DAS NEUE NETZ- UND INFORMATIONSSYSTEM-SICHERHEITSGESETZ 2026 (NISG 2026)

VOM GESETZ ZUR GEMEINDEPRAXIS

FLGÖ NÖ – LANDESFACHTAGUNG & MITGLIEDERVERSAMMLUNG

26. AUGUST 2026 | SITZENBERG-REIDLING

CleverData
WORLD OF BUSINESS SOLUTIONS

IHR VORTRAGENDER

Dipl.-Ing. Kurt Berthold
Zertifizierter Datenschutzbeauftragter
Zertifizierter ISMS-Manager & -Auditor
Zertifizierter NIS-2 Officer gem. EU-Richtlinie 2022/2555

clever data gmbh
Danhausergasse 9/Top 3
A-1040 Wien

E-Mail: kurt.berthold@cleverdata.at

Internet: https://www.cleverdata.at

AGENDA

wir sollen:

1. NIS 2 bedeutet:

wir sind:

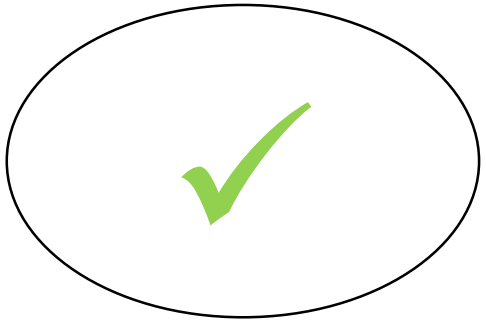
2. Cybersicherheit als Führungsaufgabe

wir müssen:

3. Rechts- und Haftungsfragen

wir werden:

4. Handlungs-bedarf



wir haben:

5. Standortanalyse

wir benötigen:

6. Equipment

7. Milestones

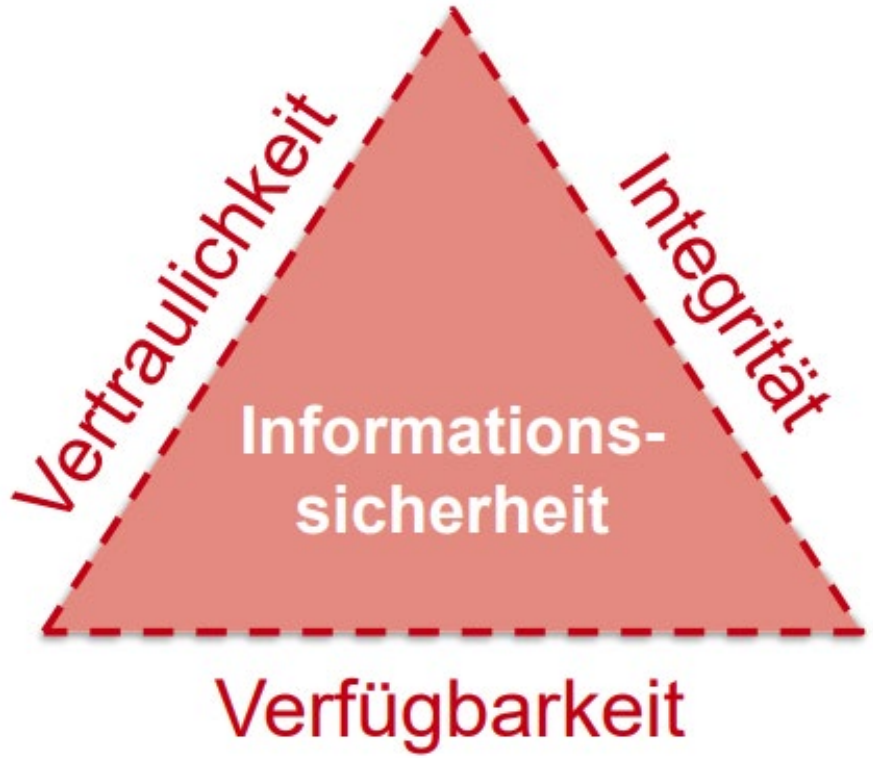
wir können!

ECKDATEN

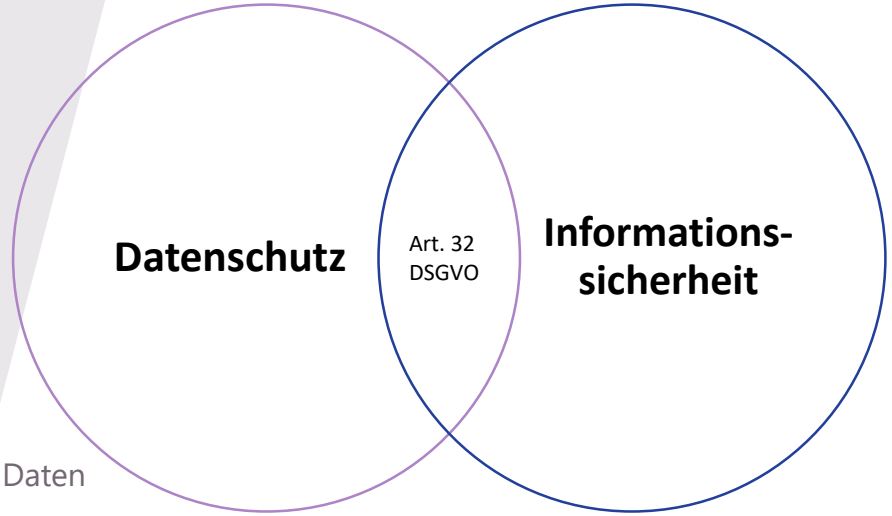
RICHTLINIE (EU) 2022/2555
vom 14. Dezember 2022
(NIS-2-Richtlinie)

Österreich NISG 2026

Definition der Informationssicherheit



Datenschutz vs. Informationssicherheit



- Schutz von personenbezogenen Daten
- Geregelt in DSGVO und DSG
- Datenschutz dient dem Zweck natürliche Personen und ihre Grundrechte und Grundfreiheiten schützen.

- Sicherheit von Daten
- Schutz von Daten allgemein
- Gewährleistung von
  - Vertraulichkeit
  - Integrität und
  - Verfügbarkeit von Daten

Artikel 32 DSGVO regelt die Sicherheit der Verarbeitung personenbezogener Daten

CleverData
WORLD OF BUSINESS SOLUTIONS

§3 Z1 NISG 2026 (SCHUTZGUT)

1. „Netz- und Informationssystem“

a) ein Kommunikationsnetz gemäß § 4 Z 1 des Telekommunikationsgesetzes 2021 (TKG 2021), BGBl. I Nr. 190/2021,

b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

c) digitale Daten, die von den in lit. a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

CleverData
WORLD OF BUSINESS SOLUTIONS

§3 Z2 UND 2 NISG 2026 (SCHUTZZIEL)

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen können;

3. „Cybersicherheit“ alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

CleverData
WORLD OF BUSINESS SOLUTIONS

WARUM NISG 2026?

WARUM NISG 2026?

THEMA SICHERHEIT

Massive Zunahme von Cyberangriffen

Stetig steigende Computerkriminalität sowie konkrete Gefahren durch Ransomware-Attacken (Verschlüsselungsangriffe) und DDoS-Attacken, die auch österreichische Unternehmen und die Verwaltung zunehmend treffen

Abhängigkeit der Gesellschaft

Da nahezu alle Bereiche des täglichen Lebens und der Wirtschaft digital durchdringen sind, ist die Gesellschaft extrem verwundbar gegenüber Störungen der Netz- und Informationssysteme geworden

Schutz der Demokratie

Moderne Demokratien benötigen ein stabiles organisatorisches und finanzielles Fundament, um der wachsenden Bedeutung von Cybersicherheit staatlich gerecht zu werden und die öffentliche Ordnung und Sicherheit zu gewährleisten

CleverData
WORLD OF BUSINESS SOLUTIONS

WARUM NISG 2026?

