TD SYNNEX

Zero Trust for Everybody
Absicherung Ihrer Hyperscaler Architektur

ONE IDENTITY
by Quest

Ihre Gastgeber

Daniel
Gordon
Senior Principal Solution Engineer
OneLogin by OneIdentity | EMEA

daniel.gordon@oneidentity.com

+49 (0)171 317 8862

Frank
Siepmann
Manager Technical Services

Frank.Siepmann@tdsynnex.com

+49 (0) 175 727 0438

TD SYNNEX

Wolfgang
Rieger
Senior Business Development Manager
Security DACH

Wolfgang.rieger@tdsynnex.com

+49 (0) 175 727 0279

TD SYNNEX

Unsere Agenda

Daniel
Gordon
Senior Principal Solution Engineer
OneLogin by OneIdentity | EMEA

daniel.gordon@oneidentity.com

+49 (0)171 317 8862

- Zugriffssteuerung
  - IAM
  - PAM
  - Auditierbarkeit

Frank
Siepmann
Manager Technical Services

Frank.Siepmann@tdsynnex.com

+49 (0) 175 727 0438

TD SYNNEX

- Zero Trust for Everybody
- Konzepte

Wolfgang
Rieger
Senior Business Development Manager
Security DACH

Wolfgang.rieger@tdsynnex.com

+49 (0) 175 727 0279

TD SYNNEX

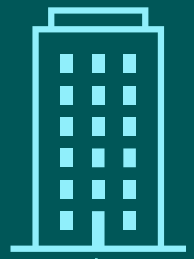
- Einleitung
- NIS2 & BSI
- Cyber Versicherung

Wer ist von NIS2 betroffen?

Alle öffentlichen und privaten Einrichtungen, aus 18 Sektoren.
Gültig ab **17.10.2024** (nationales Recht verspätet sich - NIS2UmsuCG)

50+ Mitarbeiter und/oder einem Jahresumsatz von >10Mio €

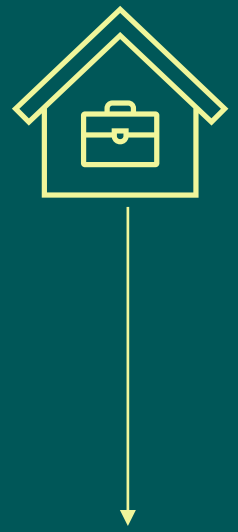
Große Unternehmen



ESSENTIAL ENTITITES

Ausnahmen von der Größenregel

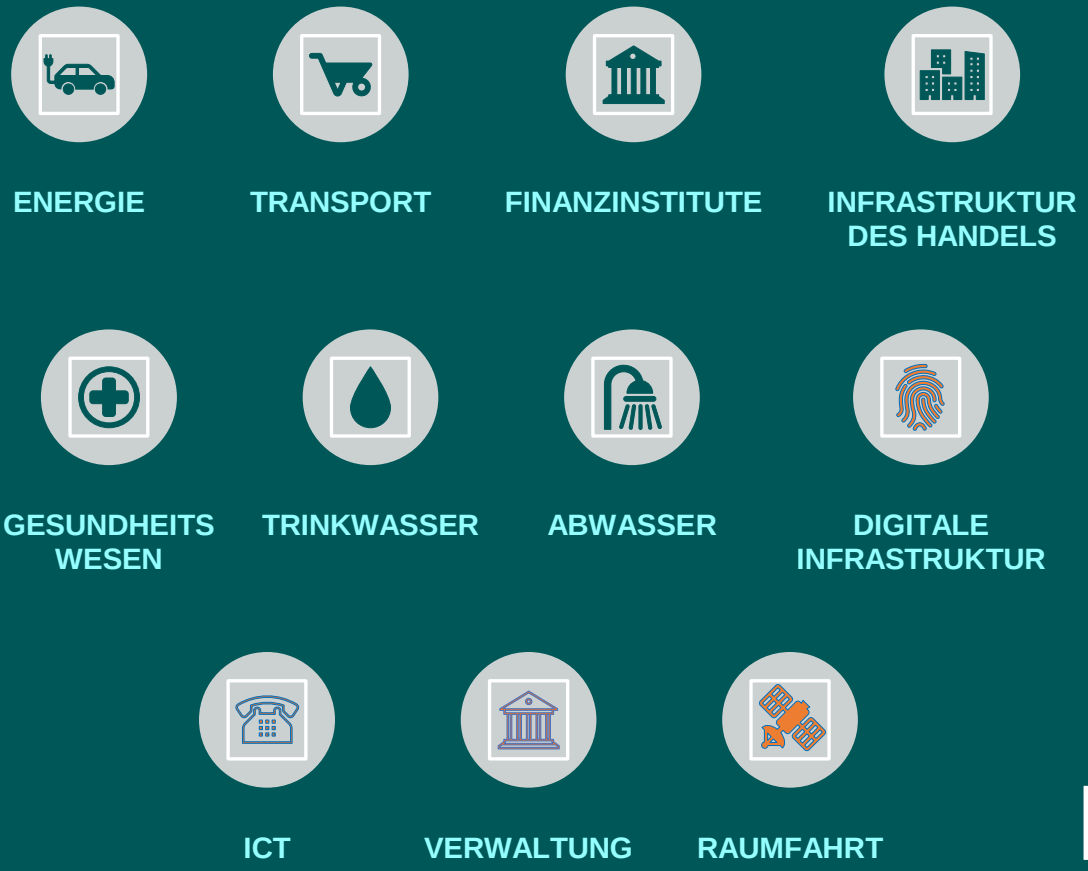
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder –dienste
- Domainnamen-Registries als DNS-Dienstanbieter
- Einziger Anbieter eines wesentlichen Dienstes in einem Mitgliedstaat
- Eine Störung des von der Einrichtung erbrachten Dienstes könnte erhebliche Auswirkungen auf die öffentliche Sicherheit, die öffentliche Sicherheit oder die öffentliche Gesundheit haben
- Bei der Einrichtung handelt es sich um eine Einrichtung der öffentlichen Verwaltung…



