NIS 2 RICHTLINIE NISG-2024

02. Oktober 2024

Mario Neubauer
Stefan Ziman

BDO

IHRE VORTRAGENDEN

IHRE VORTRAGENDEN

Mario Neubauer
Senior Manager

+43 664 60 375 - 4253
mario.neubauer@bdo.at

Stefan Ziman
Consultant

+43 664 60 375 - 1687
stefan.ziman@bdo.at

INHALT

WER WIR SIND

BDO AUSTRIA

Großartiges Unternehmertum verdient besondere Aufmerksamkeit!

Nur wer zuhört und versteht, kann Sie auch umfassend betreuen. Darum ist BDO Ihr verlässlicher Wegbegleiter. Zusammen stellen wir die Weichen für Ihr Projekt und finden passende Lösungen – damit Sie sicher ins Ziel kommen.

Für Ihre Strategie setzen wir alle Hebel in Bewegung: Je nach Aufgabenstellung stellen wir das optimale Team für Sie zusammen.

Das macht uns zu BDO.
Und uns gemeinsam great.

OFFICES

WIEN, GRAZ, LINZ, SALZBURG, KLAGENFURT, LUSTENAU, JUDENBURG, WOLFSBERG, EISENSTADT, BRUCK/LEITHA, OBERWART, SCHWAZ

SERVICE LINES

ACCOUNTING, ASSURANCE,CONSULTING, CORPORATE FINANCE, PEOPLE & ORGANISATION, TAX

KUND:INNEN
13.300+

MITARBEITER:INNEN
1.100+

PARTNER:INNEN
65+

STANDORTE
in ganz Österreich

UMSATZ 2022/23
EUR 134,3 MIO.

GRÜNDUNG
1976

Stand: Dezember 2023

WER WIR SIND

BDO INTERNATIONAL

Sie möchten Ihr Potenzial auch international ausschöpfen?

Wenn Sie Ihr Weg auf der Suche nach Greatness in die unterschiedlichsten Länder führt, sind Sie mit uns ideal unterwegs. Das BDO Netzwerk heißt Sie weltweit willkommen und begleitet Sie über alle Ländergrenzen hinweg zum Ziel.

Wir sehen Ihren großartigen Plänen mit Freude entgegen!

NETZWERK

Die BDO Gruppe Österreich ist Teil des weltweit tätigen BDO Netzwerks von Wirtschaftsprüfer:innen, Steuer- und Unternehmensberater:innen.

MITARBEITER:INNEN	LÄNDER	BÜROS	GRÜNDUNG	UMSATZ 2022/23
115.000+	160+	1.700	1963	USD 14 MRD.

Stand: Dezember 2023

Accounting

Konzentrieren Sie sich auf Ihre Kernkompetenzen. Die Abwicklung Ihrer Finanzprozesse ist bei uns in guten Händen und liefert die Basis für Ihre unternehmerischen Entscheidungen.

Assurance

Vertrauen und Mehrwert sind die Basis unserer Zusammenarbeit. Im Fokus stehen dabei stets persönliche Betreuung sowie höchste internationale Prüfungs- und Qualitätsstandards.

Consulting

Bringen Sie Ihr Unternehmen nachhaltig in Topform! Ein versiertes Team sorgt mit einer breiten Palette an Tools und Know-how für individuelle und innovative Lösungen.

Corporate Finance

Fundierte Grundlagen stellen die Basis unternehmerischer Entscheidungen dar. Mit dem richtigen Partner stellen Sie Ihr Unternehmen für die Zukunft optimal auf.

People & Organisation

Der Mensch ist der entscheidende Erfolgsfaktor eines jeden Unternehmens. Vertrauen Sie in einer Welt des Arbeitsumbruchs auf einen starken Wegbegleiter.

Tax

Sie möchten auf dem Markt erfolgreich sein? Mit einem zukunftsorientierten Partner an Ihrer Seite stehen Ihrem Erfolg die Türen offen.

EINE RUNDE SACHE

UNSERE EXPERTISE FÜR IHR UNTERNEHMEN

WARUM BRAUCHT ES NIS 2?

NIS2 legt Maßnahmen fest, mit welchen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

DI Walter Stephan (CEO) aus dem Vorstand der FACC AG mit sofortiger Wirkung abberufen

Der Aufsichtsrat hat in seiner Sitzung vom 24. Mai 2016 Herrn DI Walter Stephan als Vorsitzenden des Vorstandes der FACC AG mit sofortiger Wirkung aus wichtigem Grund abberufen. Der Aufsichtsrat ist zum Schluss gekommen, dass Herr DI Walter Stephan seine Pflichten schwerwiegend verletzt hat, insbesondere im Zusammenhang mit dem "Fake President" Vorfall.

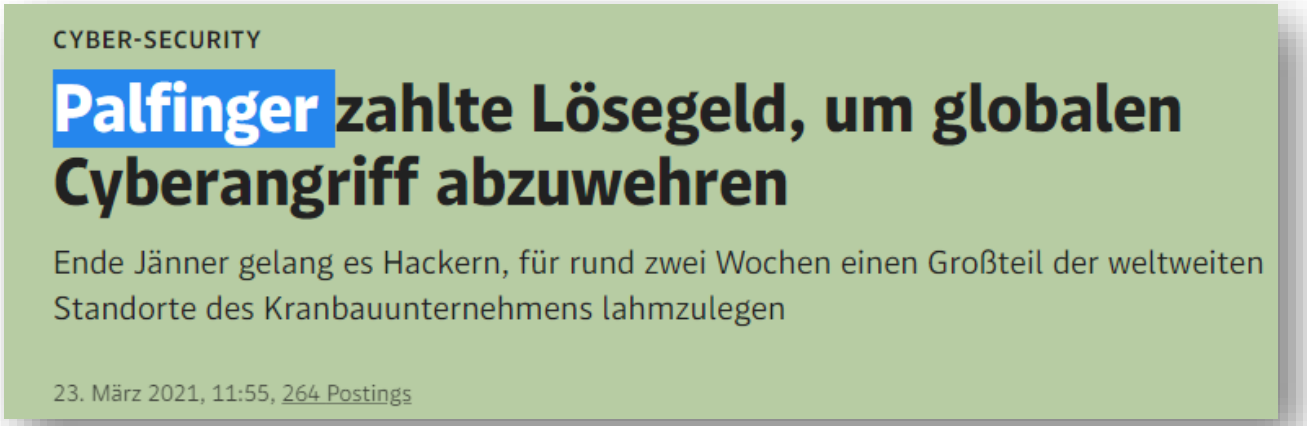
Hr. Robert Machtlinger wurde vorübergehend als CEO der FACC AG bestellt.

25/05/2016 | Ad-Hoc

*FACC war Anfang 2016 Opfer eines "Fake President Fraud" geworden. Betrüger hatten sich gegenüber der Buchhaltung des Unternehmens als Firmenchefs ausgegeben und in mehr als 92 "streng vertraulichen" Mails die Überweisung von **54 Millionen Euro** auf ausländische Konten gefordert. Die Buchhaltung kam der vermeintlichen Weisung des Vorstands nach.*

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft



CYBER-SECURITY

Palfinger zahlte Lösegeld, um globalen Cyberangriff abzuwehren

Ende Jänner gelang es Hackern, für rund zwei Wochen einen Großteil der weltweiten Standorte des Kranbauunternehmens lahmzulegen

23. März 2021, 11:55, 264 Postings

*Nachdem Hacker einen Großteil der **weltweiten Standorte für rund zwei Wochen lahmlegten**, habe sich das Salzburger Unternehmen dazu entschieden, ein Lösegeld zu zahlen*

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

Institute of Science and Technology Austria (ISTA) ist Opfer einer zielgerichteten Cyberattacke

Am 2. November 2022 sah sich das Institut dazu gezwungen, alle für den Betrieb des Instituts verfügbaren Server inklusive der Mailserver offline zu nehmen.

