Verbund

Aus eigener Kraft.

„Gefordert. Ermöglicht. Bewiesen.“ – NIS 2, Quantenkryptografie und Cyber Range

Michael Hein
Wien
September 2026

Drei Uhren laufen gleichzeitig

1

IN WENIGEN WOCHEN

NIS2 wird Aufsichtsrecht

NISG 2026 tritt am 1. Oktober 2026 in Kraft. Selbstidentifikation, 24-Stunden-Meldung, persönliche Verantwortung der Leitungsorgane.

2

IN 10 BIS 15 JAHREN

Quantum: PQC statt QKD

Der Q-Day liegt in der Zukunft, das Abgreifen der Daten nicht. Was Physik verspricht und was Mathematik heute liefert.

3

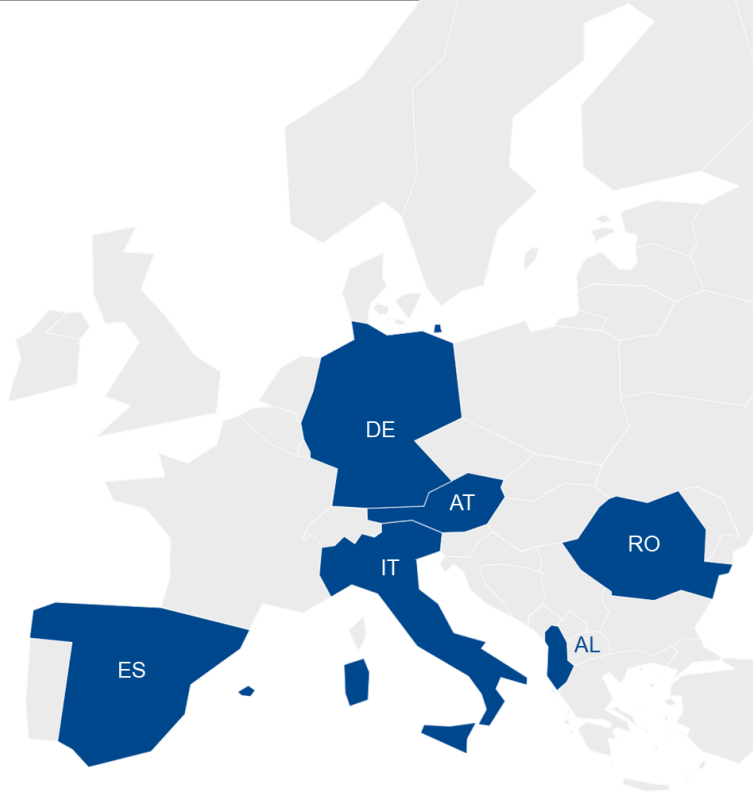
JEDERZEIT

Cyber Range als Realitätstest

Der Ernstfall fragt nicht nach Dokumenten. Übung erzeugt genau die Evidenz, die Prüfer später sehen wollen.

Für zwei dieser Uhren hat jemand anderes das Datum festgelegt. Die dritte stellen nur Sie selbst – und sie entscheidet, ob die ersten beiden etwas wert sind.

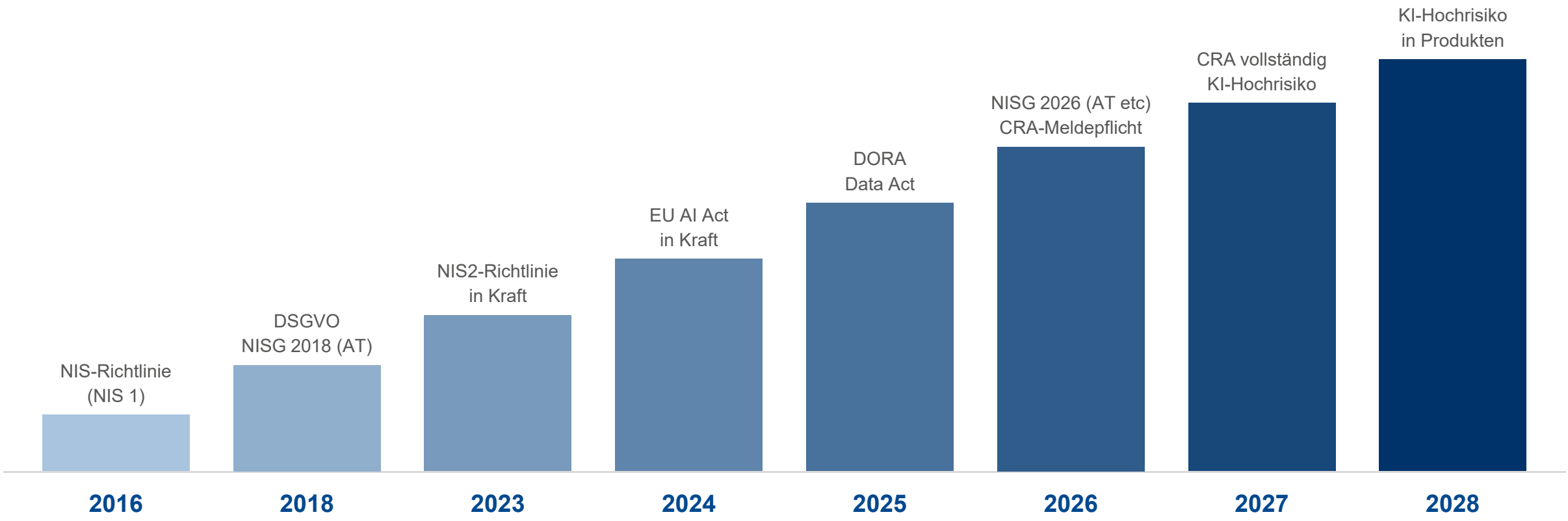
Nur für den internen Gebrauch - Internal



