NIS2 bringt die CyberSicherheits-Anforderungen der kritischen Infrastruktur in den Mittelstand

Teil 2 von 4: Die Hintergründe (persönliche Einschätzung)

1. Das BSI bekommt deutliche mehr Macht!
2. Was könnten die Gründe sein? (persönliche Einschätzung)
3. Gibt es Ansätze/Blaupausen, was auf den Mittelstand zukommen könnte?

Christian Kreß

Externer ISB und
CyberSecurity Coach

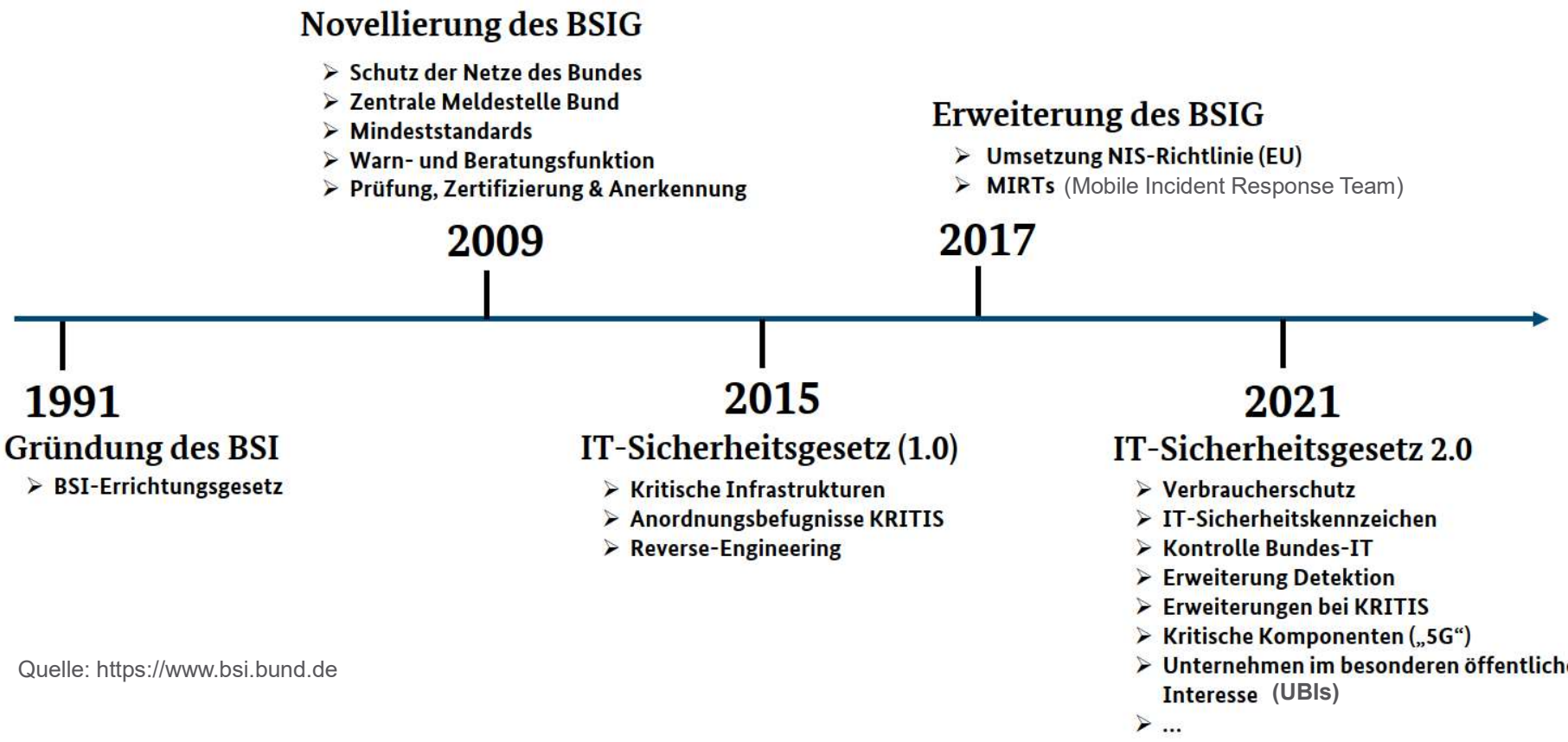
INOVASEC GmbH
Christian Kreß
In den Obergärten 28
63329 Egelsbach