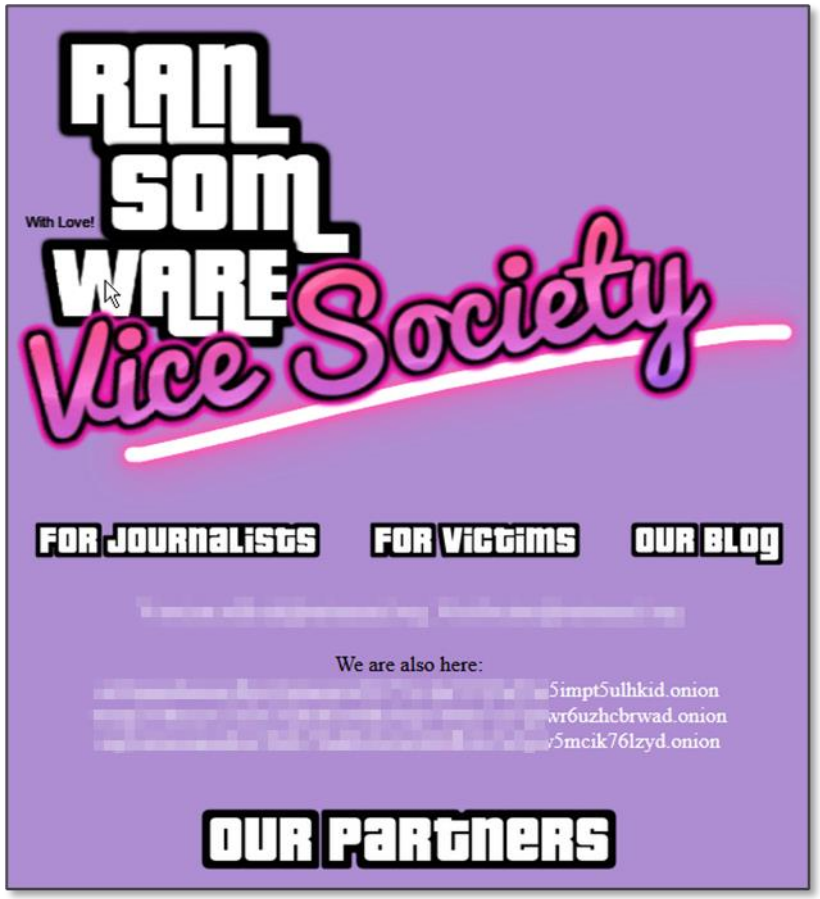
Bereits seit mehreren Tagen hatte die IT-Abteilung des Instituts vermehrte Cyberangriffe festgestellt, die zunächst abgewehrt werden konnten. Nachdem sich die Attacken jedoch intensivierten, wurde die gesamte Forschungseinrichtung aus Sicherheitsgründen vom Netz genommen.

Das ISTA arbeitet derzeit mit externer Unterstützung daran, alle technischen und rechtlichen Maßnahmen zu setzen, um die Folgen der Attacke zu beseitigen und so gering wie möglich zu halten. Einzelheiten über das Ausmaß der Attacke werden momentan untersucht.

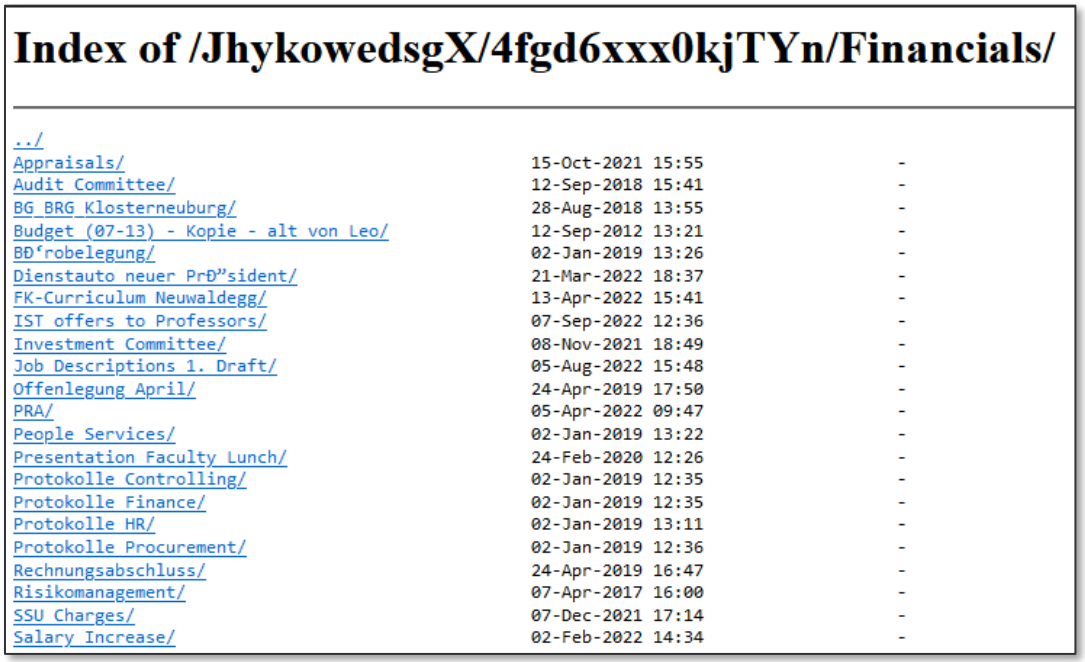
Das Institute of Science and Technology Austria wurde am 2. November 2022 Angriff eines Cyberangriffs und musste dadurch die gesamte Forschungseinrichtung vom Netz nehmen.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft



