COME baramundi
2GETHER

ENTDECKT
ERWEITERT
ENTLASTET

DriveLock

COME baramundi 2GETHER

Erweitern Sie Ihren Security-Horizont

Umfassende Absicherung Ihrer Daten und Schnittstellen mit DriveLock

Timo Stubel / DriveLock SE

AGENDA

COME baramundi 2GETHER

- Gesetze und Regularien
- Anatomie eines Angriffs
- Defense in Depth

DriveLock

COME baramundi 2GETHER

The Network and Information Security Directive 2

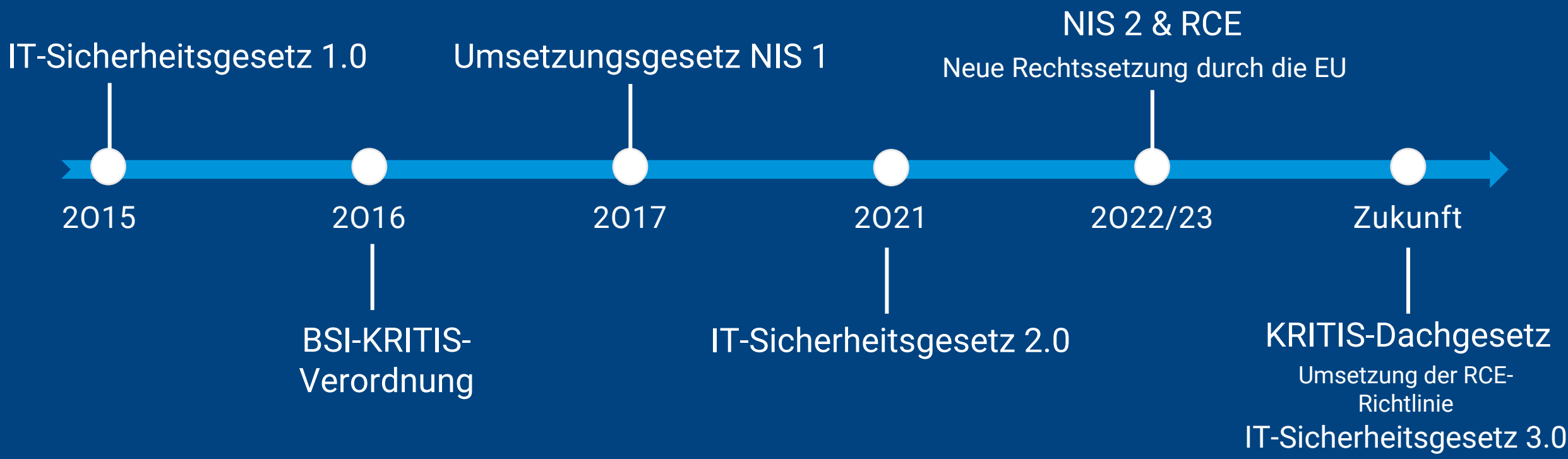
DriveLock

„Mit NIS 2 wird Cybersicherheit und -resilienz nun auch für die breite Masse der Unternehmen in Europa und damit auch in Deutschland zum Top THEMA.

André Glenzer, Partner bei pwc deutschland

DriveLock

Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit



NIS-2-Richtlinie (EU) 2022/2555

Anforderung an Risiko-Managementmaßnahmen (Art. 21 Abs. 1)

- Sicherheitsrisiken der Netz- und Informationssysteme monitoren
- Sicherheitsvorfälle verhindern bzw. deren Auswirkung minimieren
- Stand der Technik / einschlägigen Normen berücksichtigen
- Sicherheitsniveau an Risiko anzupassen
- Allgefahrenansatz einsetzen

Konkrete Maßnahmen (Art. 21 Abs. 2)

- Policies (Richtlinien)
- Incident Management
- Business Continuity
- Supply Chain
- Prevention & Detection
- Risk & Compliance
- DLP / Verschlüsselung
- Awareness
- Access Control
- Zero Trust