REGULIERUNG

Aus einzelnen Vorgaben wurde ein Regelwerk

Jede Anforderung bleibt bestehen – die Pflichten summieren sich auf

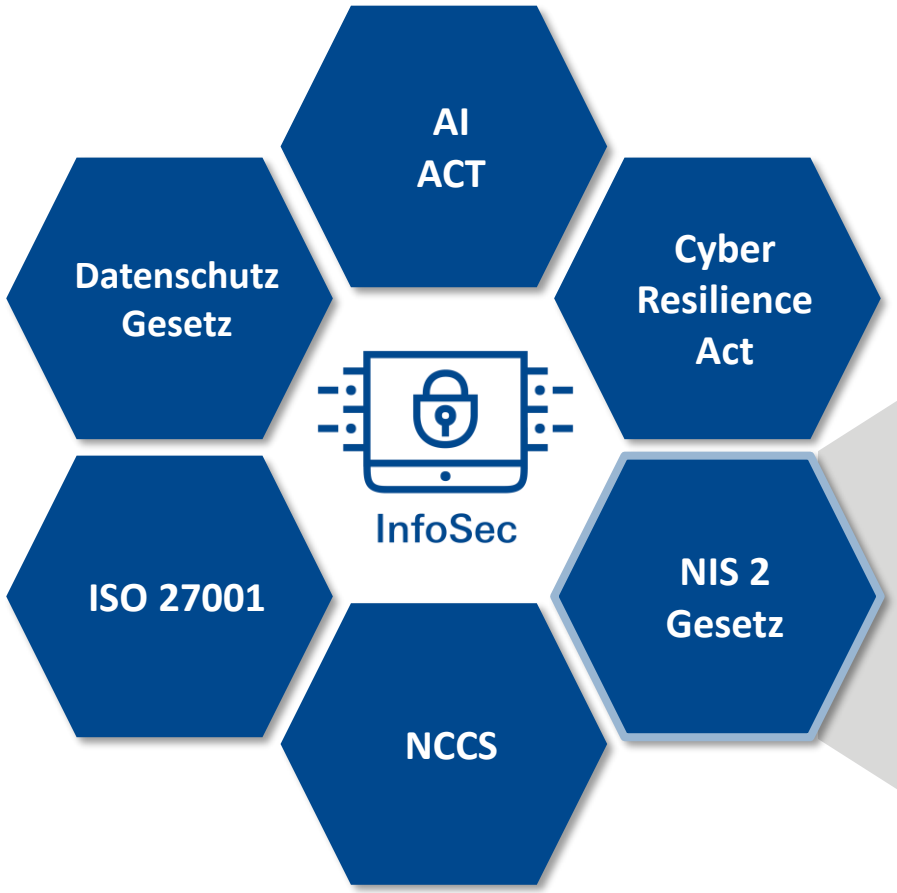


Schematische Darstellung der kumulierten Anforderungsdichte – keine Messgröße

Zeitpunkte = Anwendbarkeit bzw. Inkrafttreten der jeweiligen Pflichten. NIS 1 = Richtlinie (EU) 2016/1148, in Österreich umgesetzt durch das NISG 2018; abgelöst durch das NISG 2026 (BGBl. I Nr. 94/2025). Stand: August 2026.

Nur für den internen Gebrauch - Internal

Anstieg der Regulatorik bei VERBUND



Ausweitung des „Scope“ durch NIS 2

	NIS 1	NIS 2
Länder:	3	6
Wasserkraftwerke	6	130
Wind- und PV-Anlagen	1	158
Systeme zur Steuerung	8	10

Nur für den internen Gebrauch - Internal

AKT I · NIS2 / NISG 2026

Aus Richtlinie wird Aufsichtsrecht

Geprüft wird nicht mit einem Quantencomputer. Geprüft wird mit einer Checkliste.

Nur für den internen Gebrauch - Internal

Wo es in der Praxis klemmt

1

Betroffenheit feststellen

Sektor, Größe und Territorialität – kumulativ, je Rechtsträger und nicht je Konzern. Töchter und Auslandsgesellschaften einzeln beurteilen. Und: wesentlich oder wichtig? Die Einstufung entscheidet über das Aufsichtsregime.