*Quelle: Onion Service

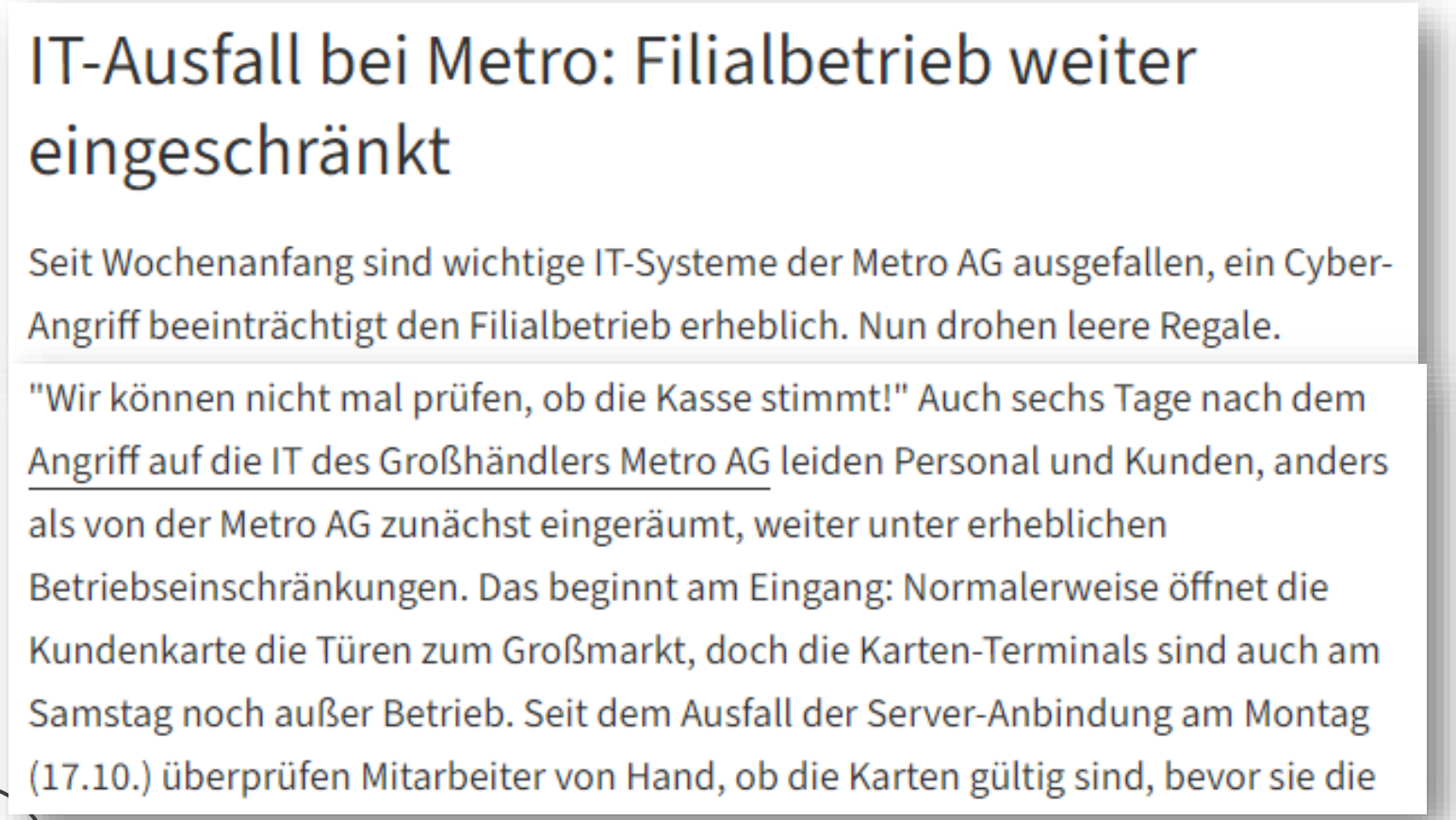


Index of /JhykowedsgX/4fgd6xxx0kjTYn/Financials/

../		
Appraisals/	15-Oct-2021 15:55	-
Audit Committee/	12-Sep-2018 15:41	-
BG BRG Klosterneuburg/	28-Aug-2018 13:55	-
Budget (07-13) - Kopie - alt von Leo/	12-Sep-2012 13:21	-
BĐ‘robelegung/	02-Jan-2019 13:26	-
Dienstauto neuer PrĐ”sident/	21-Mar-2022 18:37	-
FK-Curriculum Neuwaldegg/	13-Apr-2022 15:41	-
IST offers to Professors/	07-Sep-2022 12:36	-
Investment Committee/	08-Nov-2021 18:49	-
Job Descriptions 1. Draft/	05-Aug-2022 15:48	-
Offenlegung April/	24-Apr-2019 17:50	-
PRA/	05-Apr-2022 09:47	-
People Services/	02-Jan-2019 13:22	-
Presentation Faculty Lunch/	24-Feb-2020 12:26	-
Protokolle Controlling/	02-Jan-2019 12:35	-
Protokolle Finance/	02-Jan-2019 12:35	-
Protokolle HR/	02-Jan-2019 13:11	-
Protokolle Procurement/	02-Jan-2019 12:36	-
Rechnungsabschluss/	24-Apr-2019 16:47	-
Risikomanagement/	07-Apr-2017 16:00	-
SSU Charges/	07-Dec-2021 17:14	-
Salary Increase/	02-Feb-2022 14:34	-

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft



IT-Ausfall bei Metro: Filialbetrieb weiter eingeschränkt

Seit Wochenanfang sind wichtige IT-Systeme der Metro AG ausgefallen, ein Cyber-Angriff beeinträchtigt den Filialbetrieb erheblich. Nun drohen leere Regale.

"Wir können nicht mal prüfen, ob die Kasse stimmt!" Auch sechs Tage nach dem Angriff auf die IT des Großhändlers Metro AG leiden Personal und Kunden, anders als von der Metro AG zunächst eingeräumt, weiter unter erheblichen Betriebseinschränkungen. Das beginnt am Eingang: Normalerweise öffnet die Kundenkarte die Türen zum Großmarkt, doch die Karten-Terminals sind auch am Samstag noch außer Betrieb. Seit dem Ausfall der Server-Anbindung am Montag (17.10.) überprüfen Mitarbeiter von Hand, ob die Karten gültig sind, bevor sie die

Der Metro-Konzern wurde am 17. Oktober 2022 Opfer eines Cyberangriffs, was zu massiven Einschränkungen des Geschäftsbetriebs führte.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

NETZPOLITIK

Cyberangriff auf Feuerwehrausrüster Rosenbauer

Ausmaß und Dauer des Angriffs derzeit noch nicht abschätzbar

24. Februar 2023, 12:52, 26 Postings

Der Feuerwehrausrüster Rosenbauer wurde gehackt

ERMITTLUNGEN LAUFEN

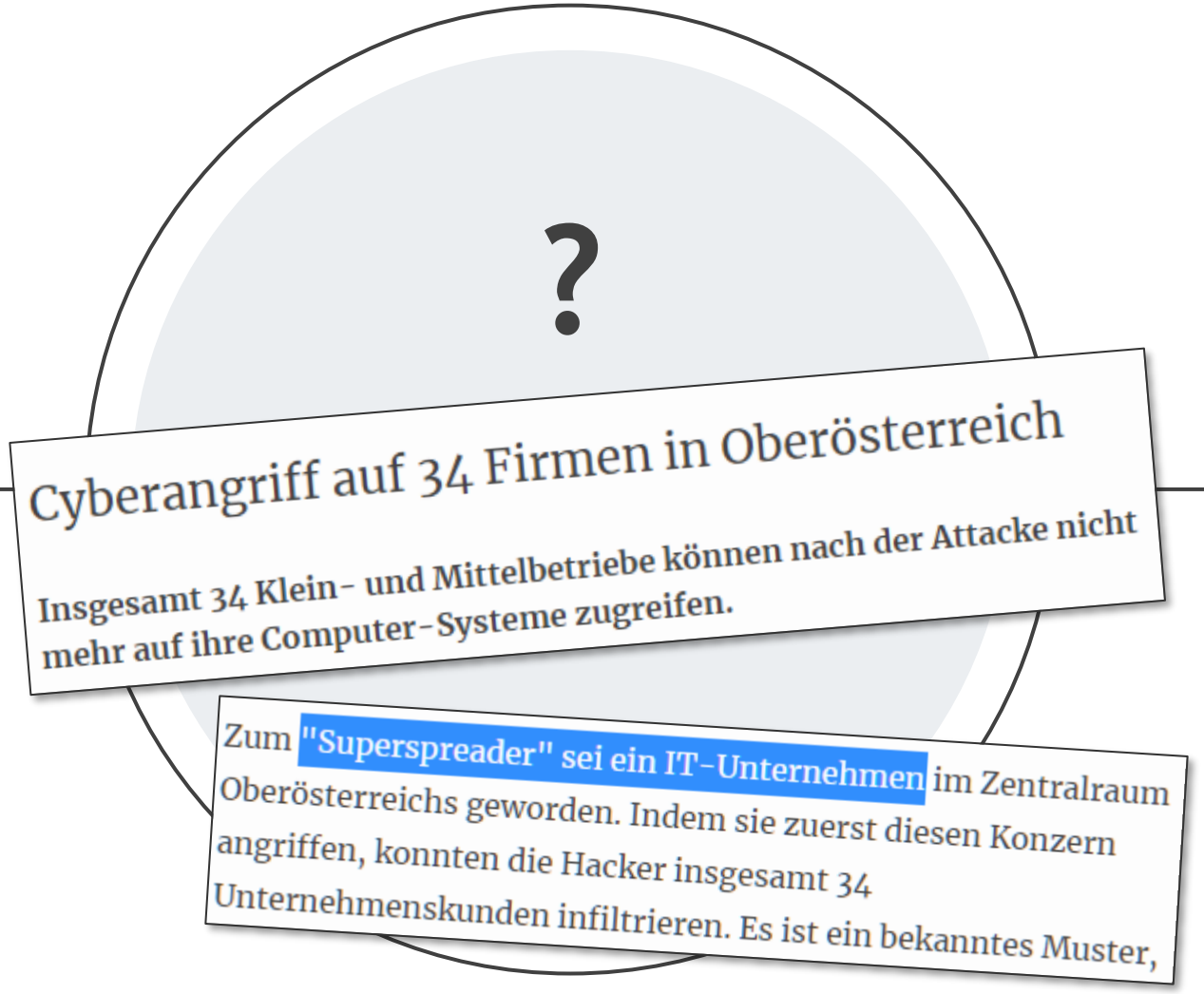
Cyberangriff auf Rosenbauer legt das Unternehmen lahm