Mittelständische Unternehmen

Erweiterter Anwendungsbereich

Wesentliche Entitäten



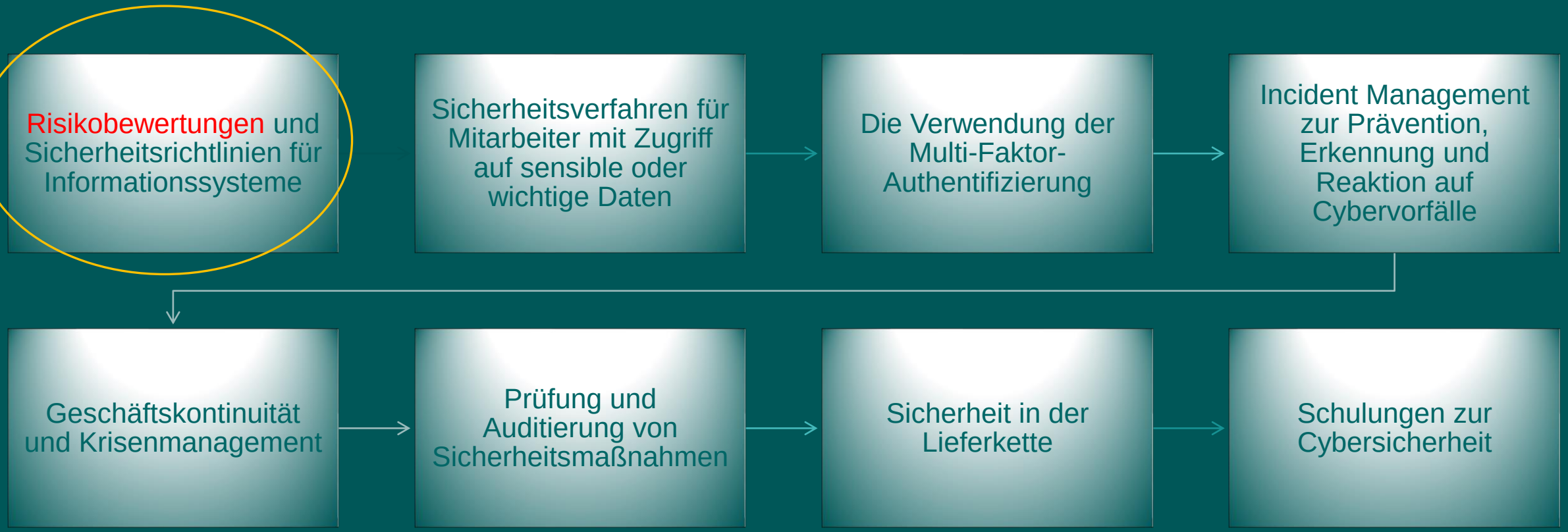
Wichtige Entitäten

und... alle Zulieferer für oben genannte Unternehmen.

BSI - NIS-Richtlinien (bund.de)

Risikomanagement und Sicherheitsmaßnahmen NIS2

Mindestmaßnahme, an die sich alle Organisationen halten müssen.



Risikomanagement und Sicherheitsmaßnahmen NIS2

Risikobewertung – wo setzt man an, was ist zu bedenken?