2

Registrierung organisieren

Bis 31. Dezember 2026, für jede betroffene Einheit einzeln, mit Kontaktdaten und Sektorzuordnung. Änderungen sind nachzuziehen. Die Frage ist weniger das Formular als die Zuständigkeit: Wer hält diese Liste über Jahre aktuell?

3

Prozesse über Gesellschaften hinweg

Die 24-Stunden-Frist gilt je Einrichtung – das Security-Team sitzt zentral. Unterschiedliche ISystemlandschaften, unterschiedliche Reifegrade, geteilte Dienstleister. Der Meldeweg muss überall funktionieren, auch dort, wo niemand Vollzeit für Security zuständig ist.

Das Gesetz kennt Einrichtungen. Ihr Konzern kennt Gesellschaften. Dazwischen liegt Ihr Projekt.

V

Nur für den internen Gebrauch - Internal

Eine zentrale Information Security: einmal bauen, überall nachweisen

ZENTRAL AUFGEBAUT, KONZERNWEIT GENUTZT

Ein Rahmenwerk
ISMS, Maßnahmenkatalog und Risikomethodik.

Ein Meldeprozess
Templates, Freigabekette und ein Eingang, der 24/7 verfügbar ist.

Ein Inventar
Assets, Kryptografie und Lieferanten – in einer Systematik.

Ein Evidenzspeicher
Nachweise einmal erzeugt, für jede Einheit verwertbar.

↓ ↓ ↓

Betroffenheit und Registrierung

Die Einstufung trifft jede Gesellschaft für sich – zentral unterstützt, aber nicht ersetzt.

Asset- und OT-Kenntnis

Was im Werk steht und wie es zusammenhängt, weiß nur, wer davor steht.

Entscheidung und Verantwortung

Abschalten, melden, unterschreiben: Das Leitungsorgan bleibt in der Pflicht.

Zentral heißt nicht, dass jemand anderes haftet – sondern dass niemand die Lösung 40-mal neu erfindet.

Nur für den internen Gebrauch - Internal

Die eigentliche Herausforderung steht nicht im Gesetz

WAS AM PAPIER STEHT

Richtlinien und Rollen sind dokumentiert.

Ein Incident-Response-Plan liegt vor.

Lieferantenfragebögen wurden versendet.

Das Backup-Konzept ist beschrieben.

Awareness-Schulungen sind absolviert.

WAS IM ERNSTFALL PASSIERT

Wer entscheidet um 03:14 Uhr über die Abschaltung der Produktion?

Wer formuliert die Frühwarnung, während der Angriff noch läuft?

Wer meldet, wenn der Vorfall beim Dienstleister ist – und Sie es erst am dritten Tag erfahren?

Wann wurde die Wiederherstellung zuletzt tatsächlich gemessen?

Hat Ihre Geschäftsleitung je unter Zeitdruck entschieden?

Die linke Spalte bekommt man mit Beratung. Die rechte nur mit Übung.

Nur für den internen Gebrauch - Internal

24 Stunden – und die laufen ab dem Moment, in dem Sie es wissen

24 h

FRÜHWARNUNG

An das zuständige CSIRT. Verdacht auf rechtswidrige Handlung oder grenzüberschreitende Auswirkungen inklusive.

→

72 h

VORFALLSMELDUNG

Schweregrad, Auswirkungen, erste Bewertung, Indikatoren für Kompromittierung.

→

1 Monat

ABSCHLUSSBERICHT

Ursachen, Art der Bedrohung, ergriffene Abhilfemaßnahmen – oder Fortschrittsbericht, wenn es noch läuft.

NIS2 prüft nicht, ob ein Plan existiert. NIS2 prüft, ob er sonntags um 03:14 Uhr funktioniert.

Die Frist startet mit der Kenntnis des Vorfalls – nicht mit dem Beginn der Bürozeiten.

Nur für den internen Gebrauch - Internal

AKT II · QUANTUM, PQC & QKD

Der Angriff, der bereits läuft

Ihre Daten von heute werden nicht heute entschlüsselt. Heute werden sie nur eingesammelt.

Nur für den internen Gebrauch - Internal

Harvest now, decrypt later: Die Rechnung, die schon aufgeht

X Schutzdauer

Wie lange müssen Ihre Daten vertraulich bleiben? Netzpläne, Verträge, Personaldaten etc.

Y Migrationsdauer

Wie lange dauert Ihre Krypto-Umstellung? Erfahrungswerte aus vergleichbaren Projekten: 5 bis 10 Jahre.

Z Zeit bis zum Q-Day

Wann kommt der kryptografisch relevante Quantencomputer? BSI-Einschätzung: 10 bis 15 Jahre – korrigiert von zuvor 20.

$$X + Y > Z$$

Wenn die Summe größer ist als die verbleibende Zeit, sind Sie heute schon zu spät – unabhängig davon, wann der Quantencomputer tatsächlich kommt.

Nur für den internen Gebrauch - Internal

Die Mathematik ist gelöst. Das Inventar nicht.