Feuer am Dach beim Feuerwehrausrüster? Schon wieder wurde ein heimisches Unternehmen Opfer einer Attacke aus dem Internet. Der weltweit operierende Feuerwehrausstatter Rosenbauer aus Leonding wurde angegriffen. „Das genaue Ausmaß und die Dauer des Angriffs sowie dessen Folgen sind derzeit noch nicht abschätzbar", teilte das Unternehmen am Freitag mit. Als Vorsichtsmaßnahme seien Teile der IT-Infrastruktur abgeschaltet worden, die Maßnahmen würden alle Rosenbauer-Standorte betreffen. Die verantwortlichen Behörden wurden eingeschaltet und ermitteln. Nach derzeitigem Wissensstand seien aber weder Kunden- noch Unternehmensdaten entwendet oder verschlüsselt worden. Experten arbeiten an einem sicheren und schnellen Neustart.

Das Unternehmen Rosenbauer mit Sitz in Leonding ist Anfang 2023 Opfer einer Cyberattacke geworden. „Als Vorsichtsmaßnahme seien Teile der IT-Infrastruktur abgeschaltet worden, die Maßnahmen würden alle Rosenbauer-Standorte betreffen […]"

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

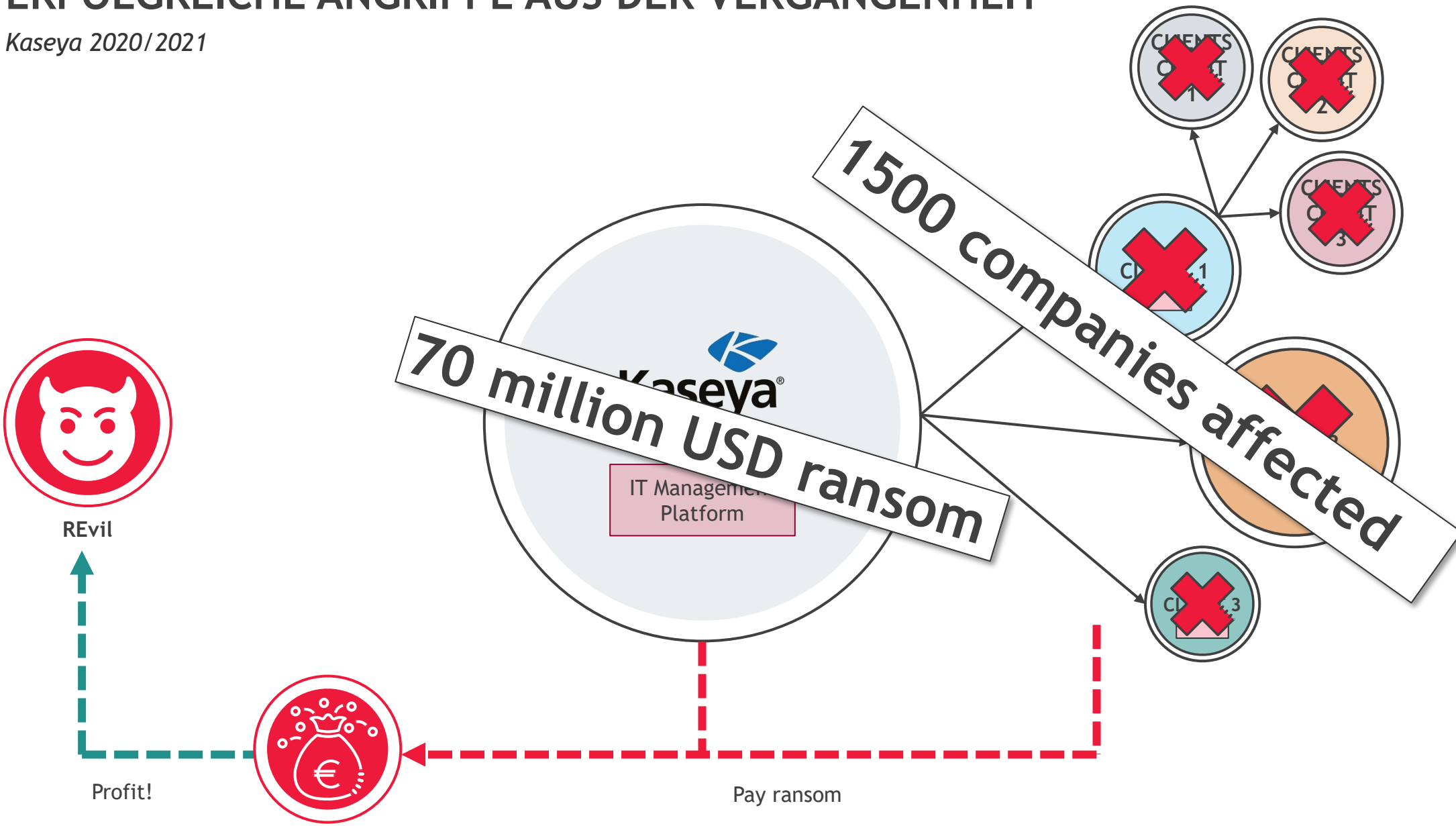


ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Kaseya 2020/2021



WER SIND DIE PROFITEURE VON CYBER CRIME?