DER GESETZLICHE AUFTRAG

Umsetzung der NIS-2-Richtlinie

Das NISG 2026 dient der verpflichtenden nationalen Umsetzung der EU-Richtlinie (EU) 2022/2555. Ziel ist ein unionsweit einheitliches und hohes Cybersicherheitsniveau

Vermeidung von Sanktionen

Eine Nicht-Umsetzung der EU-Vorgaben würde ein Vertragsverletzungsverfahren gegen Österreich nach sich ziehen

CleverData
WORLD OF BUSINESS SOLUTIONS

WARUM NISG 2026?

STRATEGISCHE ZIELE DES GESETZES (DER NUTZEN)

Reaktion auf reale Gefahren

Schutz vor Ransomware, Spionage und Sabotage angesichts steigender Cyberkriminalität

Sicherung unserer Lebensgrundlagen

Schutz der Netz- und Informationssysteme, von denen Staat, Wirtschaft und Gesellschaft heute vollständig abhängig sind

Europaweiter Sicherheitsstandard

Verbindliche Umsetzung der EU-NIS-2-Richtlinie zur Schaffung eines einheitlichen Schutzniveaus

Stärkung der nationalen Krisenfestigkeit

Aufbau effizienter Behördenstrukturen (Bundesamt für Cybersicherheit) und klarer Verantwortlichkeiten

Vertrauen in die Digitalisierung

Cybersicherheit als Grundvoraussetzung für eine funktionierende digitale Verwaltung und Wirtschaft

CleverData
WORLD OF BUSINESS SOLUTIONS

NIS 2 BEDEUTET: „WIR SOLLEN“

ÜBERBLICK NIS-2-RICHTLINIE – EINLEITUNG

Modernisierung des Rechtsrahmens

- Zunehmende Digitalisierung
- Entwicklung der Bedrohungslandschaft
- Defizite von NIS1

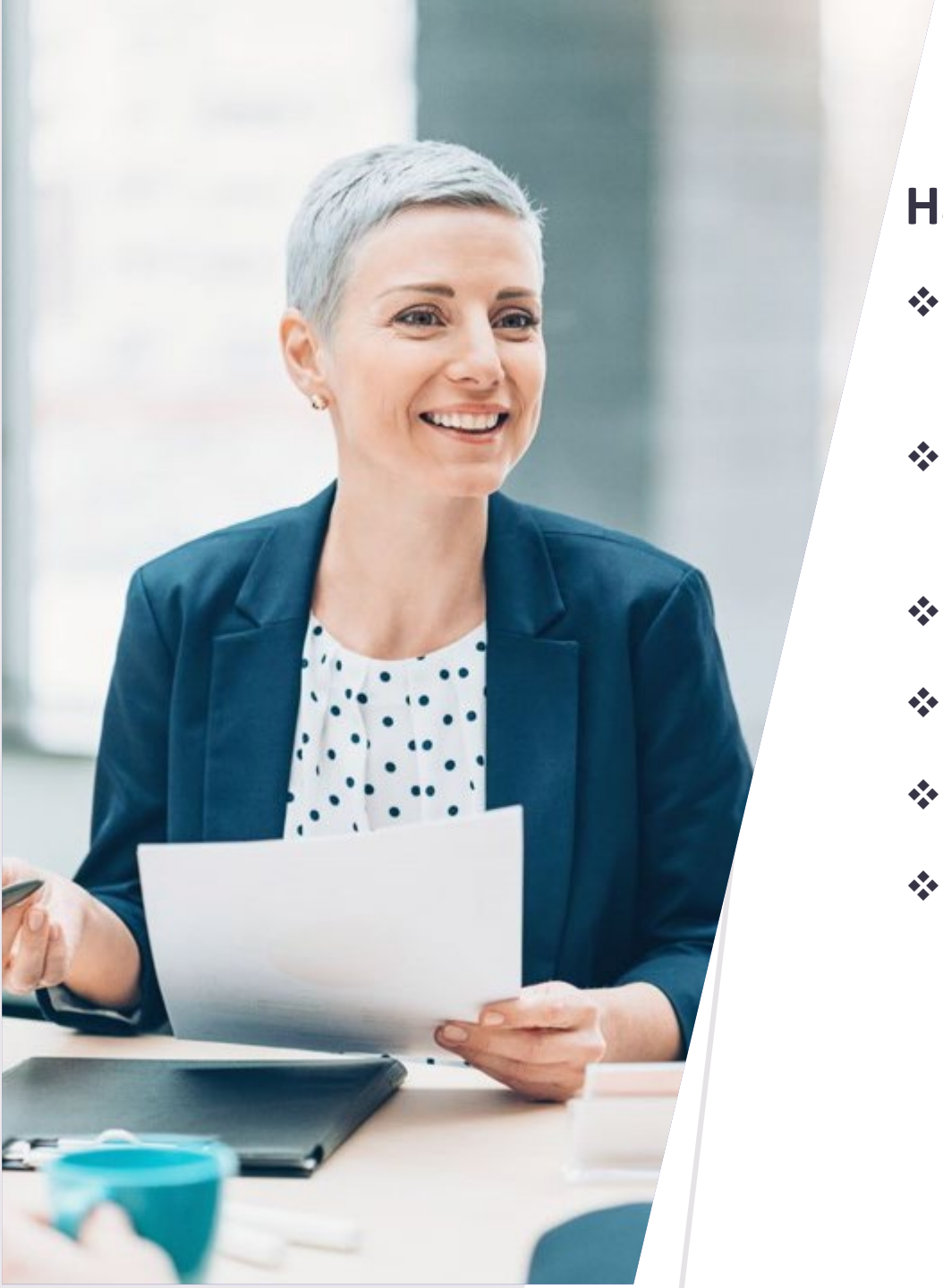
→ deutlich höhere Anforderungen + deutliche Ausweitung des Anwendungsbereiches.

Hintergrund

IT-Systeme spielen eine zentrale Rolle in der Gesellschaft – Verlässlichkeit und Sicherheit sind entscheidend für wirtschaftliche und gesellschaftliche Tätigkeiten und das Funktionieren des Binnenmarkts.

Stichwort: „Resilienz der Gesellschaft“

CleverData
WORLD OF BUSINESS SOLUTIONS



ÜBERBLICK NIS-2-RICHTLINIE – EINLEITUNG

Hauptziele NIS 2:

- Größeren Teil der Wirtschaft und Gesellschaft abdecken (mehr Sektoren)
- Systematische Konzentration auf größere, mittlere und kritische Akteure
- Angleichung der Sicherheitsanforderungen
- Straffung der Berichtspflichten
- Angleichung der Aufsicht und Durchsetzung
- Mehr operative Zusammenarbeit, inkl. EU-Cyber-Krisenmanagement

CleverData
WORLD OF BUSINESS SOLUTIONS

GELTUNGSBEREICH DER NIS-2-RICHTLINIE NATIONALE UMSETZUNG → NISG 2026

Gilt ab: 1.10.2026

Gilt für: Grundanwendungsregel ist die sogenannte size-cap-rule: betroffen sind Unternehmen („Einrichtungen“) bestimmter Sektoren, die als **besonders gesellschafts-wesentlich** erachtet werden, ab einer bestimmten Unternehmensgröße. Der Unternehmensbegriff ist weit gefasst.