STANDARDISIERT SEIT 2024

ML-KEM (FIPS 203)
Schlüsselaustausch, ehemals CRYSTALS-Kyber

ML-DSA (FIPS 204)
Digitale Signaturen, ehemals CRYSTALS-Dilithium

SLH-DSA (FIPS 205)
Hashbasierte Signaturen, ehemals SPHINCS+

HQC
2025 als zusätzliches Verfahren ausgewählt

WAS DARAUS FÜR SIE FOLGT

Krypto-Inventar
Welcher Schlüssel liegt wo, in welchem Produkt?

Hybride Verfahren
Klassisch und PQC parallel – keine Wette auf ein Verfahren.

Krypto-Agilität
Austauschbarkeit als Architekturprinzip statt Einmal-Migration.

Lieferanten und OT
Wer kann updaten? Wer weiß, was in der Firmware steckt?

Die Algorithmen bekommen Sie von der NIST. Das Inventar bekommen Sie von niemandem.

Nur für den internen Gebrauch - Internal

Auch dafür gibt es längst einen Kalender

Ende 2026	Nationale Roadmap, Krypto-Inventar, Risikoanalyse und erste Pilotprojekte für Anwendungen mit hohem und mittlerem Risiko.
Ende 2030	Hochrisiko-Anwendungen und kritische Infrastrukturen sind auf quantensichere Verfahren umgestellt.
Ende 2035	Die Umstellung ist über alle übrigen Systeme hinweg weitgehend abgeschlossen.

Der Prüfer fragt nicht nach Ihrem Quantencomputer. Er fragt nach Ihrem Krypto-Inventar.

§ 32 NISG 2026 verlangt Kryptografie nach dem Stand der Technik – und der heißt ab jetzt: quantensicher migrierbar. Quelle: EU-Roadmap der NIS-Kooperationsgruppe, Juni 2025.

Nur für den internen Gebrauch - Internal

Quantum Pioneer
Quantenkryptographie im Fokus der Security

OT Cyber Lab

Eine Quanten-Teststellung im Rahmen des OT-Cyber Security Labs

VERBUND hat sich als **erster Energieversorger Österreichs** zum Ziel gesetzt, den Bereich der Quantenkryptographie für die sichere Datenübertragung im eigenen Weitverkehrsnetz zu beleuchten, um die Versorgungssicherheit Österreichs auch in Zukunft zu gewährleisten.

Durch den Aufbau einer **hybriden Teststellung** mit Post-Quantum-Algorithmen (**PQC**) und Quantum Key Distribution (**QKD**) kann innerhalb des VERBUND Weitverkehrsnetz die Performance sowie Funktionalität der sicheren Datenübertragung durch die Teststrecke erforscht werden.

Hauptziel ist es erste Schritte in Richtung **Quantenkryptographische Technologien** als **sicheres Übertragungsverfahren** für sensible Daten vorzunehmen.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY HITACHI CANCOM qtlabs Quantum Technology Laboratories

Nur für den internen Gebrauch - Internal

Zeitstrahl des Quantum Pioneer Projekts

OT Cyber Lab

Juni – November 2023
Erste Orientierung zum Thema Quantenkryptographischer Technik durch Vorstudien und Forschung

Dezember 2023
Pentest der Hardware welche im VERBUND Weitverkehrsnetz flächendeckend verwendet warden, sowie Reise nach Genf zu IDQ

Jänner – April 2024
Konkrete Gespräche über den Aufbau des Versuchsaufbaus mit den Projektpartnern und Bestellung der ersten Geräte

Mai – Oktober 2024
Fertigstellung des Testaufbaukonzepts und Bestellung von QKD-Komponenten durch Bereitstellung interner Mittel

November – Dezember 2024
Integration des Testaufbaus im VERBUND-Rechenzentrum „Am Hof“ in Wien in das Weitverkehrsnetz mit technischer Unterstützung