E-Mail: christian.kress@inovasec.de
Tel: +49 6103 8038055
Mobil: +49 1520 9276920
Web: www.inovasec.de

NIS2 ist ein Kooperations- und Kommunikationsprojekt

Das BSI bekommt deutliche mehr Macht!

KRITIS und die Entwicklung des BSI-Gesetzes



Quelle: https://www.bsi.bund.de

Begründung aus dem „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG)

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen. Dies haben insbesondere Sachstandserhebungen zum Umsetzungsplan Bund sowie Prüfungen des BRH bestätigt. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden.

Quelle: NIS2UmsuCG

§ 57 Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern und für Heimat **bestimmt durch Rechtsverordnung**, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber, Einrichtungen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Oder kürzer: „BMI/BSI haben das Recht, das Gesetz nach Bedarf anzupassen“

…

3. welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Siedlungsabfallentsorgung, Logistik, Produktion, Chemie, Ernährung, **verarbeitendes Gewerbe**, Anbieter digitaler Dienste oder Forschung Einrichtungsarten wichtiger Einrichtungen sind.

Oder kürzer: „BMI/BSI konkretisieren im Rahmen des EU-Gesetzes, welche Unternehmen betroffen sind.“

Der Staat meint es diesmal wirklich ernst: BSI kann strafen und direkt eingreifen

heise online

19.07.2023 21:33 Uhr

IT-Sicherheit: BSI soll CEOs entmachten dürfen

Das Umsetzungsgesetz zur NIS2-Richtlinie soll dem Bundesamt für Sicherheit in der Informationstechnik Durchgriffsrechte sogar in privaten Firmen geben.

(Bild: Superstar/Shutterstock.com)

Quelle:
https://www.heise.de/news/Bundesamt-fuer-Sicherheit-in-der-Informationstechnik-soll-CEOs-entmachten-koennen-9221469.html

Was könnten die Gründe sein? (persönliche Einschätzung)

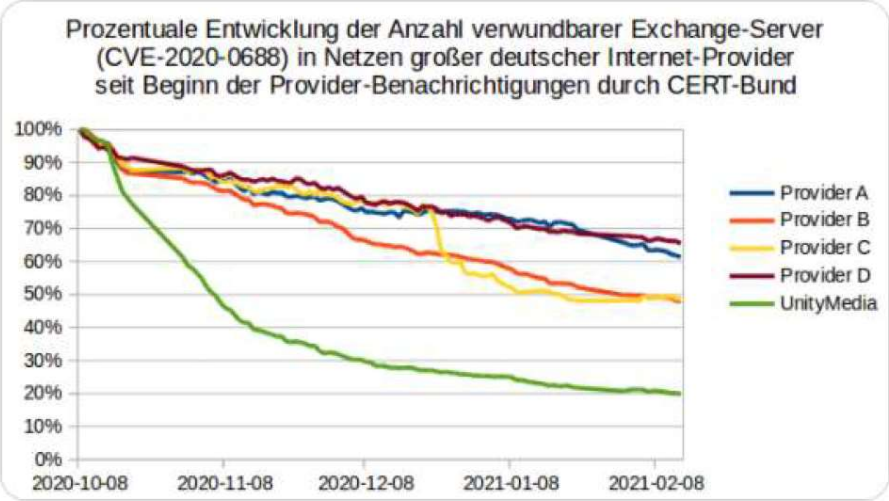
Die nächsten Seiten beschreiben nur meine ganz persönliche Sicht!