- ✓ **Policies** Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
- ✓ **Vorfallbewältigung** Erkennung, Analyse, Eindämmung und Reaktion auf Vorfälle
- ✓ **Business Continuity** Backup-Management und Wiederherstellung, Krisenmanagement
- ✓ **Supply Chain** Sicherheit in der Lieferkette
- ✓ **Einkauf** Sicherheit bemi Erwerb, Entwicklung / Wartung der IT-Systeme, inkl. Management (Offenlegung von Schwachstellen)
- ✓ **Wirksamkeit** Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- ✓ **Cyberhygiene**, Schulung Cyberhygiene (z.B. Updates) und Schulungen in Cyber Security
- ✓ **Kryptografie** Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- ✓ **Access Management** Assets Personalsicherheit, **Zugriffskontrolle** und Asset Management
- ✓ **Authentifizierung** **Multi-Faktor-Authentifizierung** oder kontinuierliche Authentifizierung
- ✓ **Kommunikation** Sichere Sprach-, Video- und Text-Kommunikation, ggf. auch im Notfall

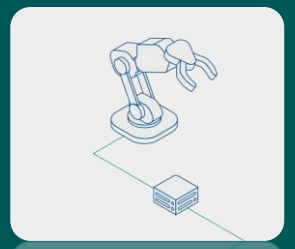
Voraussetzungen für eine Cyberversicherung

Preparing for Cyber Insurance: The Top 10 Essential Steps (oneidentity.com)

- ✓ **Patch-Management**
- ✓ **MFA**
- ✓ **Encryption (Data, Mail etc.)**
- ✓ **PAM**
- ✓ **Backup and Recovery**
- ✓ **Assessment (Zugriffsrechte, Mover, Joiner, Leaver)**
- ✓ **AD Schutz (Authentication + Authorization)**
- ✓ **Risk-based Authentication z.B. OneLogin**
- ✓ **Pentesting**
- ✓ **Notfallpläne**

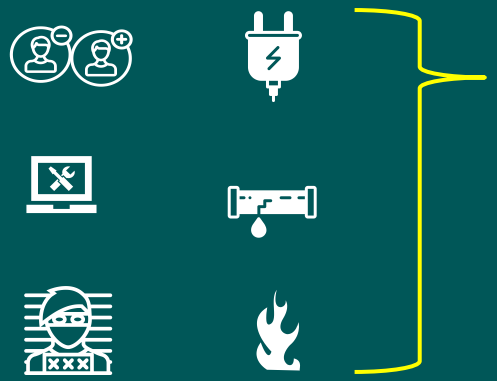
Schutzbedarf der Informationssysteme mittels Risikobewertung

TD SYNNEX



Wie wichtig ist der zu schützende Gegenstand?



+

Welche Bedrohungen gibt es?

+

Welcher Schaden kann entstehen?

+

Die Wahrscheinlichkeit eines Schadens?

⬇

Risikoklassen definieren

3 - 2 - 1 - 0

Häufigkeit des Schadens	5				€€€	
	4					
	3					
	2					
	1					
Problem	Kritisch	1	2	3	4	5
Akzeptabel	Problem					Höhe des Schadens

RISIKOKLASSE 0	**SEHR HOHES RISIKO** Sehr hoher Schutzbedarf
RISIKOKLASSE 1	**HOHES RISIKO** Hoher Schutzbedarf
RISIKOKLASSE 2	**MITTLERES RISIKO** Mittlerer Schutzbedarf
RISIKOKLASSE 3	**NIEDRIGES RISIKO** Niedriger Schutzbedarf

Risikobewertung lt. BSI
Minimum für Cyber Security Prozesse

TD SYNNEX

	Risikoklasse 3 Geringer Schutzbedarf	Risikoklasse 2 Normaler Schutzbedarf	Risikoklasse 1 Hoher Schutzbedarf	Risikoklasse 0 Sehr hoher Schutzbedarf
Physikalische Sicherheit	Öffentlich	Zugang nur für Befugte	Eintrittskontrolle, verschlossen	Überw…
Zugriffs- & Rechte-Management	Authentifizierung	Authentifizierung 2 Faktor	• Authentifi… • …	
Netzwerk, Daten und Kommunikation absichern	Abgrenzung zum Unternehmen (Guest Net)	Netze trennen und APT Schutz		…, Log Files …wachen, HA Umgebung, Echtzeit Verteidigung
Überwachung der Sicherheit	Regelmäßige Systemprüfung	Auf Security System Meldungen schnell reagieren	…erwachung aller …ysteme und Datenflüsse	Aktive Überwachung aller Systeme und Datenflüsse + SOC SOAR Team
Prozesse zur Verbesserung der Sicherheit	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung	Business Continuity Prozess härtet die Verteidigung

ONE IDENTITY by Quest

Bleiben Sie sicher!