Sektoren: Anlage 1 (hohe Kritikalität) und Anlage 2 (sonst kritisch) des NISG

CleverData
WORLD OF BUSINESS SOLUTIONS

Quelle: Newsletter 1/2026 der österreichischen Datenschutzbehörde

SIND SIE BETROFFEN? → SEKTOREN

ANLAGE 1 – NISG 2026
(Sektoren mit hoher Kritikalität)

1. Energie
2. Verkehr
3. Bankwesen
4. Finanzmarktinfrastrukturen
5. Gesundheitswesen
6. Trinkwasser
7. Abwasser
8. Digitale Infrastruktur
9. Verwaltung von IKT-Diensten (Business-to-Business)
10. öffentliche Verwaltung
11. Weltraum

ANLAGE 2 – NISG 2026
(Sonstige kritische Sektoren)

1. Post- und Kurierdienste
2. Abfallbewirtschaftung
3. Produktion, Herstellung und Handel mit chemischen Stoffen
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln
5. Verarbeitendes Gewerbe/Herstellung von Waren
6. Anbieter digitaler Dienste
7. Forschung

SIND SIE BETROFFEN? → GRÖßE DER ORGANISATION

	Mitarbeiter	oder	Umsatz / Jahr	und	Jahresbilanzsumme
Mittleres Unt.	**50+**		**10 Mio. €+**		**10 Mio. €+**
Großes Unt.	250+		50 Mio. €+		43 Mio. €+

Sektoren	Große Unternehmen	Mittlere Unternehmen	Kleine Unternehmen
Anlage 1	wesentlich	**wichtig**	-
Anlage 2	wichtig	**wichtig**	-

Wesentliche Einrichtung	Wichtige Einrichtung
Ex-ante- und Ex-post-Aufsicht	Reaktive Ex-post-Aufsicht, z.B. bei Verdacht auf Verstöße, nicht zwingend erforderlich

SONDERREGELN – ANLAGE 1 NISG 2026
§ 24 ABS. 1 NISG 2026 (EVTL. FÜR LIEFERKETTE INTERESSANT)

<table>
<tr><th>Teilsektor</th><th>Große Unternehmen</th><th>Mittlere Unternehmen</th><th>Kleine Unternehmen</th></tr>
<tr><td>Qualifizierte Vertrauensdienste-anbieter</td><td colspan="3" rowspan="4">wesentlich</td></tr>
<tr><td>TLD-Namenregister</td></tr>
<tr><td>DNS-Diensteanbieter</td></tr>
<tr><td>öffentlichen Verwaltung auf Bundesebene</td></tr>
<tr><td>Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikations-dienste</td><td colspan="2" rowspan="2">wesentlich</td><td rowspan="2">Wichtig (außer falls als wesentlich ermittelt)</td></tr>
<tr><td>Vertrauensdiensteanbieter</td></tr>
<tr><td>Betreiber von Internetknoten</td><td rowspan="4">wesentlich</td><td rowspan="4">wichtig (außer falls als wesentlich ermittelt)</td><td rowspan="4">Nicht im Anwendungsbereich außer falls ermittelt als wesentlich oder wichtig</td></tr>
<tr><td>Anbieter von Cloud-Computing-Diensten</td></tr>
<tr><td>Anbieter von Rechenzentrums-diensten</td></tr>
<tr><td>Betreiber von Inhaltszustellnetzen (Content delivery network providers)</td></tr>
</table>

QUELLE: VGL. BKA

ÜBERGREIFENDE INHALTE UND ZIELE DER NIS-2-RICHTLINIE

Besonders im Fokus steht dabei die Verantwortung der Leitungsorgane

Sie muss gewährleisten, dass Cybersicherheit integraler Bestandteil der Geschäfte des Unternehmens und des Risikomanagements ist. Diese besondere Verantwortung der Geschäftsleitungen ist gesetzlich vorgeschrieben, ebenso wie eine Schulungspflicht für die Leitungsorgane

CleverData
WORLD OF BUSINESS SOLUTIONS

REGISTER DER EINRICHTUNGEN

§ 29 (2) NISG 2026: Betroffene Einrichtungen haben sich bei der Cybersicherheitsbehörde zu registrieren und dieser im elektronischen Weg folgende Angaben über einen sicheren Kommunikationskanal strukturiert zu übermitteln:

1. den Namen der Einrichtung;
2. die Anschrift und aktuelle Kontaktdaten sowie gegebenenfalls den gemäß § 28 Abs. 4 benannten Vertreter;
3. den Sektor oder die Sektoren, den Teilsektor oder die Teilsektoren und die Art oder Arten der Einrichtung gemäß Anlage 1 oder 2;
4. die Mitgliedstaaten der Europäischen Union, in denen sie Dienste erbringt;
5. gegebenenfalls die IP-Adressbereiche der Einrichtung;
6. die Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls sie nicht in der Europäischen Union niedergelassen ist, die Anschrift ihres gemäß § 28 Abs. 4 benannten Vertreters;
7. Informationen zu den in § 25 angeführten Schwellenwerten und darüber, ob es sich um eine wesentliche oder wichtige Einrichtung handelt

CleverData
WORLD OF BUSINESS SOLUTIONS

RELEVANTE GESETZESSTELLEN

§ 33 NISG 2026 – Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

- (1) Selbstdeklaration: Wesentliche und wichtige Einrichtungen haben innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht der Cybersicherheitsbehörde Informationen hinsichtlich umgesetzter Risikomanagementmaßnahmen gemäß § 32, insbesondere betreffend die genutzten Netz- und Informationssysteme und die Sicherheit der Lieferketten sowie die Ergebnisse der durchgeführten Risikoanalyse, nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form zu übermitteln.

- (2) Prüfung durch unabhängige Stelle (wesentliche Einrichtungen)

CleverData
WORLD OF BUSINESS SOLUTIONS

RELEVANTE GESETZESSTELLEN

§ 34 NISG 2026 – Berichtspflichten | § 35 NISG 2026 Erheblicher Cybersicherheitsvorfall

Berichtspflichten bestehen bei erheblichen Sicherheitsvorfällen – Was heißt erheblich?

- schwerwiegende Betriebsstörungen der Dienste oder schwerwiegende finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
- andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann

§ 35 NISG 2026: Angaben zur Beurteilung eines erheblichen (Cyber)Sicherheitsvorfalls, z.B.:

- Sind andere Sektoren betroffen? Auswirkungen auf Umwelt, öffentliche Ordnung, Gesundheit, Geographische Ausbreitung , Marktanteil, ...
- Präzisierung für bestimmte Bereiche der Digitalen Infrastruktur in der Durchführungsverordnung (EU) 2024/2690
- Meldung (unverzüglich!) an das zuständige sektorspezifische CSIRT (GovCERT.at)
- Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter.

CleverData
WORLD OF BUSINESS SOLUTIONS

MELDESTELLEN

Computer-Notfallteams (CERTs/CSIRTs)

CERT.at (www.cert.at)

GovCERT.at (www.govcert.gv.at)

AEC (Austrian Energy CERT) (www.energy-cert.at)

Austrian HealthCERT (https://a-healthcert.at)

plus zahlreiche firmen-/behördeneigene CERTs

CYBERSICHERHEIT ALS FÜHRUNGSAUFGABE „WIR SIND“

ZIEL

Verantwortlichkeiten und Wirkungszusammenhänge deutlich machen → nicht technische Details vermitteln

Die Leitung trägt die strategische Verantwortung für die Umsetzung und muss daher wissen, worauf sie besonderes Augenmerk legen sollte

CleverData
WORLD OF BUSINESS SOLUTIONS

LEITUNGSORGANE

Eine oder mehrere natürliche Personen oder Verwaltungsorgane, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung berufen sind, z.B. Geschäftsführung oder Vorstand, Bgm, Gemeinderat (?).