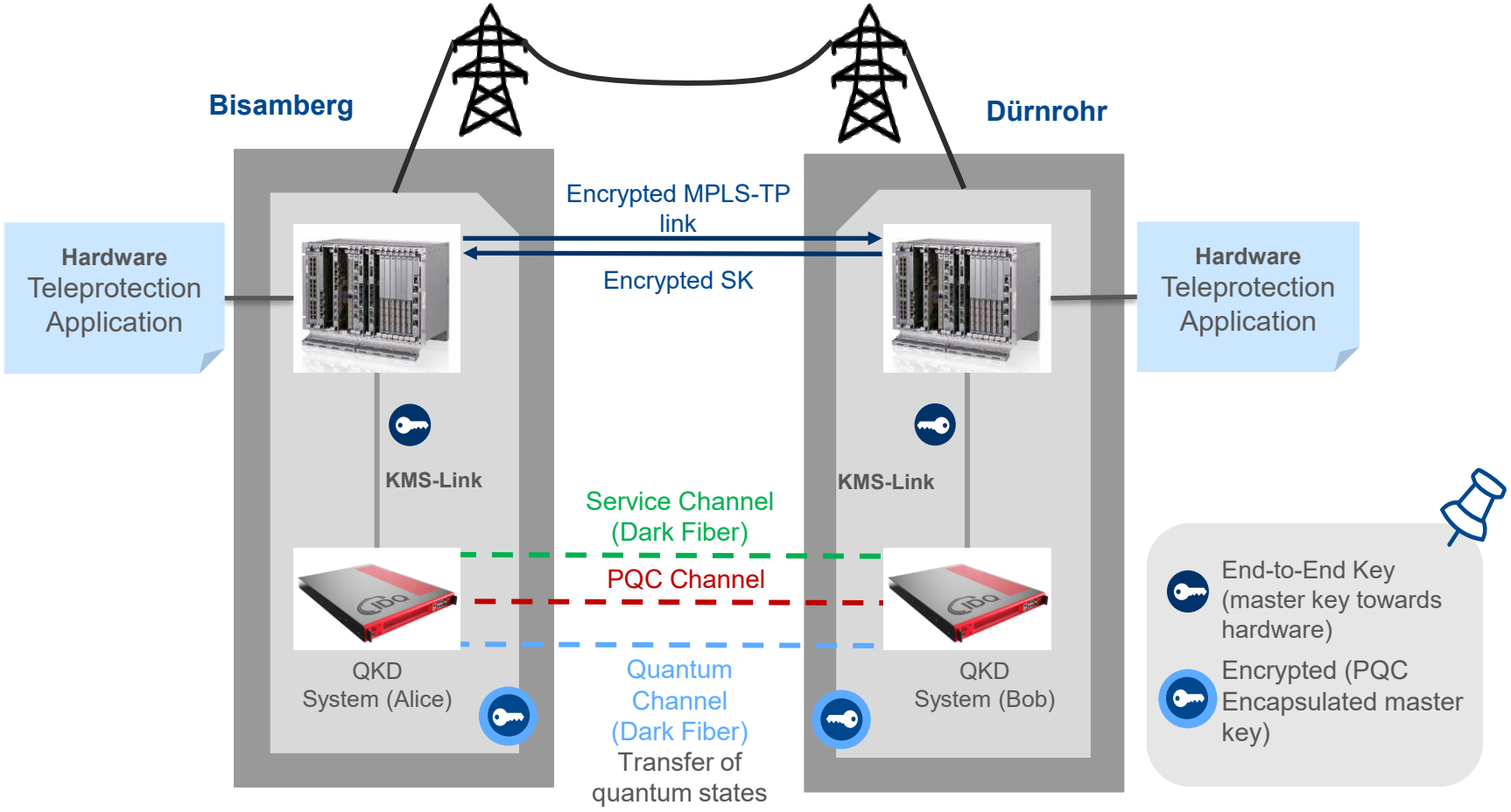
Dezember 2024 & darüber hinaus
Nutzung des Testaufbaus mit spezifischen, auf Energieversorger ausgerichteten Anwendungsfällen zur Erprobung quantenkryptographischer Technologien

Entscheidung über mögliche weitere Implementierungen
Definition weiterer PoCs

Nur für den internen Gebrauch - Internal

Hybride Quanten-Teststellung

Verschlüsselung durch Quantum Key Distribution und Post-Quantum Cryptography



Nur für den internen Gebrauch - Internal

Zwei Antworten auf dieselbe Bedrohung

	QKD	PQC
Sicherheitsannahme	Die Gesetze der Quantenphysik	Mathematisch „harte“ Probleme
Schutzgegenstand	Der Schlüsselaustausch über eine einzelne Strecke	Verschlüsselung und digitale Signaturen
Voraussetzung	Dedizierte Hardware an beiden Enden, begrenzte Reichweite	Software und Kenntnis des eigenen Kryptobestands
Reifegrad	Pilot- und Forschungsinfrastruktur	Standardisiert seit 2024: FIPS 203, 204 und 205
Regulatorischer Bezug	Keine Frist, keine Vorgabe	EU-Roadmap mit Zwischenzielen 2026, 2030 und 2035

Die eine Technologie sichert eine Strecke, die andere eine Infrastruktur. Nur eine davon steht in einem Kalender.

V

Nur für den internen Gebrauch - Internal

AKT III · CYBER RANGE

Compliance, die man schwitzen sieht

Die Feuerwehr übt nicht mit einer Präsentation über Feuer.

Nur für den internen Gebrauch - Internal

Zwischen Plan und Ernstfall liegt eine Lernkurve

SAMSTAG, 03:14 UHR

In der Leitwarte fallen die Fernwirkverbindungen zu drei Kraftwerken aus. Die Maschinen laufen weiter, aber Sollwerte lassen sich nicht mehr verändern.

Die Fernwartung des Leittechnik-Herstellers läuft über denselben Zugang, der in der Nacht kompromittiert wurde. Der Techniker ist in vier Stunden am Standort. Die Gruppe ist für Sekundärregelleistung präqualifiziert.

