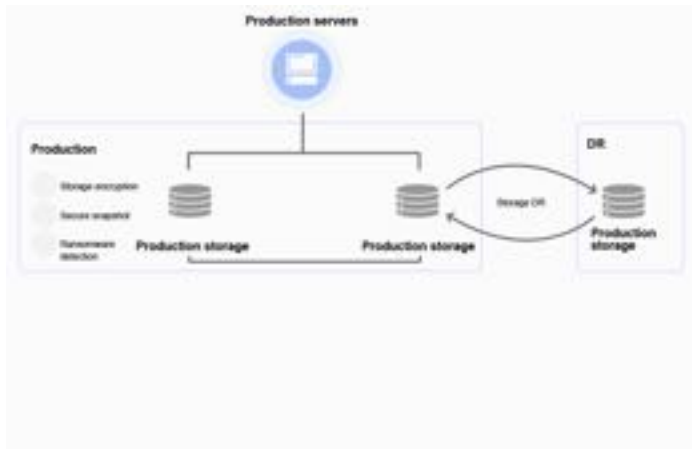


Womit können wir helfen?

Risikoanalyse und Sicherheit für Informationssysteme 

Bewältigung von Sicherheitsvorfällen 

Dual Ransomware Protection

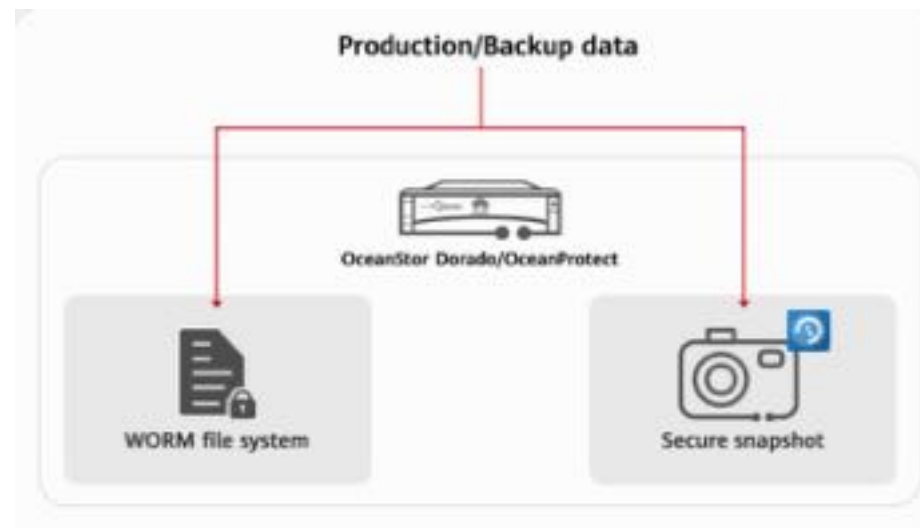


Womit können wir helfen?

Aufrechterhaltung des Betriebs
Backup-Management und
Wiederherstellung



File System WORM and Secure Snapshot



Womit können wir helfen?

Sicherheitsmaßnahmen bei Erwerb





Zurverfügungstellung von
Zertifizierungen

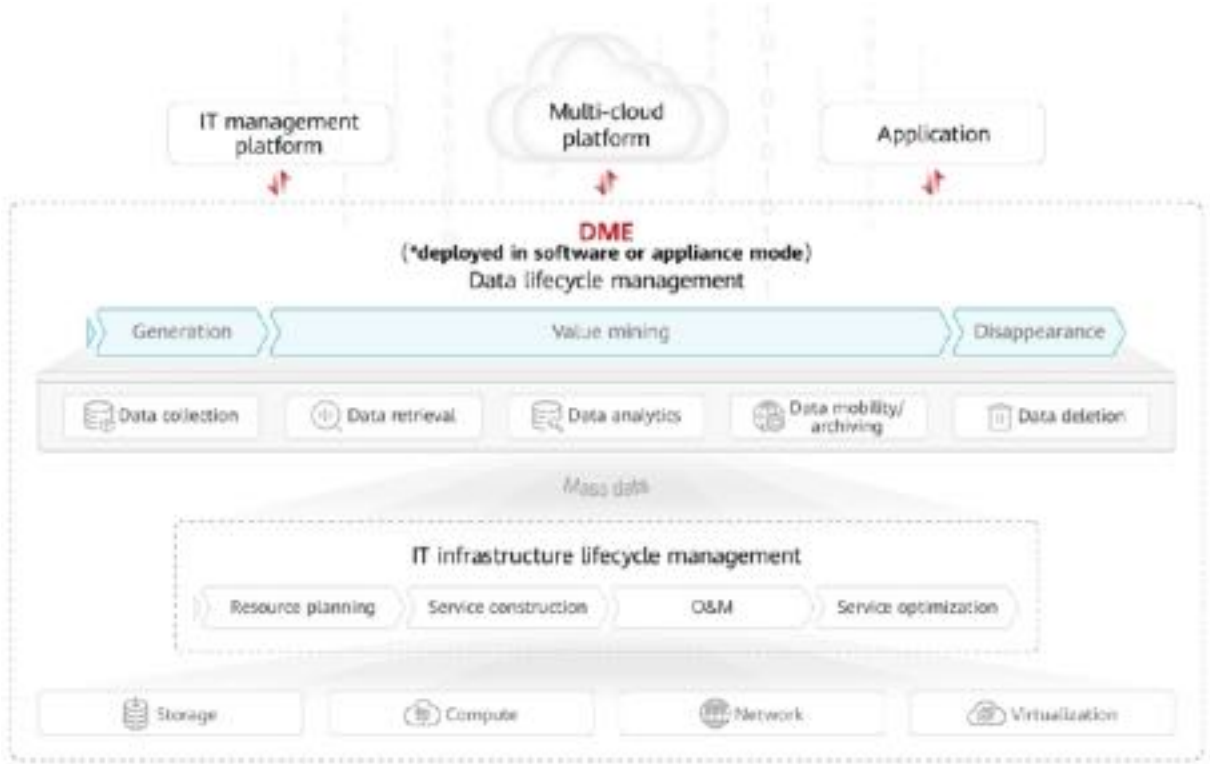
Erwerb von neuen Zertifizierungen

No-Back-Door Agreements

Womit können wir helfen?

Cyberhygiene und Schulungen 

Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Lösungen zur Multi-Faktor-Authentifizierung 



Vielen Dank!

Besuchen Sie uns am Stand!

Alexios Grammatikopoulos