Ziel: Bewältigung von Sicherheitsvorfällen
Praxis: Verwundbarer Exchange Server

CERT-Bund @certbund

Antwort an @certbund

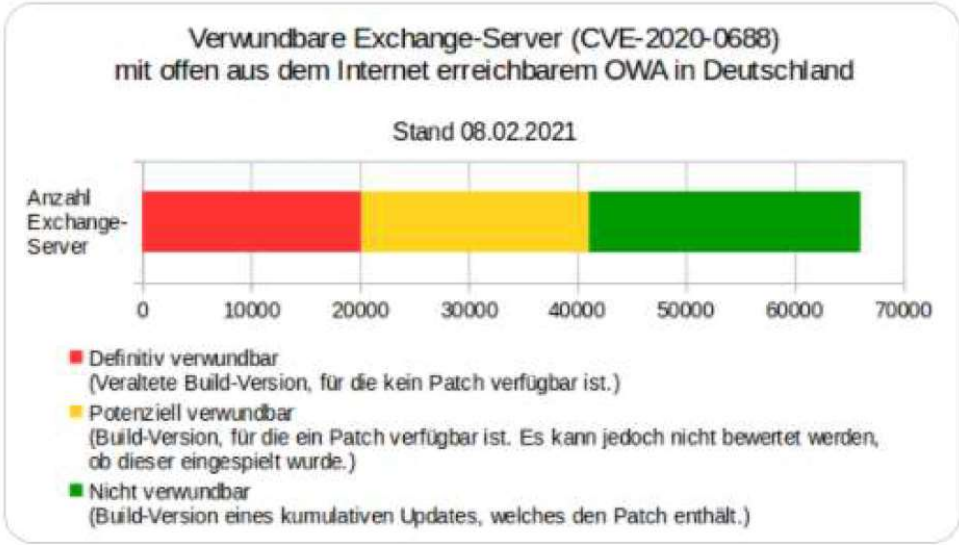
An dieser Stelle ein großer Dank an das Customer-Security-Team von UnityMedia, das es mit der schnellen Benachrichtigung betroffener Kunden auch hier geschafft hat, die Anzahl verwundbarer Systeme in relativ kurzer Zeit auf die typischen 20% "Bodensatz" zu reduzieren. 👏



4:43 nachm. · 19. Feb. 2021 · Twitter Web App

CERT-Bund @certbund · 9. Feb.

Ein Jahr nach Veröffentlichung des #Sicherheitsupdates sind noch immer mindestens 31% (potenziell bis zu 63%) der #Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem #OWA für die kritische #Schwachstelle CVE-2020-0688 verwundbar.