Und die 24-Stunden-Frist läuft ab jetzt.

FÜNF FRAGEN, DIE JETZT BEANTWORTET WERDEN MÜSSEN

Wer stuft den Vorfall als „erheblich“ ein – nach dem Security-Kriterium oder nach der ausgefallenen Erzeugungsleistung?

Wer entscheidet über Handbetrieb oder Abfahren der Maschinen: Security, Betriebsführung oder Kraftwerksleitung?

Wer trennt IT und OT – und wer weiß, welche Anlagen danach nur noch vor Ort bedienbar sind?

Wer meldet an wen: CSIRT, Regelzonenführer, Konzernmutter?

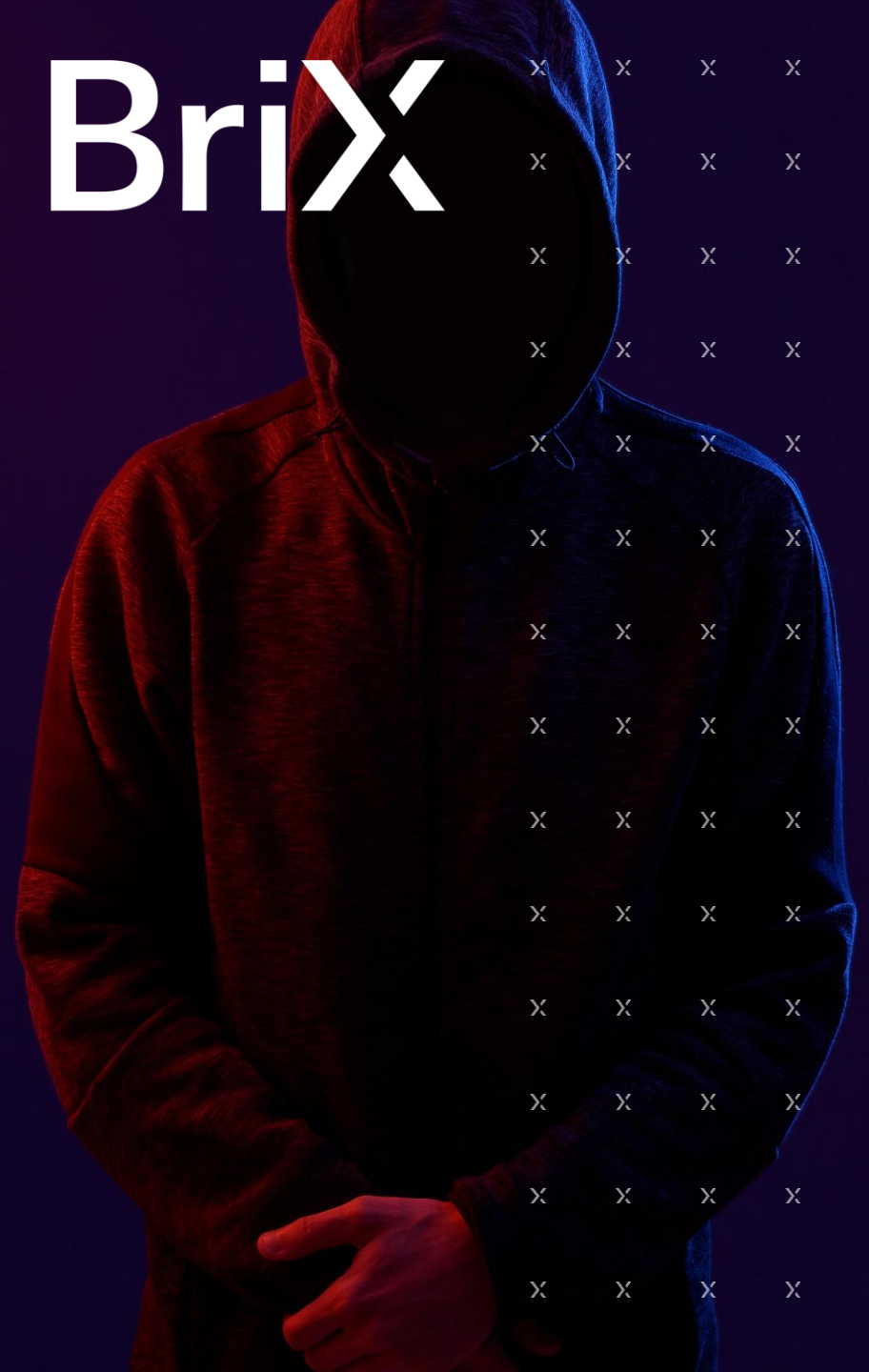
Wo entsteht die Evidenz, wenn die Leittechnik keine forensischen Logs vorhält?

Diese Fragen beantwortet man genau einmal zum ersten Mal: in der Übung oder in der Presseaussendung.