CleverData
WORLD OF BUSINESS SOLUTIONS

KENNTNISSE UND FÄHIGKEITEN DER LEITUNGSORGANE

- Erkennung und Bewertung von Risiken
- Risikomanagementpraktiken
- Beurteilung der Auswirkungen von Risiken sowie Risikomanagementpraktiken

CleverData
WORLD OF BUSINESS SOLUTIONS

RECHTS- UND HAFTUNGSFRAGEN „WIR MÜSSEN“

HAFTUNG: VERWALTUNGSSTRAFEN

- Der Verdacht einer Verwaltungsübertretung ist von der Cybersicherheitsbehörde der Bezirks-verwaltungsbehörde anzuzeigen (§ 44 NISG)
- Wichtige Einrichtungen: bei Nichteinhaltung der gesetzlichen Vorgaben Verwaltungsstrafen bis zu **EUR 7 Mio**. bzw. 1,4 % des weltweiten (Konzern-) Jahresumsatzes (§ 45 Abs 3 NISG)
- Wesentliche Einrichtungen: bis zu **EUR 10 Mio**. bzw. 2 % des weltweiten (Konzern-) Jahresumsatzes (§ 45 Abs 2 NISG)
- Für Leitungsorgane sind keine Verwaltungsstrafen vorgesehen. Eine Verletzung der Pflichten der Leitungsorgane kann jedoch zu Schaden-ersatzansprüchen führen, wenn ein Leitungsorgan sorgfaltswidrig gehandelt hat und dies für den Eintritt eines Schadens ursächlich war.

CleverData
WORLD OF BUSINESS SOLUTIONS

NICHTEINHALTUNG VON VERPFLICHTUNGEN DURCH STELLEN DER ÖFFENTLICHEN VERWALTUNG

- Keine Geldstrafen: Im Gegensatz zu privaten Unternehmen sieht das Gesetz für Behörden und Stellen der öffentlichen Verwaltung keine Verwaltungsstrafen (Geldstrafen) vor
- Verfahren bei Verstößen: Stellt die Cybersicherheitsbehörde Mängel fest, erfolgt eine Anzeige bei der zuständigen Bezirksverwaltungsbehörde
- Feststellungsbescheid: Die Bezirksverwaltungsbehörde stellt die Nichteinhaltung der gesetzlichen Verpflichtungen mittels Bescheid förmlich fest
- Fristsetzung zur Behebung: In diesem Bescheid wird der Behörde eine angemessene Frist eingeräumt, um den rechtmäßigen Zustand herzustellen (Mängelbehebung)

NICHTEINHALTUNG VON VERPFLICHTUNGEN DURCH STELLEN DER ÖFFENTLICHEN VERWALTUNG

- Sanktion durch Veröffentlichung: Wird der Mangel nicht fristgerecht behoben, kann die Behörde verpflichtet werden, den Verstoß öffentlich bekannt zu machen (z. B. auf der Webseite oder via Medien)
- Politischer Druck statt Bußgeld: Da Geldstrafen im öffentlichen Bereich oft nur eine „Budgetumverteilung" wären, setzt der Gesetzgeber auf öffentliche Transparenz als wirksames Korrektiv
- Schutz der nationalen Sicherheit: Eine Veröffentlichung unterbleibt zwingend, wenn dadurch die öffentliche Ordnung oder die nationale Sicherheit gefährdet würde

CleverData
WORLD OF BUSINESS SOLUTIONS

RELEVANTE GESETZESSTELLEN

§ 31 NISG 2026 – Governance

- (1) Die Leitungsorgane wesentlicher und wichtiger Einrichtungen haben die Einhaltung der Risikomanagementmaßnahmen gemäß § 32 sicherzustellen und zu beaufsichtigen.

- (2) Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen an für diese spezifisch gestalteten Cybersicherheitsschulungen teilnehmen. Die Einrichtungen haben den Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, damit diese ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste erwerben können.

DIE VERANTWORTUNG DER LEITUNGSORGANE

NISG – Führungsposition aufgrund:

1. der Befugnis zur Vertretung der juristischen Person oder der eingetragenen Personengesellschaft,

2. der Befugnis, Entscheidungen im Namen der juristischen Person oder der eingetragenen Personengesellschaft zu treffen, oder

3. einer Kontrollbefugnis innerhalb der juristischen Person oder der eingetragenen Personengesellschaft

VERWALTUNGSÜBERTRETUNGEN, Z.B.

- Fehlende Cybersicherheitsschulungen für Leitungsorgane oder Mitarbeiter
- Fehlende Risikomanagementmaßnahmen gemäß § 32 NISG
- Unterlassene Meldung eines erheblichen Cybersicherheitsvorfalls
- Mangelhafte Berichterstattung im Fall eines erheblichen Cybersicherheitsvorfalls
- Verstöße gegen die Registrierungspflicht
- Verstöße gegen die Pflicht zur Selbstdeklaration
- Verstöße bei behördlichen Überprüfungen / Aufsichtsmaßnahmen

CleverData
WORLD OF BUSINESS SOLUTIONS

AUFSICHTSBEHÖRDE

- Bundesamt für Cybersicherheit gem. § 3a NISG 2026
- dem Innenminister direkt nachgeordnet, Leitung durch Direktor/in
- organisatorisch außerhalb der Generaldirektion für öffentliche Sicherheit, bundesweite Zuständigkeit
- Sitz in Wien, ggf. Außenstellen
- Weisungen des Bundesministers für Inneres sind schriftlich zu erteilen, zu begründen und in einem halbjährlichen Bericht zu veröffentlichen
- ab Inkrafttreten des NISG 2026, demnach **1.10.2026**

CleverData
WORLD OF BUSINESS SOLUTIONS

BEHÖRDLICHE AUFSICHT NACH DEM NISG

2 Aufsichtssysteme

- Vollwertige Aufsicht (ex ante & ex post) für wesentliche Einrichtungen
- Abgeschwächte Aufsicht (ex post) für wichtige Einrichtungen

CleverData
WORLD OF BUSINESS SOLUTIONS

AUFSICHTSMAßNAHMEN – WICHTIGE EINRICHTUNGEN

Bei mutmaßlichen Verstößen, insbesondere beim Risikomanagement und den Meldepflichten, kann die Cybersicherheitsbehörde die Aufsichtsmaßnahmen auch gegenüber wichtigen Einrichtungen setzen.

- Umsetzung der Risikomanagementmaßnahmen (Vor-Ort und remote)
- Durchführung von Sicherheitsscans
- Anforderung von Informationen über Risikomanagementmaßnahmen, einschließlich Cybersicherheitskonzepten
- Anforderung des Zugangs zu Daten, Dokumenten, sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind

Quelle: § 38. (1) Z 1 – 4 NISG 2026

CleverData
WORLD OF BUSINESS SOLUTIONS

FRISTEN

23.12.2025	Datum der Kundmachung des NISG 2026
01.10.2026	Inkrafttreten des NISG 2026, NISG tritt am 30.9.2026 außer Kraft Risikomanagementmaßnahmen inklusive Sicherheit der Lieferkette, Meldepflichten, Aufsicht- und Durchsetzungsmaßnahmen der Behörde möglich
01.01.2027	Ende der Frist zur Registrierung der Einrichtungen
01.10.2027	Ende der Frist zur Selbstdeklaration
01.10.2028	Frühestes Datum zur Aufforderung zur Prüfung durch NIS-Behörde
30.09.2030	Frühester Zeitpunkt zu dem wichtige Einrichtung Prüfbericht durch unabhängige Stelle nachzuweisen hat; jeweils nur nach Aufforderung; wichtige Einrichtungen nur bei begründeten Hinweisen (ex-post-Prüfung)

CleverData
WORLD OF BUSINESS SOLUTIONS

HANDLUNGSBEDARF „WIR WERDEN“

RISIKOMANAGEMENT

§ 32 NISG 2026 ABS. 1

Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

CleverData
WORLD OF BUSINESS SOLUTIONS

RISIKOMANAGEMENT

§ 32 NISG 2026 ABS. 2

Die Risikomanagementmaßnahmen haben zudem unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen sowie bewährter Verfahren und der Kosten der Umsetzung ein Cybersicherheitsniveau zu gewährleisten, das dem bestehenden Risiko angemessen ist.