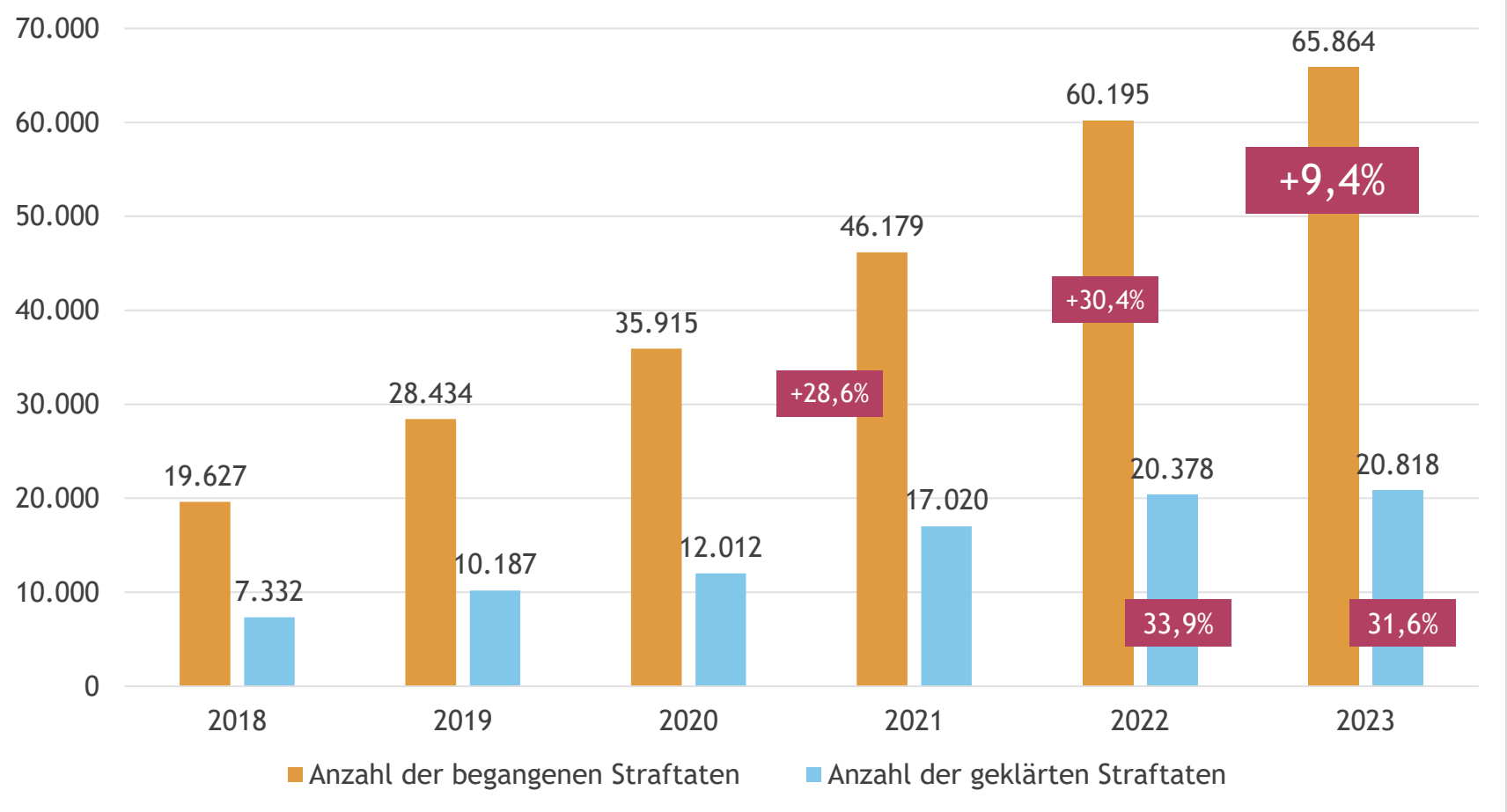
Cyber Crime und seine Auswirkungen

Hacker Group REvil

https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring
https://www.bbc.com/news/technology-59297187

CYBER CRIME IN ÖSTERREICH

Straftaten vs. geklärte Straftaten – Report 2023



https://www.bundeskriminalamt.at/306/files/Cybecrime_Report_2023_WebBF.pdf

ECKDATEN ZUR NIS 2

Richtlinie (EU) 2022/2555

NIS 2 Richtlinie (EU)

- Die NIS 2 RL wurde am 16.12.2020 von der EU-Kommission als Teil der neuen Cybersicherheitsstrategie vorgelegt
  - Seit 16. Jänner 2023 in Kraft
  - Legt Maßnahmen fest, mit welchen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll
  - Ersetzt die bisherigen Regeln der NIS 1 RL

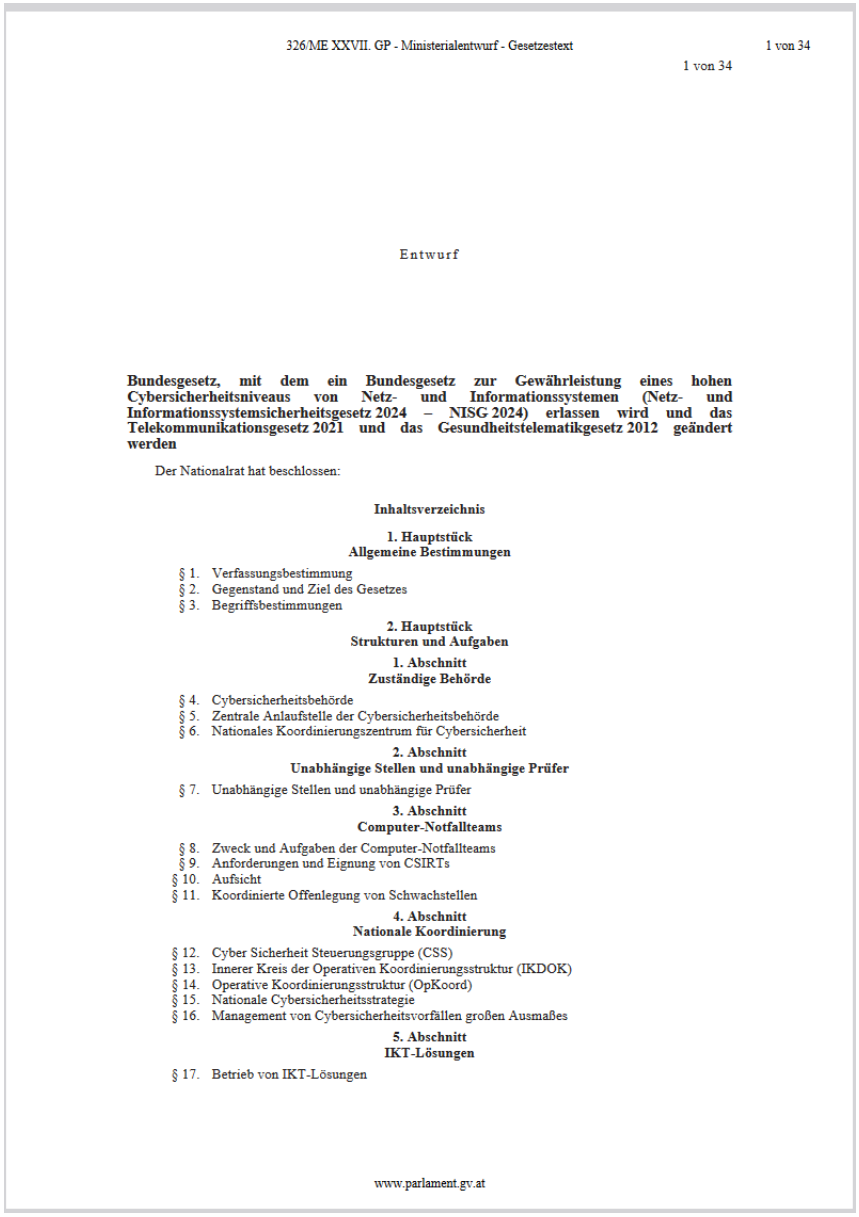
Nationale Umsetzung

- 21-monatige Umsetzungsfrist (bis 17. Oktober 2024)
- Details der nationalen Umsetzungsgesetzgebung derzeit noch offen

AUSGANGSSITUATION IN ÖSTERREICH

AUSGANGSSITUATION IN ÖSTERREICH

Umsetzung der NIS 2 Richtlinie ins nationale Recht – Status Quos



326/ME XXVII. GP - Ministerialentwurf - Gesetzestext 1 von 34

1 von 34

Entwurf

Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

www.parlament.gv.at

https://www.parlament.gv.at/dokument/XXVII/A/4129/fname_1635702.pdf

Umsetzung der NIS 2 RL ins nationale Recht

- Gemäß der NIS 2 RL ist bis zum 17.10.2024 ein nationales Gesetz zu erlassen und ab dem 18.10.2024 anzuwenden
- NISG 2024 Entwurf liegt vor
  - Wurde am 03.07.2024 im Parlament verhandelt und nicht beschlossen
- Es ist davon auszugehen, dass eine Fristgerecht Umsetzung nicht erfolgen wird
- Direktanwendbarkeit der RL?
  - Möglich in bestimmten Fällen, um die Rechte der Einzelnen zu schützen
  - wenn ihre Bestimmungen uneingeschränkt und hinreichend klar und eindeutig sind
  - und wenn der Mitgliedstaat die Richtlinie nicht fristgerecht umgesetzt hat (“Van Duyn gegen Home Office”)
  - aber ein Mitgliedstaat kann sich nicht auf Richtlinien gegenüber Einzelnen berufen („Ratti“)

ANWENDUNGSBEREICH DER NIS 2

ANWENDUNGSBEREICH DER NIS 2 RL

NIS 2 im Detail

- Gemeinden und Gemeindeverbunde sind nicht im Anwendungsbereich der RL!
  Andere Gebietskörperschaften jedoch schon.