Nur für den internen Gebrauch - Internal

Yellow BriX

Cyber Skill Academy



powered by Verbund

Wir vereinen jahrzehntelange Erfahrung im Sicherheitsbereich mit einem vorausschauenden Blick in die Zukunft

UNSERE DIFFERENZIERUNG

Jahrzehntelange **Erfahrung** im sicheren Betrieb kritischer Infrastruktur

Maßgeschneiderte, kundenspezifische Szenarien mit Fokus auf OT-Komponenten

Vereinigung einer **hybriden** Cyber-Range (Cloud, On-Premise und Virtualisierung)

UNSER STANDORT

Historische Kraftwerksstandort als **einzigartige Trainingsumgebung**

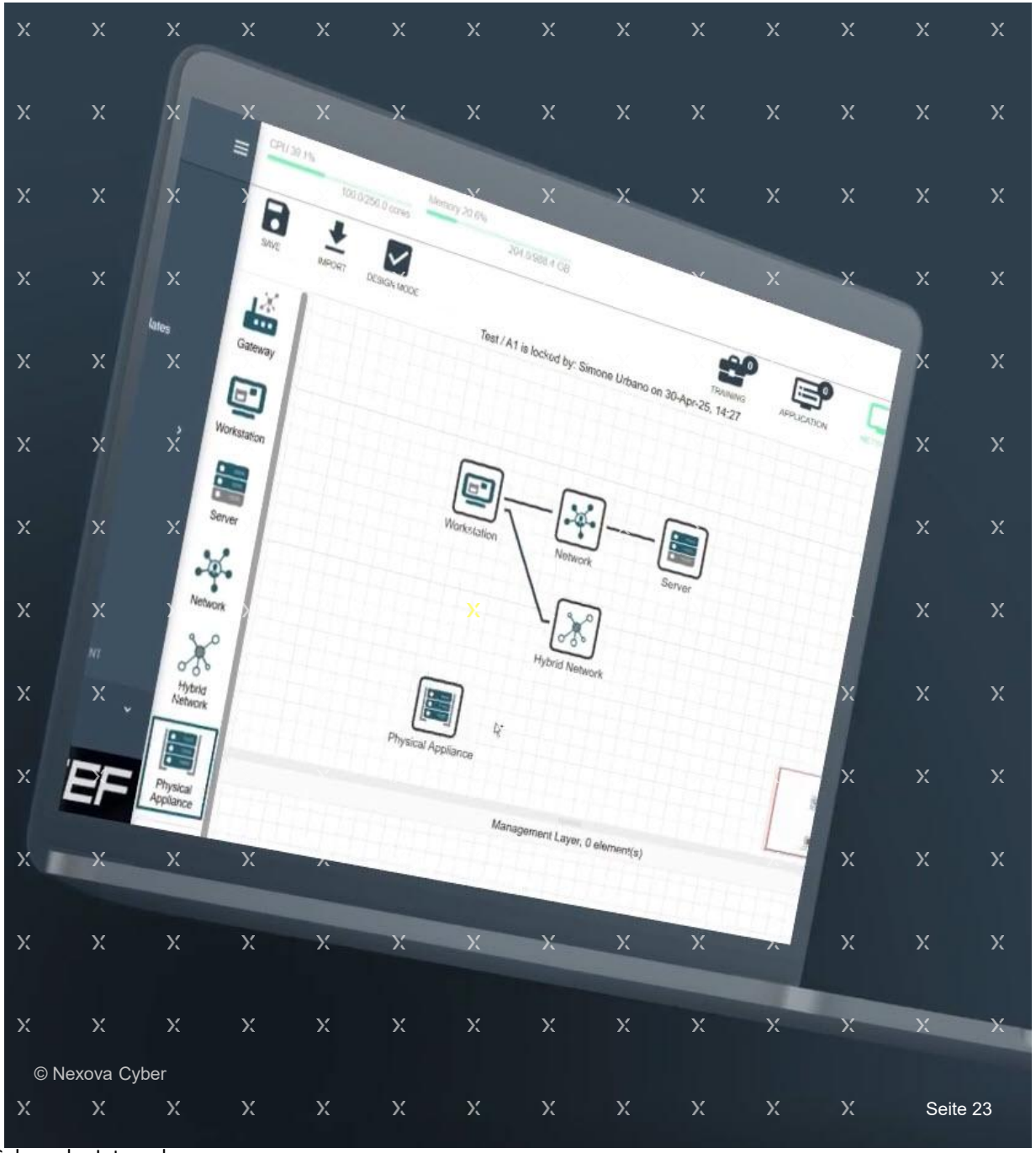
Interaktives Trainingscenter mit moderner Technik, Beobachtungsräumen und sichtbaren OT-Geräten für ein authentisches Trainingserlebnis