CleverData
WORLD OF BUSINESS SOLUTIONS

RISIKOMANAGEMENT

ERW. 81 NIS2

Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Risikomanagementmaßnahmen im Bereich der Cybersicherheit in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand und gegebenenfalls europäischen oder internationalen Normen sowie den Kosten ihrer Umsetzung Rechnung getragen.

RISIKOMANAGEMENT

§ 32 NISG 2026 ABS. 3

Bei der Beurteilung der Verhältnismäßigkeit der Risikomanagement-maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

CleverData
WORLD OF BUSINESS SOLUTIONS

RISIKOMANAGEMENT ("ALL-HAZARDS-APPROACH")

- Allgefahrenansatz, Gefahrenübergreifender Ansatz oder Umfassender Risikomanagementansatz)
- **Ganzheitlich**: umfasst das gesamte Spektrum von natürlichen Gefahren (z. B. Stürme, Pandemien), Terrorismus, IT-System-versagen oder kriegerischen Handlungen.
- Die Risikoanalyse muss alle potentiellen Gefahrenarten berücksichtigen

CleverData
WORLD OF BUSINESS SOLUTIONS

RISIKOMANAGEMENT

§ 32 ABS. 4 NISG 2026

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Cybersicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette […]

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

CleverData
WORLD OF BUSINESS SOLUTIONS

RISIKOMANAGEMENT

§ 32 ABS. 4 NISG 2026

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

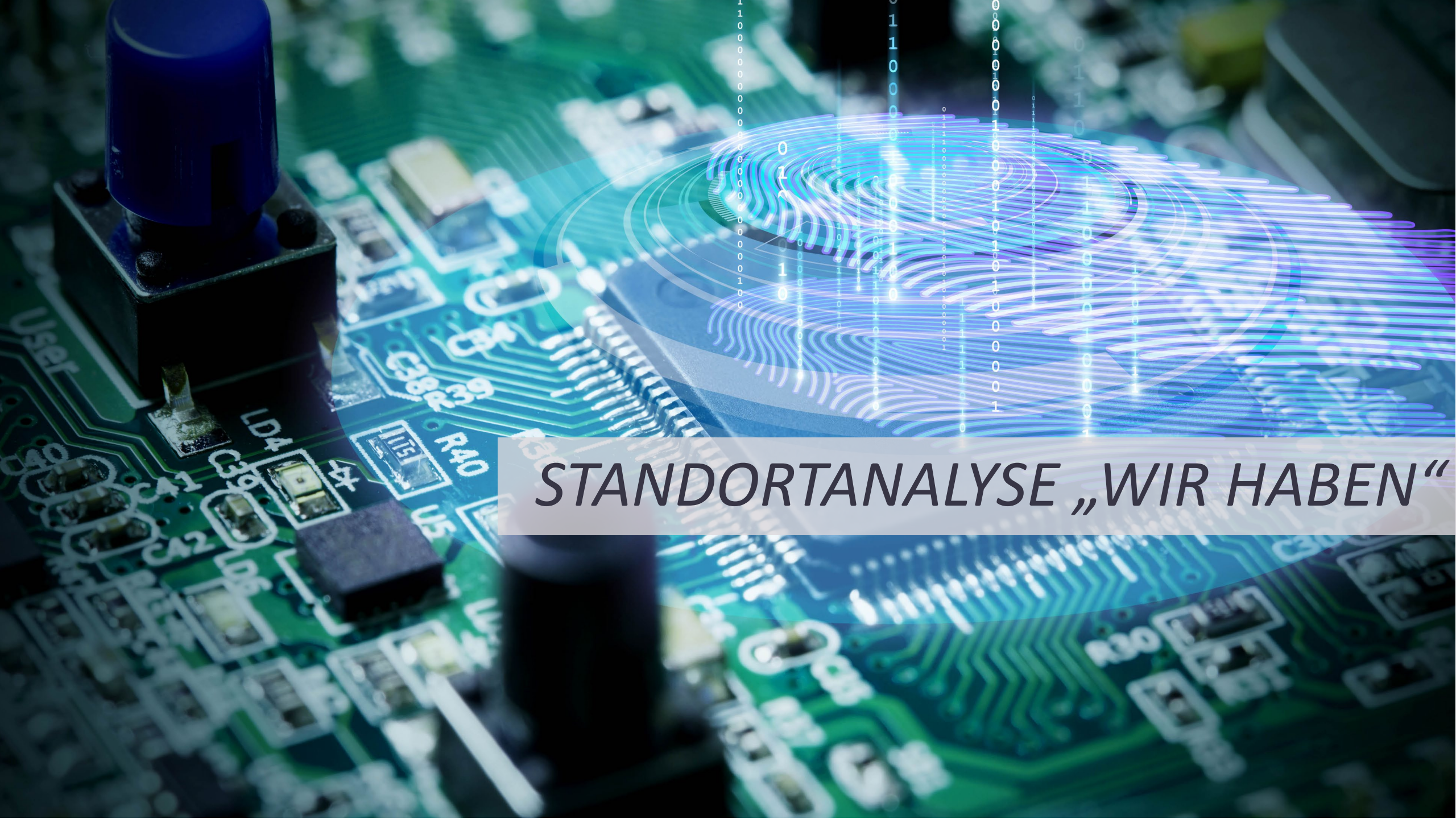
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

RISIKOMANAGEMENTMAßNAHMEN

- DURCHFÜHRUNGSVERORDNUNG (EU) **2024/2690** DER KOMMISSION vom 17. Oktober 2024
- (fast) allumfassend
- Kann als Vorgabe angesehen werden
- **JEDOCH**: Die Cybersicherheitsbehörde kann durch Verordnung nähere Anforderungen an die Risikomanagementmaßnahmen festlegen. (§ 32 Abs. 5 NISG 2026)

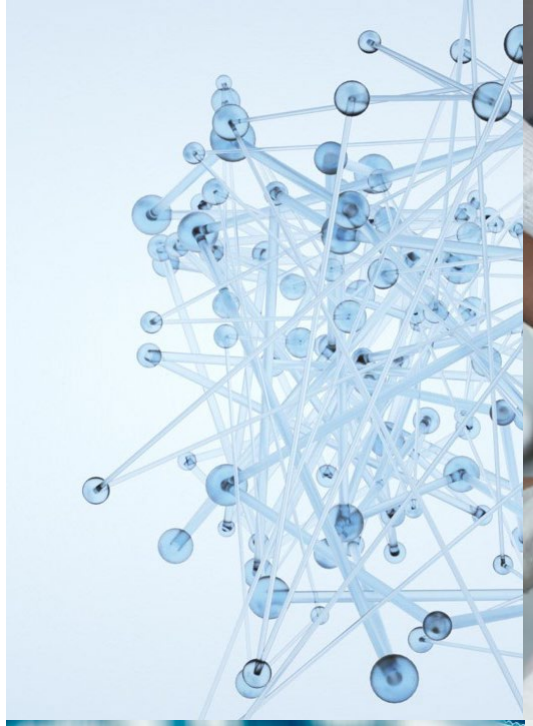
CleverData
WORLD OF BUSINESS SOLUTIONS

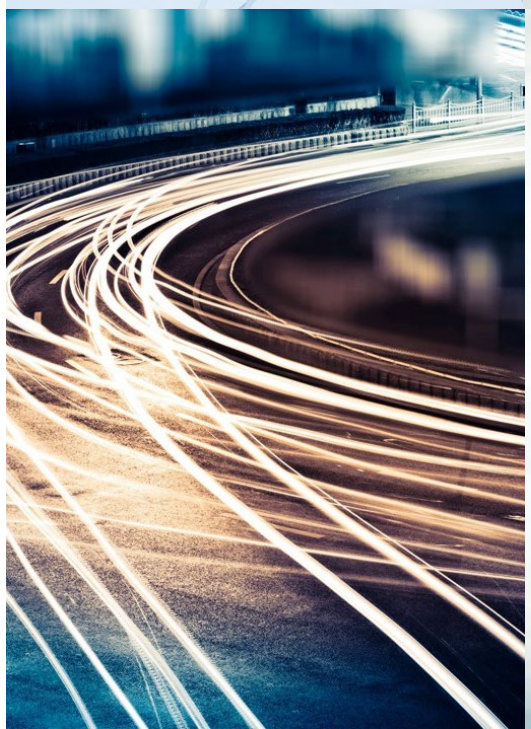


STANDORTANALYSE „WIR HABEN“

VORFRAGEN

- Was ist die Kernaufgabe der jeweiligen Einrichtung?
- Wofür steht die Organisation?
- Was "muss" immer funktionieren?
- Erkenntnis von Abhängigkeiten (Kausalketten, Betriebsnotwendigkeiten, Logistik, Produktion, Verkauf), vor allem von IT
- Was kann passieren und die Geschäftstätigkeit stören?