- **Größenabhängig**
  - mittlere und große Unternehmen
  - Schwellenwerte für mittlere Unternehmen
  - mind. 50 Beschäftigte ODER Jahresumsatz von mehr als EUR 10 Mio. und Jahresbilanzsumme von mehr als EUR 10 Mio.
  - Achtung bei der Berechnung der Zahlen!
  - Beherrschende und Verbundene Unternehmen sind mitzuberücksichtigen
  - Beherrschende Unternehmen
  - Verbundene Unternehmen

- **Größenunabhängig**
  - Sektor- und Tätigkeitsspezifische Parameter
  - z.B. Vertrauensdiensteanbieter, Betreiber öffentlicher Kommunikationsnetze, Anbieter von Leistungen mit Auswirkung auf öffentliche Ordnung und Sicherheit, etc.

- **Kleine Unternehmen** sind von der NIS 2 RL **nicht betroffen**
  - d.h. Unternehmen mit weniger als 50 Mitarbeitenden und einem Jahresumsatz bzw. einer Jahresbilanzsumme von höchstens EUR 10 Mio.

- Unterscheidung in wesentliche und wichtige Einrichtungen

ANWENDUNGSBEREICH DER NIS 2 RL

Exkurs: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen

- Bei der Einstufung als mittleres oder großes Unternehmen ist die Empfehlung K(2003) 1422 zu beachten
- Artikel 2 Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen

(1) Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.

(2) Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.

(3) Innerhalb der Kategorie der KMU wird ein Kleinstunternehmen als ein Unternehmen definiert, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.

- Artikel 2 Abs 2 ist als 10 Mio. EUR Jahresumsatz und Jahresbilanz zu lesen!
- Bei der Größen Berechnung sind Beherrschende Unternehmen und Partnerunternehmen zu beachten
- (2) „Partnerunternehmen“ sind alle Unternehmen, die nicht als verbundene Unternehmen gelten und zwischen denen folgende Beziehung besteht: Ein Unternehmen (das vorgeschaltete Unternehmen) hält — allein oder gemeinsam mit einem oder mehreren verbundenen Unternehmen — 25 % oder mehr des Kapitals oder der Stimmrechte eines anderen Unternehmens (des nachgeschalteten Unternehmens). Ein Unternehmen gilt jedoch weiterhin als eigenständig, auch wenn der Schwellenwert von 25 % erreicht oder überschritten wird, sofern es sich um folgende Kategorien von Investoren handelt und unter der Bedingung, dass diese Investoren einzeln oder gemeinsam mit dem betroffenen Unternehmen nicht verbunden sind:

a) staatliche Beteiligungsgesellschaften, Risikokapitalgesellschaften, natürliche Personen bzw. Gruppen natürlicher Personen, die regelmäßig im Bereich der Risikokapitalinvestition tätig sind („Business Angels“) und die Eigenmittel in nicht börsennotierte Unternehmen investieren, sofern der Gesamtbetrag der Investition der genannten „Business Angels“ in ein und dasselbe Unternehmen 1 250 000 EUR nicht überschreitet; **b**) Universitäten oder Forschungszentren ohne Gewinnzweck; **c**) institutionelle Anleger einschließlich regionaler Entwicklungsfonds; **d**) autonome Gebietskörperschaften mit einem Jahreshaushalt von weniger als 10 Mio. EUR und weniger als 5 000 Einwohnern.

- (3) „Verbundene Unternehmen“ sind Unternehmen, die zueinander in einer der folgenden Beziehungen stehen:

a) Ein Unternehmen hält die Mehrheit der Stimmrechte der Aktionäre oder Gesellschafter eines anderen Unternehmens; **b)** ein Unternehmen ist berechtigt, die Mehrheit der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsgremiums eines anderen Unternehmens zu bestellen oder abzuberufen; **c)** ein Unternehmen ist gemäß einem mit einem anderen Unternehmen abgeschlossenen Vertrag oder aufgrund einer Klausel in dessen Satzung berechtigt, einen beherrschenden Einfluss auf dieses Unternehmen auszuüben; **d)** ein Unternehmen, das Aktionär oder Gesellschafter eines anderen Unternehmens ist, übt gemäß einer mit anderen Aktionären oder Gesellschaftern dieses anderen Unternehmens getroffenen Vereinbarung die alleinige Kontrolle über die Mehrheit der Stimmrechte von dessen Aktionären oder Gesellschaftern aus.

ANWENDUNGSBEREICH DER NIS 2 RL

Ihre Fragen

- **Fragen:**
  - Werden freie Dienstverträge auch als Mitarbeiter gezählt?
  - Wie sind geringfügig Beschäftigten – zu behandeln?
- **Antwort:**
- **Artikel 5 Mitarbeiterzahl**
- Die Mitarbeiterzahl entspricht der Zahl der Jahresarbeitseinheiten (JAE), d. h. der Zahl der Personen, die in dem betroffenen Unternehmen oder auf Rechnung dieses Unternehmens während des gesamten Berichtsjahres einer Vollzeitbeschäftigung nachgegangen sind. Für die Arbeit von Personen, die nicht das ganze Jahr gearbeitet haben oder die im Rahmen einer Teilzeitregelung tätig waren, und für Saisonarbeit wird der jeweilige Bruchteil an JAE gezählt. In die Mitarbeiterzahl gehen ein:
  - a) Lohn- und Gehaltsempfänger;
  - b) für das Unternehmen tätige Personen, die in einem Unterordnungsverhältnis zu diesem stehen und nach nationalem Recht Arbeitnehmern gleichgestellt sind;
  - c) mitarbeitende Eigentümer;
  - d) Teilhaber, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen.

Auszubildende oder in der beruflichen Ausbildung stehende Personen, die einen Lehr- bzw. Berufsausbildungsvertrag haben, sind in der Mitarbeiterzahl nicht berücksichtigt. Die Dauer des Mutterschafts- bzw. Elternurlaubs wird nicht mitgerechnet.

- Begriff des Arbeitnehmers ist nach dem nationalen Recht auszulegen.
- D.h. Personen, welche nicht Vollzeitbeschäftigt sind werden ihren Anteil nach berechnet. Somit sind geringfügig Beschäftigte anteilsmäßig zu berücksichtigen.
- Freie Dienstnehmer die auch als solche Arbeitsrechtlich einzustufen sind, sind nicht in die Berechnung der Mitarbeiter:innenanzahlen einzubeziehen.

WICHTIGE UND WESENTLICHE EINRICHTUNGEN

NIS 2 im Detail

Wesentliche (Essential)

- Energie (Strom inkl. Fernwärme, Öl, Gas, Wasserstoff)
- Verkehr (Luft, Schiene, Wasser, Straßen)
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheit (Gesundheitsdienstleister, EU-Referenzlaboratorien, Arzneimittelforschung und -entwicklung, pharmazeutische Grundstoffe und Präparate & medizinische Notfallgeräte
- Trinkwasserversorgung
- Abwasser
- Digitale Infrastruktur
- IKT-Dienstleistungsmanagement
- Öffentliche Verwaltung
- Raumfahrt

Wichtige (Important)

- Post- und Kurierdienste
- Abfallwirtschaft
- Herstellung, Produktion und Vertrieb von Chemikalien
- Herstellung, Verarbeitung und Vertrieb von Lebensmitteln
- Herstellung von medizinischen Geräten, Computern, elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, Maschinen und Ausrüstungen, Kraftfahrzeugen, Anhängern und Sattelanhängern, sonstigen Transportmitteln
- Digitale Anbieter (Online-Marktplätze, Online-Suchmaschinen & Plattformen für soziale Netzwerkdienste)
- Forschung