6 47 42

Deutschlands staatliche Cybersicherheitsarchitektur

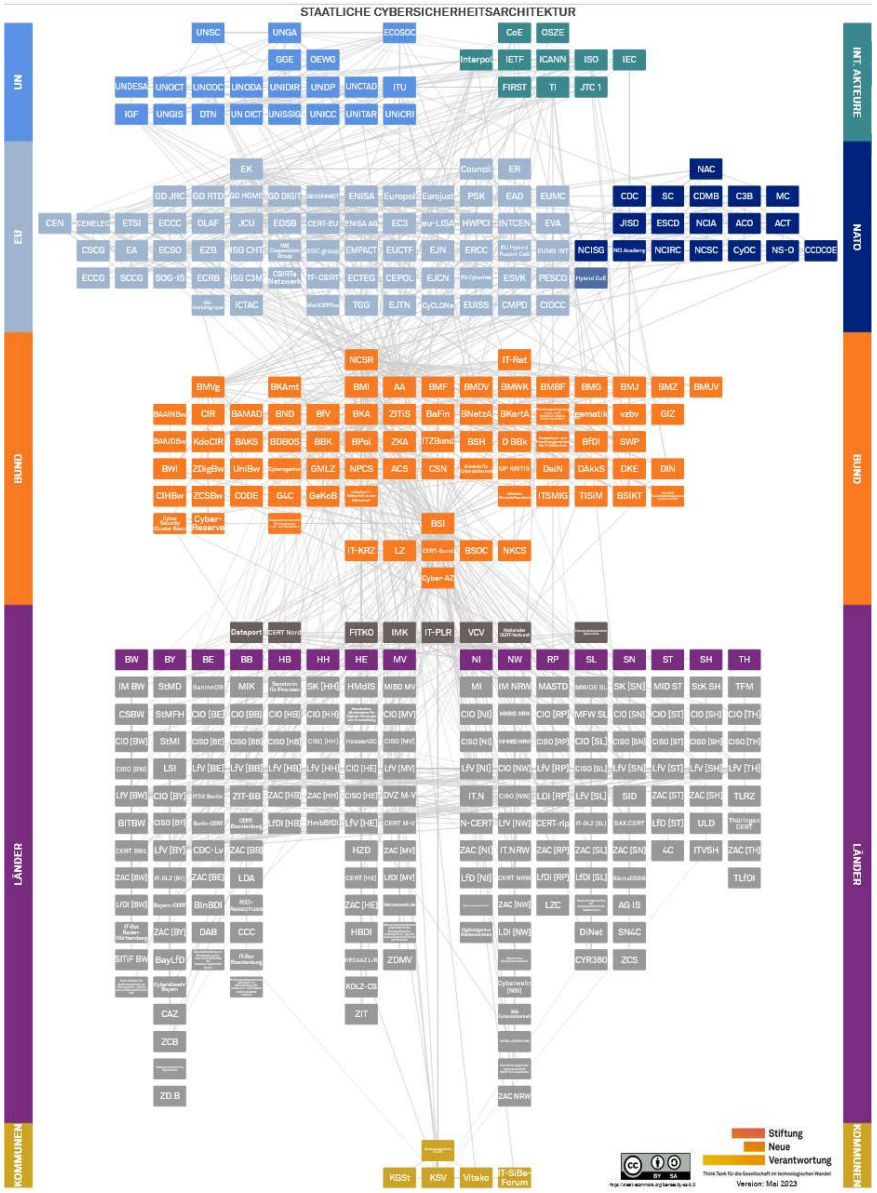
UN

EU

Bund

Länder

Kommunen



Internationale Akteure

Nato

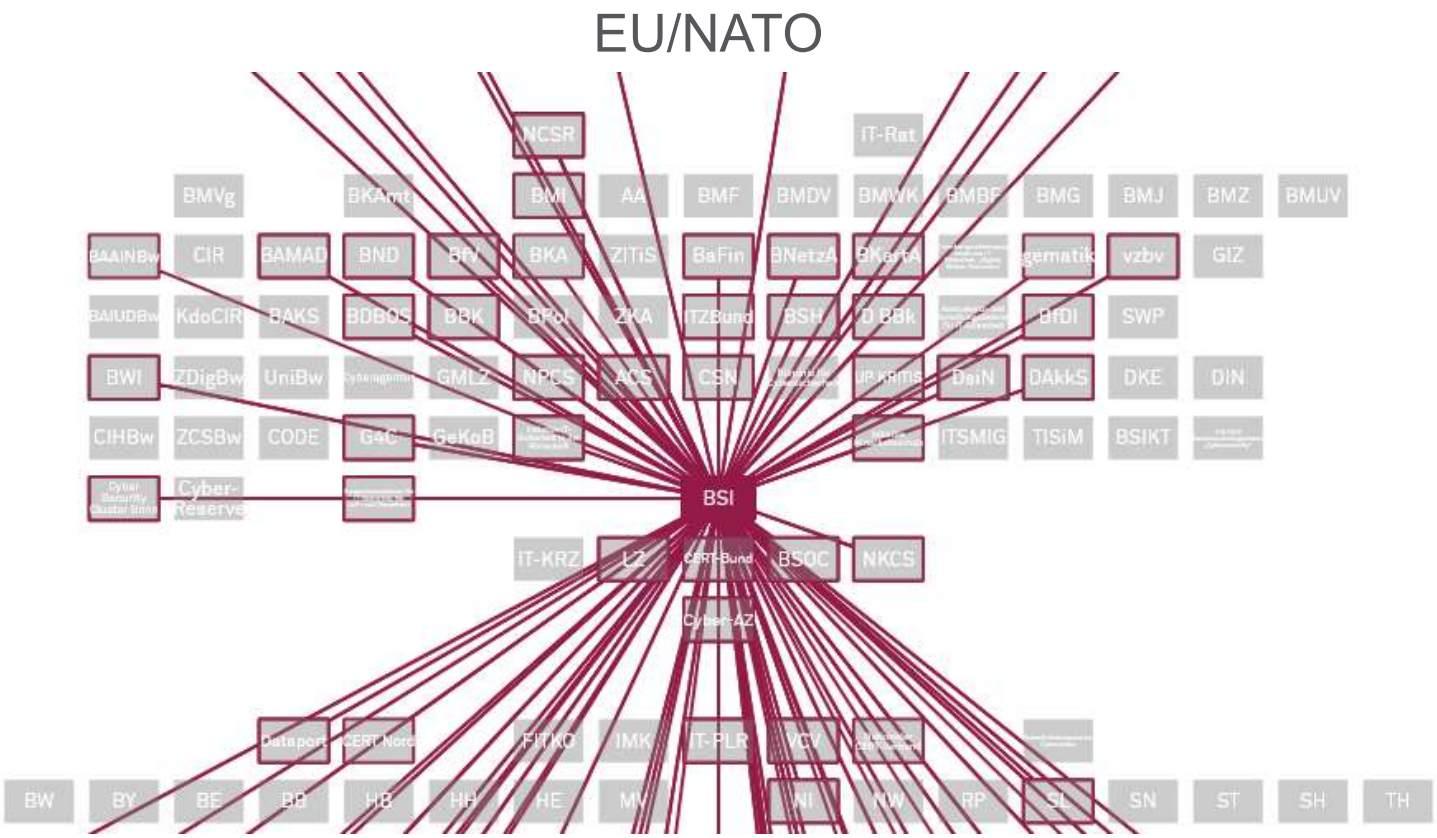
Bund

Länder

Kommunen

Quelle: https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

Deutschlands staatliche Cybersicherheitsarchitektur



Quelle: https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

Grundgesetzänderung zur Cybersecurity???

Innenministerin Faeser will Grundgesetzänderung zur Cybersecurity