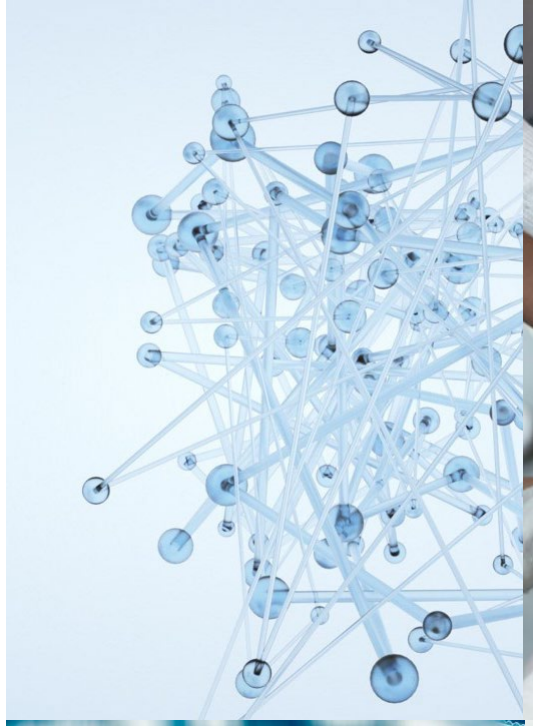


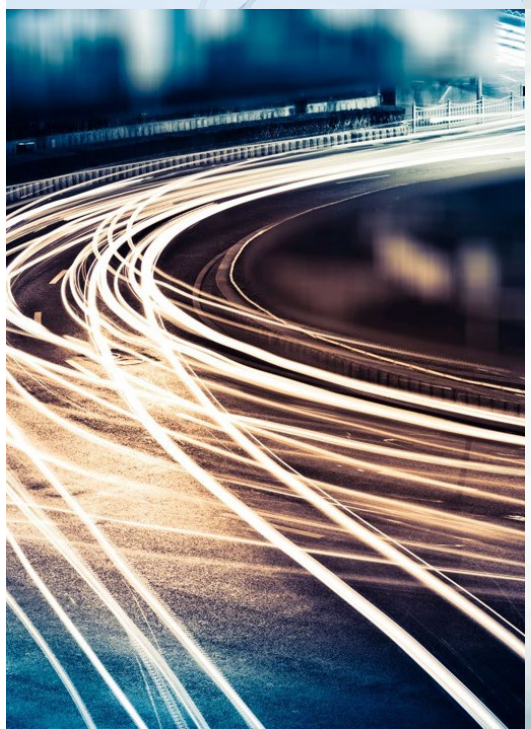


VORFRAGEN

- Daraus soll abgeleitet werden können, was die schlimmsten Auswirkungen (auf die Einrichtung oder deren Kunden) bei Ausfall von IT wären.
- Welche Maßnahmen können getroffen werden, um die Risiken zu verringern?
- Welche Maßnahmen erscheinen wirtschaftlich sinnvoll und angemessen?
- (Diese Risiken und Maßnahmen sind regelmäßig zu aktualisieren und zu dokumentieren.)

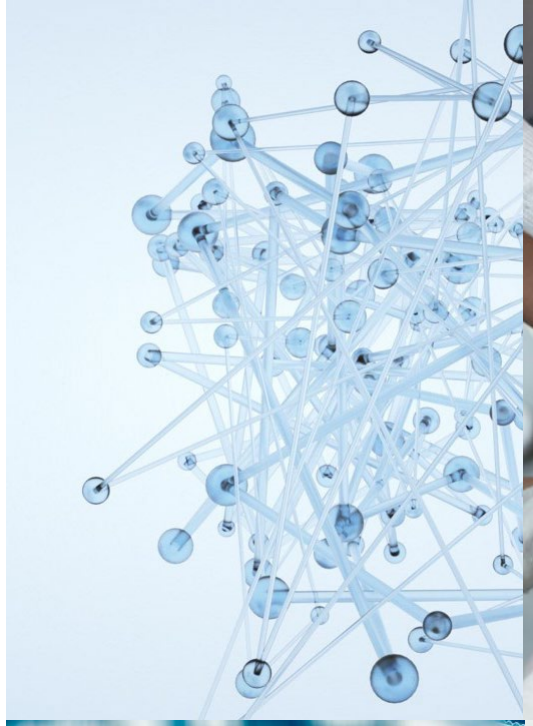
CleverData
WORLD OF BUSINESS SOLUTIONS

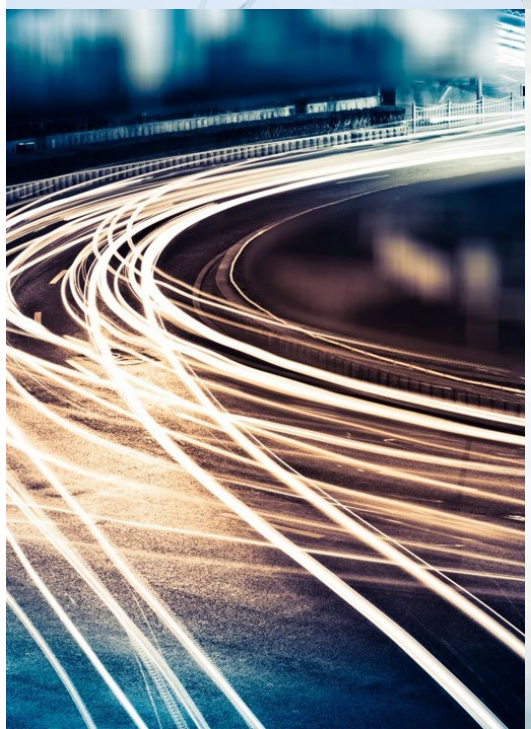




ZUSTÄNDIGKEITSFRAGEN

- Informationssicherheit
- Wer kümmert sich in der Einrichtung um Informationssicherheit?
- Ist jemand damit beauftragt?
- Gibt es ein aktuelles Informations-Sicherheits-Regelwerk? (z.B. Informationssicherheitsrichtlinie)





KERNAUFGABEN

- *RISIKOANALYSE*
- *IT RISIKEN MANAGEN*
- *BIA (BUSINESS IMPACT ANALYSE)*

Vorgeschrieben ist die Durchführung einer konkreten Risikoanalyse, über deren Ergebnis auch in der Selbstdeklaration an die Behörde zu berichten ist (§ 33 NISG).