ANWENDUNGSBEREICH DER NIS 2 RL

NIS2 im Behindertenbereich

- Anhang I: Gesundheit (Gesundheitsdienstleister, EU-Referenzlaboratorien, Arzneimittelforschung und -entwicklung, pharmazeutische Grundstoffe und Präparate & medizinische Notfallgeräte
- Behindertenbereich als Gesundheitsdienstleister?
- Die NIS2 Verweist auf 2011/24/EU:
  - Artikel 3 a) „Gesundheitsversorgung“ Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten;
  - Artikel 3 g) „Gesundheitsdienstleister“ jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt;
- „Gesundheitsdiensteanbieter“ im Österreichischen Recht: Verantwortlicher oder Auftragsverarbeiter (Art. 4 Z 7 und 8 DSGVO), die regelmäßig in einer Rolle nach der gemäß § 28 Abs. 1 Z 1 erlassenen Verordnung Gesundheitsdaten oder genetische Daten in elektronischer Form zu folgenden Zwecken verarbeiten:
  - medizinische Behandlung oder Versorgung oder
  - pflegerische Betreuung oder
  - Verrechnung von Gesundheitsdienstleistungen oder
  - Versicherung von Gesundheitsrisiken oder
  - Wahrnehmung von Patient/inn/en/rechten.
  - Wenn solch eine Verarbeitung im Behindertenbereich erfolgt handelt es sich also um eine Gesundheitsversorgung bzw. Gesundheitsdienstleister und die Anwendbarkeit der NIS 2 ist somit eröffnet

PFLICHTEN UND ANFORDERUNGEN

PFLICHTEN UND ÜBERWACHUNG

Relevante Artikel

Pflichten

Die wesentlichen Pflichten der von der NIS 2 RL erfassten Einrichtungen sind in **Art 20 ff NIS 2 RL** festgelegt und umfassen:

- Governance (**Art 20**)
- Risikomanagementrahmen (**Art 21**)
- Berichtspflichten bei erheblichen Sicherheitsvorfällen (**Art 23**)

Überwachung

- Aufsichts- & Durchsetzungsmaßnahmen (**Art 32**)
- Sanktionen (**Art 34**)

SANKTIONEN

Umsetzung Artikel 34

Geldbußen

- Strafhöhe variiert für wesentliche und wichtige Einrichtungen
  - wesentliche Einrichtungen: Bis zu EUR 10 Mio. oder 2% des weltweiten Gesamtumsatzes im vorangegangenen Geschäftsjahr
  - wichtige Einrichtungen: Bis zu EUR 7 Mio. oder 1,4% des weltweiten Gesamtumsatzes im vorangegangenen Geschäftsjahr
  - Vergleich NISG: EUR 50.000 (im Wiederholungsfall EUR 100.000)
  - Zwangsstrafen und sonstige Durchsetzungsmaßnahmen weiterhin ergänzend zulässig
  - Leitungsorgane, die ihre Pflichten verletzen können für den schuldhaft verursachten Schaden haftbar gemacht werden

UMSETZUNG DER ANFORDERUNGEN

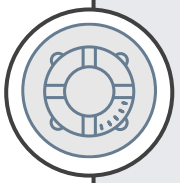
4 HAUPTBEREICHE FÜR UNTERNEHMEN

Pflichten und Anforderungen

Artikel 20 NIS 2 RL
§ 31 NISG 2024 Entwurf

Governance

- Nimmt Leitungsorgane der Einrichtungen in die Verantwortung.
- **Haftungsthema!** (*„[…] management bodies […] can be held liable for infringements […]“* Artikel 20 Abs.1)



Artikel 21 NIS 2 RL
§ 32f NISG 2024 Entwurf

Risikomanagement-maßnahmen

- gefahrenübergreifenden Ansatz / All-Hazards Approach
- Geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen sowie Berücksichtigung des Stands der Technik sowie der Kosten der Umsetzung

Artikel 23 NIS 2 RL
§ 34 NISG 2024 Entwurf

Berichtspflichten

- Es muss das CSIRT **unverzüglich** über jeden Sicherheitsvorfall unterrichtet werden, wenn der Sicherheitsvorfall **erhebliche Auswirkungen** auf die Erbringung der Dienste hat.

Artikel 32 NIS 2 RL
§38ff NISG 2024 Entwurf

Aufsichts- und Durchsetzungsmaßnahmen

- Zuständige Behörden mit Aufsichtsaufgaben, welche die Umsetzung der Maßnahmen (v.a. Artikel 21) überprüfen und Verstöße aufzeigen.

GOVERNANCE

Umsetzung Artikel 20 NIS 2 RL, § 31 NISG 2024 Entwurf

Management Prozess zum Informationssicherheits-management einführen

- Leitungsorgane müssen sich aktiv in das Informationssicherheitsmanagement integrieren.
- Mögliche Implementierung durch regelmäßige Management-Meetings zwischen Informationssicherheitsverantwortlichen und den Leitungsorganen.

Einrichtung einer zentralen Stelle für Cyber Security (CISO)

- Da die Leitungsorgane keine operativen Tätigkeiten im Cyber Security Bereich wahrnehmen werden können, sollte eine eigene Stabstelle eingerichtet werden, die sich mit der kontinuierlichen Weiterentwicklung der Cyber Sicherheit beschäftigt und an die Leitungsorgane berichtet.

Regelmäßige Schulung für Leitungsorgane

- Regelmäßige Präsenzschulungen für Leitungsorgane durchführen.
- Inhalt speziell an die Zielgruppe anpassen!

Regelmäßige Schulungen für Mitarbeiter zum Thema Cyber Security

- Regelmäßige Schulungen für Belegschaft durchführen.
- Hier können auch Online-Trainings zur Anwendung kommen.
- Ggf. Spezialtrainings für besondere Personenkreise (z.B. IT-Administratoren, Bereichsleiter etc.)

RISIKOMANAGEMENTMAßNAHMEN

Umsetzung Artikel 21 NIS 2 RL, § 32f NISG 2024 Entwurf

ALLGEMEINE ÜBERLEGUNGEN ZUR UMSETZUNG

- **Verhältnismäßigkeit**, **Stand der Technik**, nationale und internationale Standards sowie die **Kosten der Maßnahmen** müssen berücksichtigt werden.

  Unterschiedliche Anforderungen an Maßnahmen je Unternehmen!

- Anforderungen sind nichts Neues! Alle Anforderungen (10) aus der NIS2-RL sind in den österreichischen Anforderungen der NISV Anlage 1 bereits enthalten.

- NIS2-RL-Schreiber „lernen“ aus den Angriffen der Vergangenheit:

  - Verstärkter Fokus auf die **Lieferkette** → Angriffe auf Dienstleister (Solarwinds) bzw. Standardsoftware (Microsoft Exchange)

  - **Betriebskontinuität**, Verschlüsselung und Mitarbeitersicherheit → Phishing & Ransomware (z.B. REvil)

VERGLEICH NIS1 ZU NIS2

Risikomanagementmaßnahmen – Artikel 21

Kapitel	NIS 1 / Bezeichnung
1	Governance und Risikomanagement
2	Umgang mit Dienstleistern, Lieferanten und Dritten
3	Sicherheitsarchitektur
4	Systemadministration
5	Identitäts- und Zugriffsmanagement
6	Systemwartung und Betrieb
7	Physische Sicherheit
8	Erkennung von Vorfällen
9	Bewältigung von Vorfällen
10	Betriebskontinuität
11	Krisenmanagement

Nr	NIS 2 / Maßnahmen / Beschreibung
1	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
2	Bewältigung von Sicherheitsvorfällen;
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
4	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen; (Anm.: Betriebssicherheit)
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
7	grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
8	Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung. (Anm.: Kommunikationssicherheit)