Seit dem Einmarsch Russlands in die Ukraine steigt die Gefahr der Cyberangriffe auf Deutschland. Die Innenministerin will die Schutzmaßnahmen ausbauen.

Handelsblatt 02.04.2022 - 11:37 Uhr

Die Bundesministerin für Inneres und Heimat spricht im Deutschen Bundestag

Nancy Faeser (SPD) will für mehr Cybersicherheit in Deutschland sorgen.
(Foto: dpa)

ZEIT ONLINE

Nancy Faeser will für Cybersicherheit Grundgesetz ändern

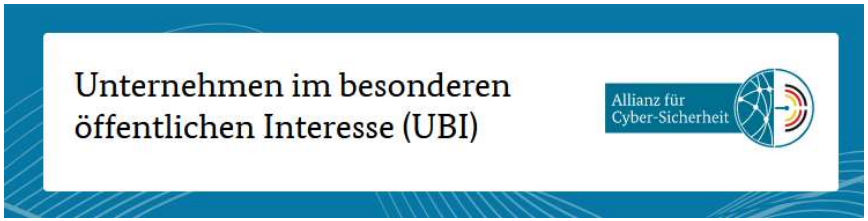
Die Bundesinnenministerin sieht eine hohe Gefahr durch russische IT-Angriffe. Um gegenzusteuern, will sie die Verfassung ändern und den Behörden Hackbacks erlauben.