DriveLock

Critical Security Controls

Security Control	DriveLock Module
Inventory	
Media Protection	**Device Control**
Malware Defenses	**Application Control**
Secure Configuration	
Data Protection	**Encryption**
Security Awareness	**Security Awareness Campaigns**
Vulnerability Management	
Privilege Control	
Incident Response	

https://www.sans.org/blog/cis-controls-v8/
https://www.nist.gov/cyberframework

DriveLock

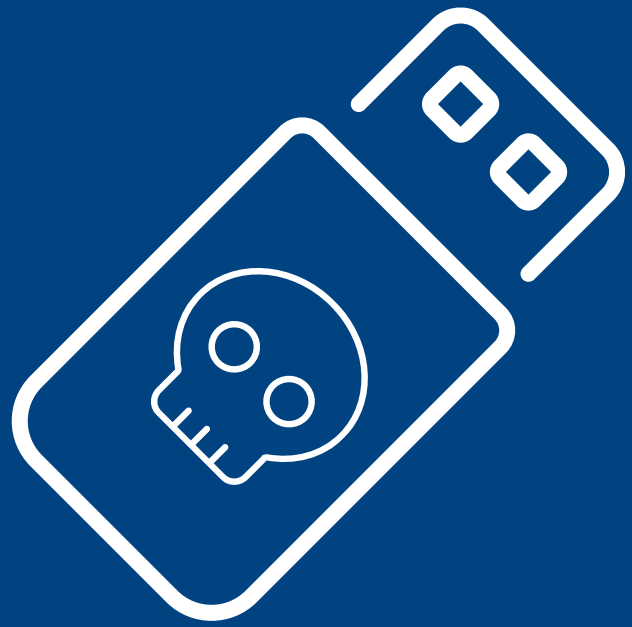
COME baramundi 2GETHER

USB ist tot – es lebe USB!

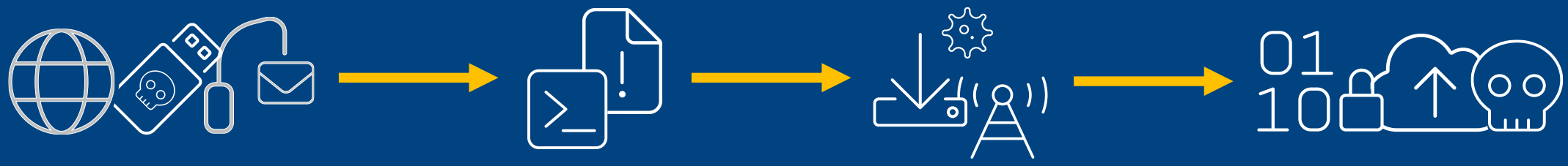
DriveLock

USB-Malware Angriffe

- Raspberry Robin
- Snowydrive
- USB-Borne
- Pteranodon



Raspberry Robin



Initial Access

Execution

Persistence

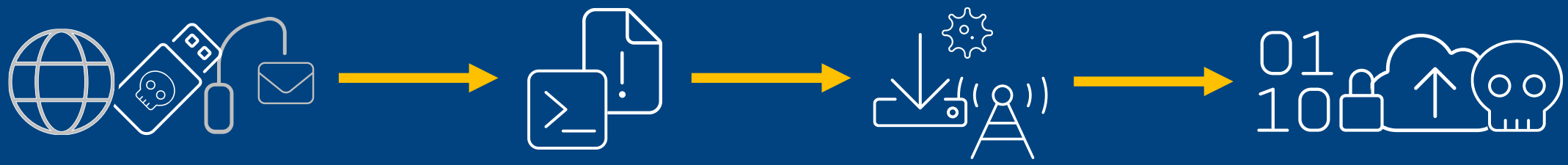
...