CleverData
WORLD OF BUSINESS SOLUTIONS

KATALOG DER ELEMENTAREN GEFÄHRDUNGEN (QUELLE: BSI DEUTSCHLAND) – BEISPIELE

G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- oder Software
G 0.22	Manipulation von Informationen
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.24	Zerstörung von Geräten oder Datenträgern
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.27	Ressourcenmangel

CleverData
WORLD OF BUSINESS SOLUTIONS

BUSINESS IMPACT ANALYSE (BIA)

- Auswirkungen auf die Erbringung wesentlicher Dienste
- Auswirkungen auf Gesundheit und Sicherheit von Personen
- Auswirkungen auf die Bevölkerung
- Auswirkungen auf öffentliche Ordnung und Verwaltung
- Auswirkungen auf andere kritische Einrichtungen
- Verfügbarkeit, Integrität und Vertraulichkeit von Informationen
- Reputationsschäden und rechtliche Konsequenzen

BUSINESS IMPACT ANALYSE (BIA) – BEISPIEL (GEMEINDE)

Prozess	Wesentliche Assets	Business Impact	Begründung
Trinkwasserversorgung	Pumpwerke, SPS-Steuerungen, Brunnenanlagen, Fernwirktechnik	sehr hoch	Ausfall kann die Versorgung der Bevölkerung mit Trinkwasser beeinträchtigen. Erhebliche Auswirkungen auf Gesundheit und öffentliche Sicherheit.
Abwasserentsorgung	Pumpstationen, Kläranlage, Steuerungssysteme	sehr hoch	Mögliche Umwelt- und Gesundheitsgefährdung sowie Beeinträchtigung kritischer Infrastruktur.
IT-Betrieb / EDV	Server, Netzwerk, Firewall, Backup-Systeme, Fachanwendungen	sehr hoch	Querschnittsfunktion. Ausfall betrifft nahezu alle Verwaltungs- und Versorgungsprozesse.
Soziale Einrichtungen	Fachanwendungen, Gesundheitsdaten, IT-Infrastruktur	mittel	Betroffenheit schutzbedürftiger Personen, hohe Anforderungen an Verfügbarkeit und Datenschutz.
Meldewesen / Bürgerservice	ZMR-Zugang, Fachverfahren, Telefonie, IT-Infrastruktur	mittel	Gesetzliche Aufgaben können nicht erfüllt werden; erhebliche Auswirkungen auf Bürgerinnen und Bürger.
Personalverrechnung	Personalsoftware, Personaldaten	mittel	Verzögerungen bei Gehaltszahlungen, jedoch meist kurzfristig beherrschbar.
Rechnungswesen	Buchhaltungssysteme, Zahlungsverkehr	gering bis mittel	Verzögerungen bei Zahlungen und Budgetvollzug.
Bauhof	Fahrzeuge, Einsatzplanung, Kommunikationsmittel	gering bis mittel	Einschränkungen bei Winterdienst und Infrastrukturbetreuung.
Allgemeine Verwaltung	Büroarbeitsplätze, Dokumentenmanagement	gering bis mittel	Organisatorische Beeinträchtigungen, jedoch oft kompensierbar.
Bauamt	Fachanwendungen, Akten	gering	Verzögerungen bei Verfahren, meist keine unmittelbaren Auswirkungen auf die Daseinsvorsorge.
Gemeindewohnungen	Verwaltungssoftware, Vertragsdaten	gering bis mittel	Abhängig von Anzahl der Wohneinheiten und technischen Einrichtungen.
Datenschutzkoordination	Personenbezogene Daten, Verzeichnis der Verarbeitungstätigkeiten	mittel	Erhöhte Compliance- und Haftungsrisiken, jedoch keine unmittelbare Gefährdung der Versorgung.

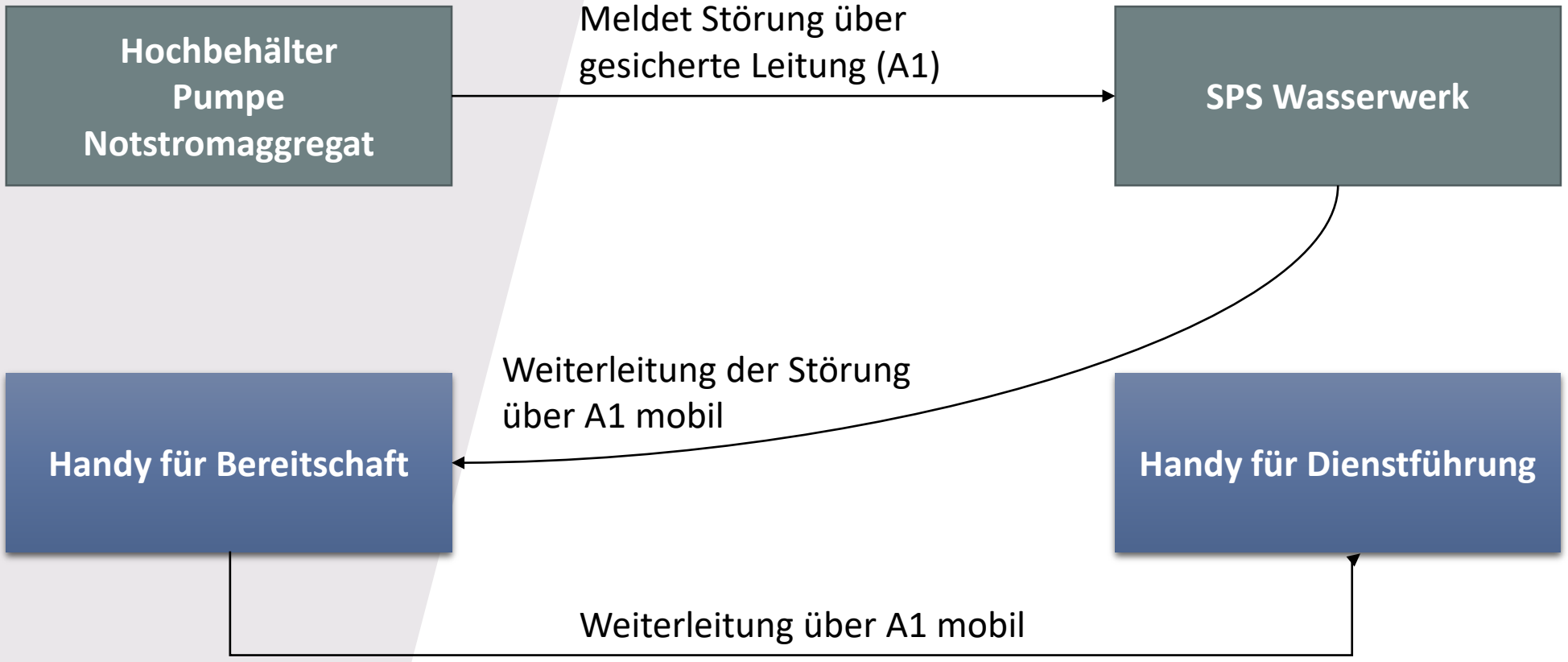
BUSINESS IMPACT ANALYSE (BIA) – BEISPIEL (GEMEINDE)

Prozess	Impact	Max. tolerierbare Ausfallzeit	Wiederherstellungsziel
Trinkwasser	sehr hoch	8 Stunden	4 Stunden
Abwasser	sehr hoch	8 Stunden	4 Stunden
IT-Betrieb	sehr hoch	24 Stunden	8 Stunden
Soziale Einrichtungen	mittel	1 Arbeitstag	1 Arbeitstag
Meldewesen	mittel	1 Arbeitstag	1 Arbeitstag

ASSETS – BEISPIEL WASSERWERK

- Diensthandy für Bereitschaft
- Datenübertragung von der Anlage zum Diensthandy
- Fahrzeuge
- Alarmanlagen
- Rechner, Drucker, Netzwerk(e)
- Pumpen, Notstromaggregat, Niveaustandsmessung, Ventile, Hochbehälter, etc.
- Diverse Software zur Steuerung und Messung

RISIKEN AM BEISPIEL WASSERWERK
WAS KANN PASSIEREN?