3. April 2023, 2:06 Uhr / Quelle: ZEIT ONLINE

Sie können helfen, dass es nicht so weit kommt!

Gibt es Ansätze/Blaupausen, was auf den Mittelstand zukommen könnte?

Möglicherweise ja!



Mit dem IT-Sicherheitsgesetz 2.0. werden seit 2021 Unternehmen im besonderen öffentlichen Interesse (**UBI**), die jedoch nicht unter die KRITIS-Verordnung fallen, erfasst. Ihnen kommen mit diesem Status besondere Rechte und Pflichten zu.

IT-Sicherheitsgesetz 2.0, § 8f (Mai 2021)
… eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen, aus der hervorgeht,

1. welche **Zertifizierungen im Bereich der IT-Sicherheit** in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,

2. welche **sonstigen Sicherheitsaudits** oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder

3. wie sichergestellt wird, dass die für das Unternehmen **besonders schützenswerten informationstechnischen Systeme**, Komponenten und Prozesse angemessen geschützt werden, und ob dabei der **Stand der Technik** eingehalten wird.

Auszüge aus den UBI FAQ

Ist es sinnvoll, schon vor Ablauf der Fristen ein ISMS zu etablieren? —

Ja, unabhängig von gesetzlichen Vorgaben ist die Implementierung eines ISMS empfehlenswert.

Wird eine Umsetzung der ISO 27001 empfohlen für die Erfüllung der Anforderungen an UBI? —

Der Einsatz eines ISMS wird unabhängig von den gesetzlichen Anforderungen dringend empfohlen. Als BSI empfehlen wir hierfür den IT-Grundschutz. Alternativ kann aber auch nach der ISO 27000er-Reihe vorgegangen werden.

Wie erfahren potentielle UBI, dass sie sich registrieren müssen? —

Unternehmen sind verpflichtet selbst zu prüfen, ob sie die Kriterien erfüllen und UBI sind. Informationsveranstaltungen und die FAQ des BSI dienen der Bekanntmachung und Beantwortung von Fragen.

Gibt es ein zentrales Register, um zu erfahren, welche Unternehmen unter die UBI-Regulierung fallen? —

Es gibt kein öffentliches Register zu UBI.

Quelle: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/FAQ/ubi_allgemein/faq_ubi_allgemein_node.html

Aktuell existiert für den Mittelstand nur ein einziger sicher Weg: Sich zeitnah beim BSI registrieren und die Reaktion abwarten!

Forderung: UBIs werden überführt/abgelöst

Wie von diversen Verbänden in der jüngsten Vergangenheit gefordert, soll die Unterscheidung zwischen den Kategorien von Unternehmen im besonderen öffentlichen Interesse (UBI-Kategorien 1, 2 und 3), wie sie im IT-SiG 2.0 implementiert sind, im Zuge der Umsetzung der NIS-2-Richtlinie in Deutschland nicht mehr geführt werden. **UBI sind bereits größtenteils in den betroffenen wesentlichen bzw. besonders wichtigen und wichtigen Einrichtungen enthalten**.

Quelle:
Wirtschaftsrat der CDU e.V.

Umsetzung der
NIS-2-Richtlinie in Deutschland
Stand 21.06.2023

NIS2 ist ein Kooperations- und Kommunikationsprojekt

- **Teil 1 von 4: Die Grundlagen** 
- **Teil 2 von 4: Hintergründe (persönliche Einschätzung)** 
- Teil 3 von 4: Die allgemeine Lösung für NIS2
- Teil 4 von 4: Eine konkrete Lösung für den Mittelstand