RISIKOMANAGEMENTMAßNAHMEN NISG 2024 ENTWURF

Themengebiet
1. Leitungsorgane
a. Rollen und Verantwortlichkeiten der Leitungsorgane
2. Sicherheitsrichtlinien
a. Sicherheitsrichtlinien
b. Funktionen, Aufgaben und Verantwortlichkeiten
3. Risikomanagement
a. Risikomanagementrichtlinie und -prozess
b. Beurteilung der Effektivität von Risikomanagementmaßnahmen
c. Überwachung der Einhaltung von Vorgaben
d. Unabhängige Überprüfungen
4. Verwaltung von Vermögenswerten
a. Inventarisierung von Vermögenswerten
b. Klassifikation von Vermögenswerten
c. Handhabung von Vermögenswerten
d. Umgang mit Wechseldatenträger
e. Rücknahme oder Löschung von Vermögenswerten
5. Personalwesen
a. Sicherheit im Personalwesen
b. Hintergrundüberprüfung
c. Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
d. Disziplinarmaßnahmen
6. Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
a. Bewusstseinsschaffung und Cyberhygiene
b. Cybersicherheitsschulungen
7. Sicherheit von Lieferketten
a. Richtlinie zur Sicherheit von Lieferketten
b. Lieferantenverzeichnis

Themengebiet
8. Zugangssteuerung
a. Zugangssteuerungsrichtlinie
b. Verwaltung von Zugriffsberechtigungen
c. Privilegierte und administrative Zugänge
d. Systeme und Anwendungen zur Systemadministration
e. Identifikation
f. Authentifikation
g. Multi-Faktor-Authentifikation
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
a. Konfigurationsmanagement
b. Änderungsmanagement und Wartung
c. Umgang mit Schwachstellen und deren Offenlegung
d. Sicherheitstests
e. Patchmanagement
f. Sicherheit bei der Beschaffung von Dienstleistungen, Systemen und Produkten
g. Sichere Softwareentwicklung
h. Netzwerksegmentierung
i. Netzwerksicherheit
j. Schutz vor bösartiger und unautorisierter Software
10. Kryptographie
a. Kryptographierichtlinie
11. Umgang mit Cybersicherheitsvorfällen
a. Richtlinie zum Umgang mit Cybersicherheitsvorfällen
b. Überwachung und Protokollierung
c. Meldung von Ereignissen
d. Erhebung und Klassifikation von Ereignissen
e. Reaktion auf Cybersicherheitsvorfällen
f. Erkenntnisse nach Cybersicherheitsvorfällen
12. Betriebskontinuitäts- und Krisenmanagement
a. Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
b. Backup-, Redundanz- und Wiederherstellungsmanagement
c. Krisenmanagement
13. Umgebungsbezogene und physische Sicherheit
a. Sicherheitsperimeter und physische Zutrittskontrollen
b. Schutz vor umgebungsbezogenen Gefährdungen
c. Versorgungseinrichtungen

BERICHTSPFLICHTEN

Umsetzung Artikel 23 NIS 2 RL, § 34 NISG 2024 Entwurf

Prozess zur Meldung von signifikanten Sicherheitsvorfällen

- Wesentliche und wichtige Einrichtungen haben innerhalb **24 Stunden eine Frühwarnung** und innerhalb **72 Stunden** jeden Vorfall, der **erhebliche Auswirkungen auf die Erbringung ihrer Dienstleistungen** hat, zu melden.
- Es sollte innerhalb des Unternehmens ein **Prozess eingeführt** werden, der die Verantwortlichkeiten regelt und den kompletten Ablauf der Meldungen beschreibt (Wer, Wann, Was, Wo, Woher, etc.).
- Aktuell müssen Meldungen an CERT.at erfolgen -> Wahrscheinlichkeit, dass dieser Prozess beibehalten wird.

Dokumentation, Know-How und Notfallpläne

- Mitarbeiter sollten zu den internen Meldeprozessen für Sicherheitsvorfälle informiert werden.
- Es sollten Methoden geschaffen werden, dass diese Meldungen und alle damit verbundenen Informationen (IOCs, Umfang, Auswirkung, Maßnahmen, etc.) zentral dokumentiert werden können.
- Entsprechendes Know-How zur Reaktion und Abarbeitung auf/von Vorfällen sollte aufgebaut werden (IT-Forensik, Kommunikationsstrategien intern/extern, etc.)

AUFSICHTS- UND DURCHSETZUNGSMAßNAHMEN

Artikel 32 NIS 2 RL, §38ff NISG 2024 Entwurf

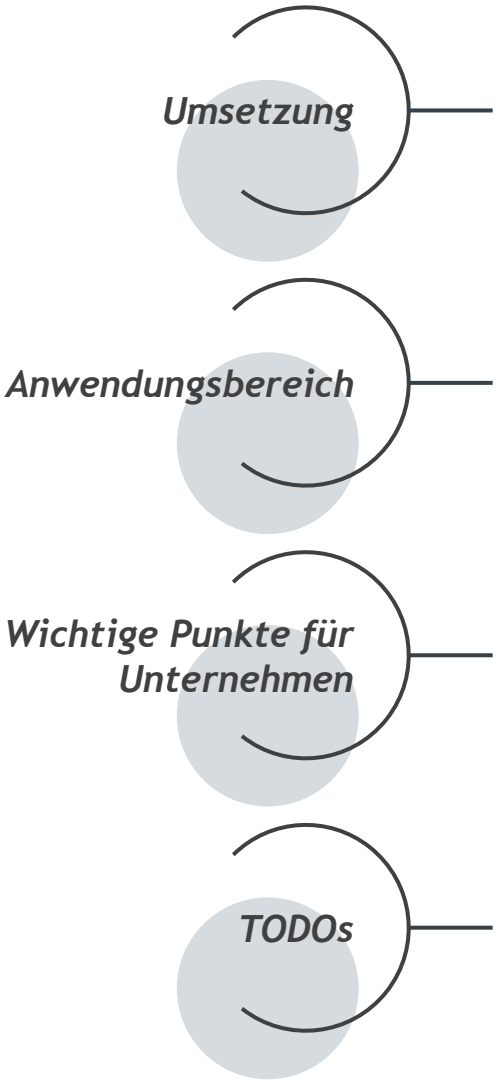
Vorbereitung auf Audits

- Nachweise zu den Anforderungen werden regelmäßig durch externe Experten geprüft. Aktuell (NIS1) alle 3 Jahre -> mögl. Richtwert für NIS2
- Dokumentation, v.a. zu Artikel 21 Maßnahmen, sollte zentral abgelegt werden. So sind alle Informationen zum Zeitpunkt des Audits verfügbar. Dies 1) zeigt dem Auditor Professionalität des Auditierten und 2) vermindert das Risiko, dass man dem Auditor zusätzliche Daten präsentiert (z.B. durchstöbern des Laufwerks nach Dateien).
- Mitarbeiter sollten zum Umgang mit Auditoren geschult werden. Nicht jedes kleinste Detail muss preisgegeben werden.
- (Zeit-)Ressourcen während on-site Audits reservieren. Vor allem die relevanten Leitungsorgane sollten am Anfang des Audits persönlich teilnehmen.
- Sollte das Zeitintervall bei 3 Jahren bleiben, so empfehlen wir interne „Zwischenaudits“ durchzuführen. Dadurch wird Verbesserungspotenzial frühzeitig erkannt und negative Audit-Ergebnisse vermieden.

ZUSAMMENFASSUNG

GROBER ÜBERBLICK DER NIS 2 RL

Zusammenfassung



- Seit 16. Jänner 2023 in Kraft
- 21-monatige Umsetzungsfrist (bis 17. Oktober 2024)
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
- NISG 2024 Entwurf

- Größenabhängig und Größenunabhängig
- Unterscheidung in wesentliche und wichtige Einrichtungen

- Governance, Risikomanagement, Berichtspflichten (bei erheblichen Sicherheitsvorfällen)
- Aufsichts- & Durchsetzungsmaßnahmen, Sanktionen

- Betroffenheit des eigenen Unternehmens prüfen
- Laufend informiert bleiben
- Umsetzungsmaßnahmen planen & starten -> nicht weiter bis Oktober 2024 warten!

IHRE VORTRAGENDEN

IHRE VORTRAGENDEN

Mario Neubauer
Senior Manager

+43 664 60 375 - 4253
mario.neubauer@bdo.at

Stefan Ziman
Consultant

+43 664 60 375 - 1687
stefan.ziman@bdo.at

WE SEARCH FOR GREATNESS.

BDO