CleverData
WORLD OF BUSINESS SOLUTIONS

EQUIPMENT „WIR BENÖTIGEN“

MAßNAHMEN

- Interdisziplinäres NIS-2-Steuerungsteam bilden
- Regelmäßiges Reporting an die oberste Leitung sicherstellen und Reporting-Vorlagen definieren
- Externe Dienstleister und Behörden frühzeitig einbinden
- Meldepflichten - Meldeketten aufbauen
- Vollständige Verfahrens-, Maßnahmen- und Entscheidungsdokumentation anlegen
- Notwendigkeit eines aktuellen (!) Verzeichnisses über alle IT-Systeme, Anwendungen und der Daten der Organisation

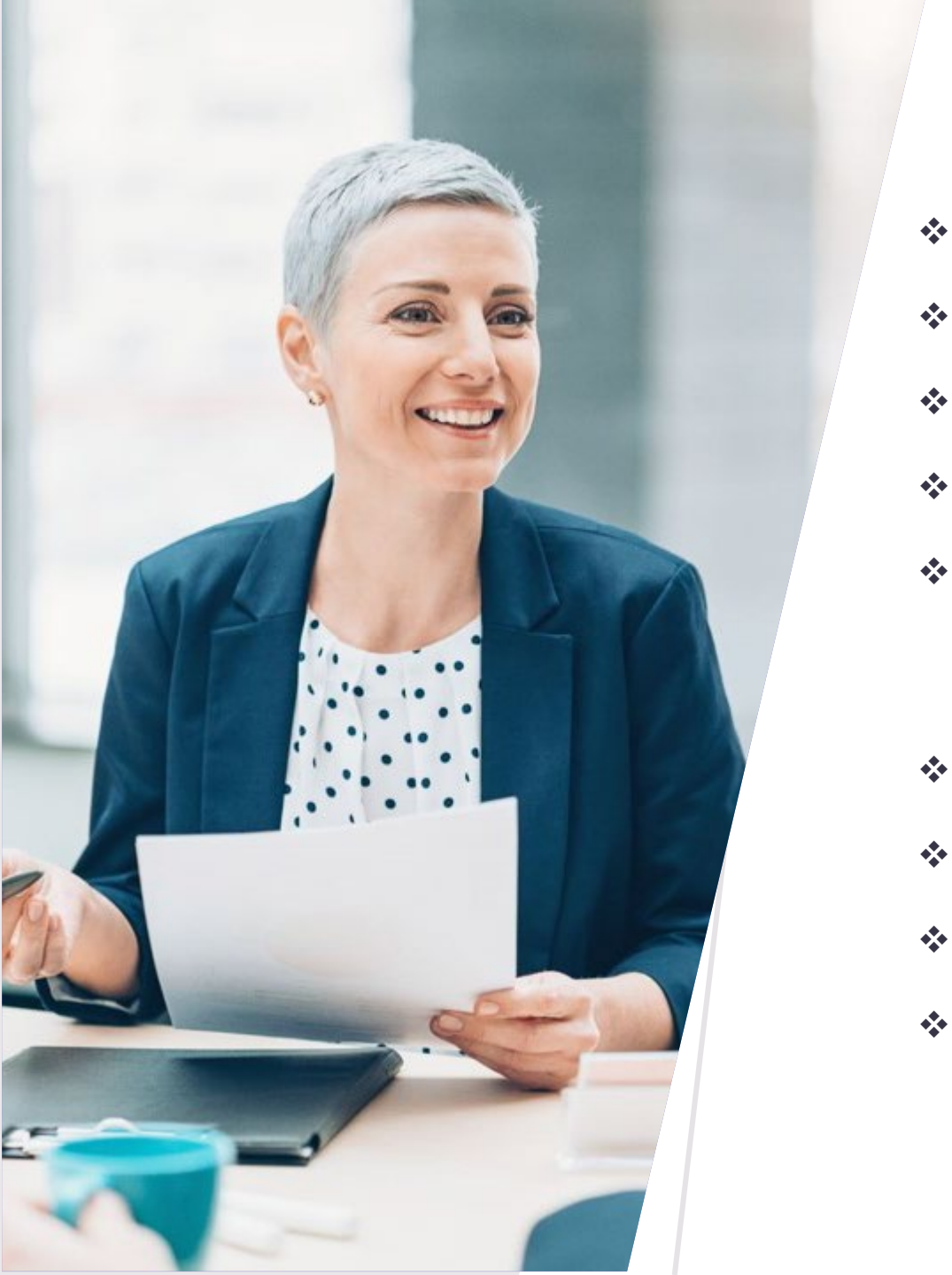
CleverData
WORLD OF BUSINESS SOLUTIONS

MAßNAHMEN

- Nachweisführung für Aufsichtsbehörden vorbereiten
- Drittparteimanagement einführen
- Sicherheitsanforderungen an Dienstleister und Lieferanten definieren (Nachweise für die Sicherheit von Dienstleistern und Lieferanten?)
- Automatisierte Monitoring- und Alarmierungssysteme einführen
- Krisenstab (Situationsbewältigung, Umgang mit den Konsequenzen des Angriffes)
- Krisenbudgets

CleverData
WORLD OF BUSINESS SOLUTIONS

MILESTONES „WIR KÖNNEN!“



UMSETZUNG

- individueller Meilensteinplan – „Ziel / Zeitrahmen“
- Quick Wins
- Technologische Altlasten reduzieren
- Qualitätskontrollen festlegen
- Security Awareness Training – machen Sie Ihre Mitarbeiter zum ersten Schutzschild gegen Cyberbedrohungen (§ 31 Abs 2 NISG - Schulungsangebot)
- Security-Champions-Programme
- Verstetigung & kontinuierliche Verbesserung
- Lessons Learned etablieren
- Schulung nach § 31 Abs 2 NISG der Leitungsorgane

CleverData
WORLD OF BUSINESS SOLUTIONS

FAZIT I

Fast jeder hohe und mittlere Risiko-Auslöser lässt sich auf ein Defizit in der IT-Hygiene zurückführen.

Technische Angriffe gelingen meistens nur deshalb, weil im Vorfeld menschliche Fehler (Klick auf Phishing) oder organisatorische Versäumnisse (fehlende Updates/MFA) die Tür offengelassen haben.

CleverData
WORLD OF BUSINESS SOLUTIONS

FAZIT II

Die wirksamste Einzelmaßnahme mit dem größten Hebel ist die flächendeckende Einführung von Mehrfaktor-Authentifizierung (MFA) in Kombination mit dem Entzug von lokalen Administrator-Rechten für die Endanwender.

Damit sperrt man bereits den Großteil aller automatisierten Angriffe effektiv aus.

CleverData
WORLD OF BUSINESS SOLUTIONS

FAZIT III (LEIDER)

Eine 100%ige Sicherheit ist dennoch nicht erreichbar.

CleverData
WORLD OF BUSINESS SOLUTIONS

NÄCHSTE SCHRITTE

1. Status-Quo-Aufnahme: Fragebogen bearbeiten und vorhandene Maßnahmen dokumentieren.
2. Abweichungsanalyse (Gaps): Nicht angemessene/durchführbare Anforderungen identifizieren und deren Nichtumsetzung nachvollziehbar begründen und dokumentieren.
3. Risikomanagement: Identifizierte Gaps bewerten und in einen Risikobehandlungsplan überführen.
4. Richtlinienerstellung & Anpassung: Dokumente unter Einbeziehung der Lieferkettensicherheit und technischer Standards anhand der Mustervorlagen erstellen und intern/(ggf.) extern kommunizieren.
5. Governance & Awareness: Formelle Billigung der Maßnahmen durch die oberste Leitung einholen sowie Schulungsprogramme für Personal und Management starten.
6. Compliance-Monitoring: Einhaltung laufend prüfen.

FRAGEN?

VIELEN DANK!

clever data gmbh

Danhausergasse 9/Top 3
1040 Wien
Tel.: +43 664 61415 23
Fax.: +43 664 61415 80

office@cleverdata.at

https://www.cleverdata.at

CleverData
WORLD OF BUSINESS SOLUTIONS