C&C

Exfiltration

Impact

Raspberry Robin



Verbreitung
via USB-Laufwerk

Ausführung per
Autorun.inf oder
LNK-Datei

Verwendung von msiexec,
odbcconf und fodhelper

Verwendung von
Run-Regkeys

C&C via TOR

Datendiebstahl

Verschlüsselung und
Erpressung

COME baramundi 2GETHER

Defense in Depth

DriveLock

Präventive Maßnahmenn

Szenario	Maßnahme
 Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	**Device Control**
 Infektion mit Schadsoftware über Internet und Intranet	**Application Control**
 Menschliches Fehlverhalten und Sabotage	**Security Awareness**

Application Control

Verteidigung Ihrer Systeme vor
bekannten und unbekannten Bedrohungen

Vollständiger Überblick über die
Anwendungen auf Ihren Systemen

Erfüllung von Compliance-Anforderungen
und regulatorische Standards

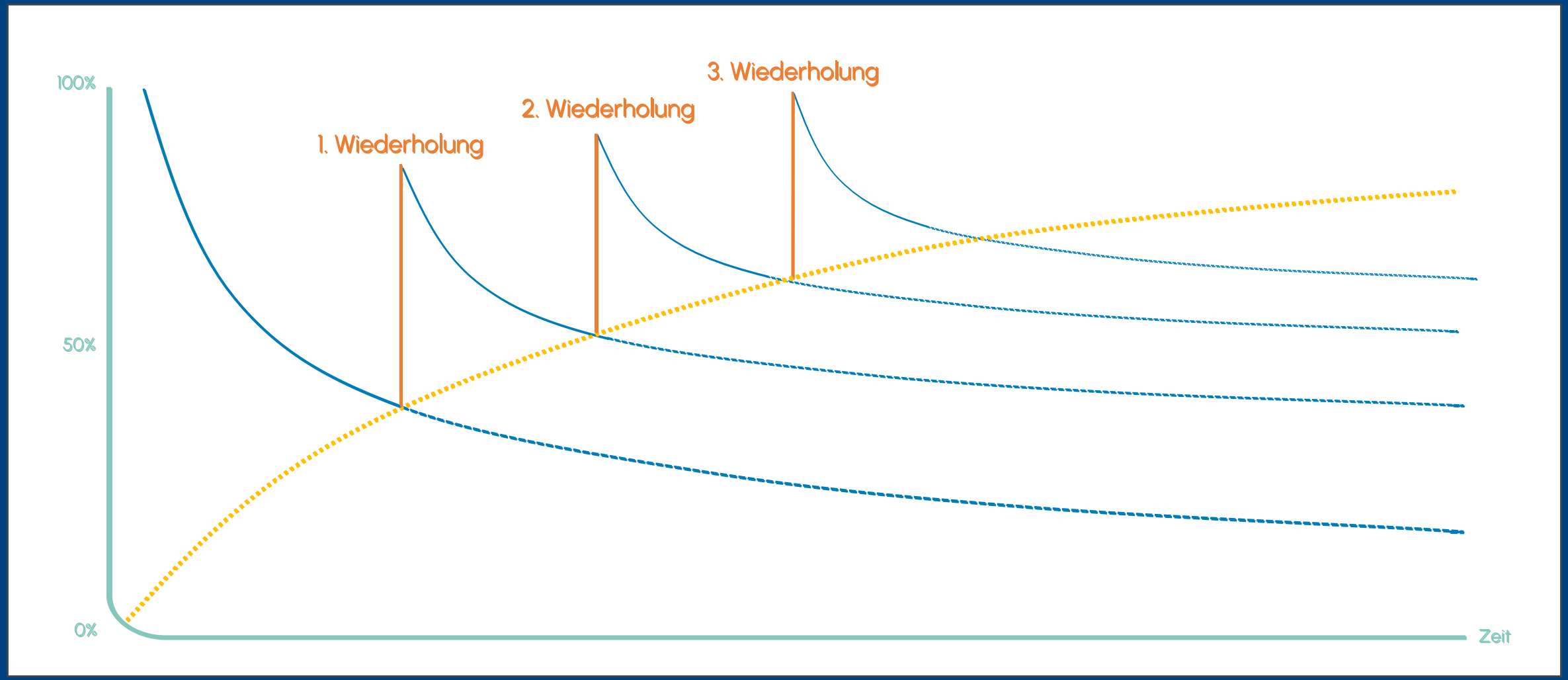
Device Control

Kontrolle aller Geräte und Laufwerke

Schutz vor Datendiebstahl und Schadsoftware

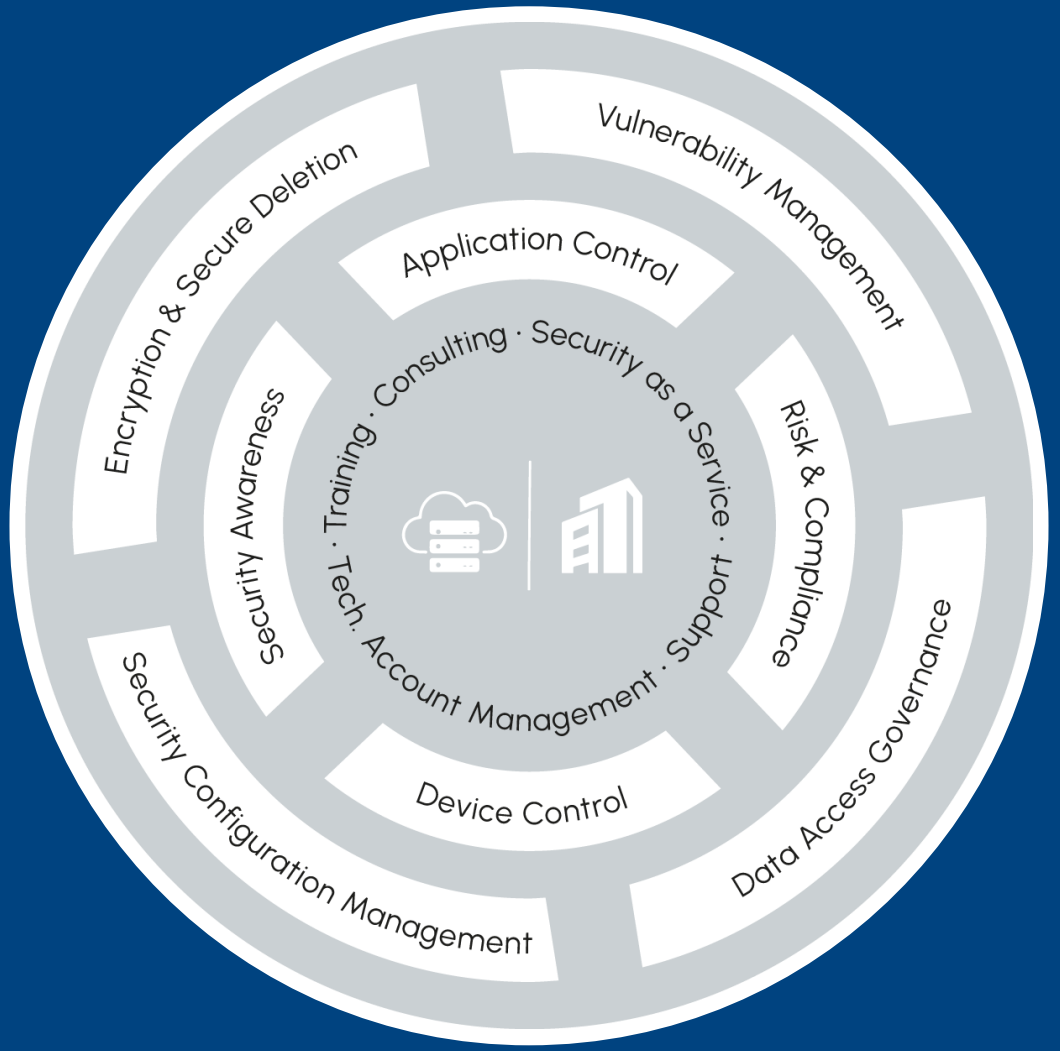
Transparenz über die Nutzung sämtlicher Peripherie

Security Awareness Schulungen



DriveLock

Zero Trust – Next Level



HYPERSECURE IT®

Platform

DriveLock

COME baramundi 2GETHER

Danke für die Aufmerksamkeit!

Timo Stubel

Senior PreSales Consultant

+49 170 346 08 60

Timo.Stubel@drivelock.com

+ Folgen

HYPERSECURE IT®

DriveLock