Umfangreiche **Trainingsmöglichkeiten** und virtuelle Trainingsoptionen

Nur für den internen Gebrauch - Internal

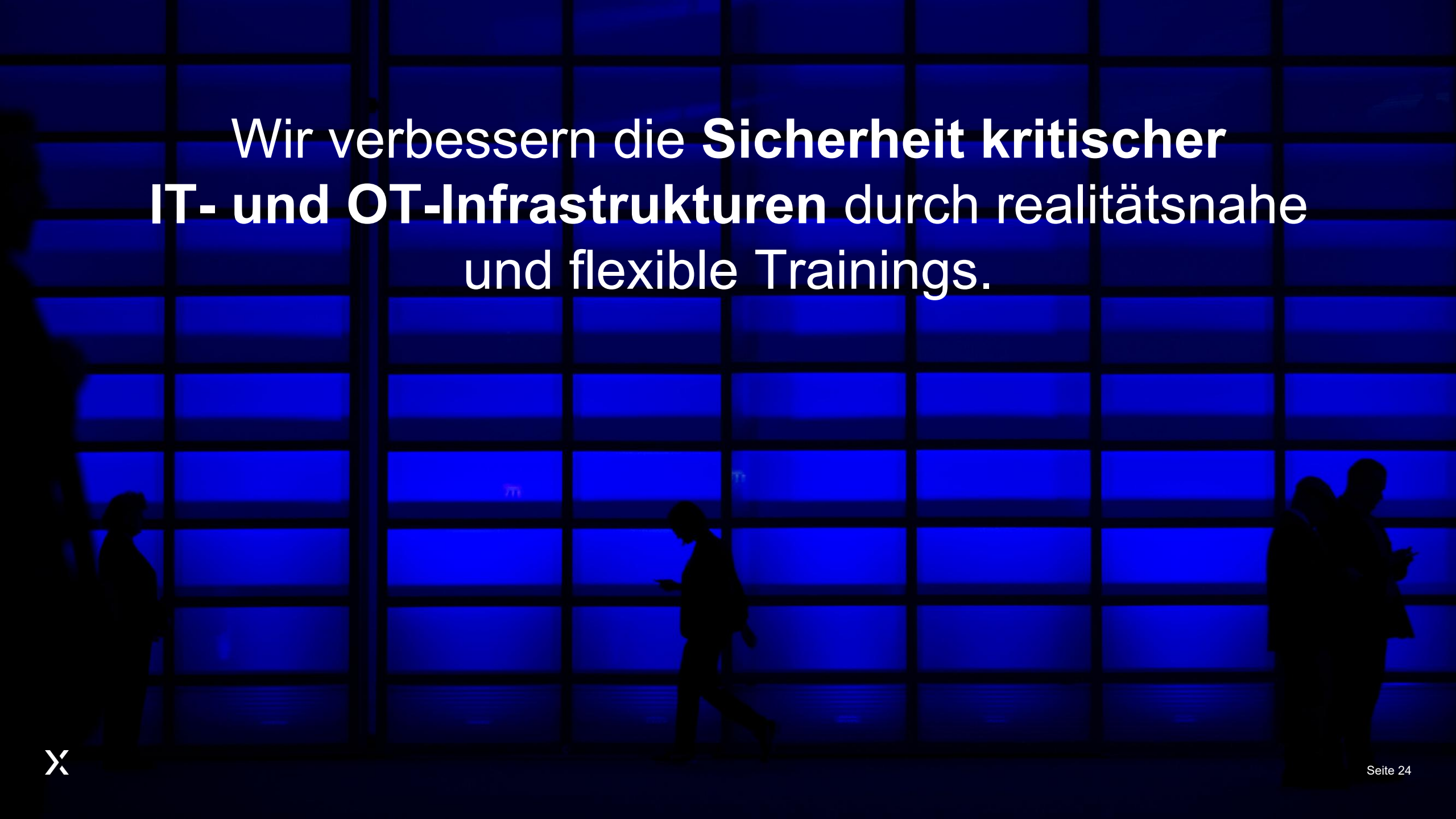
Das Herzstück von Yellow Brix bildet die Cyber Range mit einer speziell entwickelten Simulationssoftware.

- Gemeinsame Trainingsumgebung für virtuelle IT- und OT-Systeme sowie reale technische Komponenten
- Realitätsnahe Abbildung von Netzwerken und Industrieanlagen
- Nachvollziehbare Angriffswege



© Nexova Cyber

Nur für den internen Gebrauch - Internal


Wir verbessern die **Sicherheit kritischer IT- und OT-Infrastrukturen** durch realitätsnahe und flexible Trainings.

Drei Fragen zum Mitnehmen…

1

Wissen Sie, wo Ihre Kryptografie liegt?

Das Krypto-Inventar ist die erste Bringschuld der EU-Roadmap – Frist: Ende 2026.

2

Können Sie in 24 Stunden melden – nachts und am Wochenende?

Rollen, Templates und Freigaben gehören vorab definiert, nicht während des Vorfalls.

3

Wann wurde zuletzt realitätsnah geübt?

Nur Übungen nahe an der Realtität ermöglichen eine wirkliche Verbesserung.

Kein Gesetz, kein Standard und kein Algorithmus wirkt, bevor ihn jemand implementiert.

Nur für den internen Gebrauch - Internal

Yellow BriX

Cyber Skill Academy

Are you ready?