FINANCE ROUNDTABLE

Herzlich willkommen zum FINANCE-Roundtable Security ist Chefsache

VERANSTALTER

FINANCE
Das Magazin für Finanzchefs

MITVERANSTALTER

GREEN FIELD BECHTLE

FINANCE ROUNDTABLE

Begrüßung

Thomas Holzamer
Redakteur
FINANCE

FINANCE ROUNDTABLE

Begrüßung

Michael Beilfuss
Head of Customer Success
Bechtle

Martin Schmidl
Geschäftsführer
Bechtle Frankfurt

FINANCE ROUNDTABLE

Agenda

17.00 Uhr	Begrüßung
17.10 Uhr	Impulse • David Thornewill, Grey Beard Advisory / Mathias Schick, Bechtle • Sophia Eltrop, naturstrom AG • Dr. Daniel Pauly, Linklaters LLP
18.10 Uhr	Wissensvermittlung & Gruppenarbeit in Form einer Gamification
18.45 Uhr	Wrap up
ca. 19.15 Uhr	Dinner im Holbein‘s Restaurant

FINANCE ROUNDTABLE

IT-Security - Warum muss uns das beschäftigen?

David Thornewill
Cyber Security Expert
Grey Beard Advisory

Mathias Schick
Business Manager IT-Security
Bechtle

NIS-2 – Überblick

EU-weite Richtlinie, die bis 17. Oktober 2024 in nationales Recht umgesetzt werden muss (In DE wird es voraussichtlich Anfang 2025)

Ca. 30.000 betroffene Organisationen in DE, Unterscheidung in wichtige und wesentliche Einrichtungen (Öffentliche Einrichtungen, Versorger, Energie, Banken, Verkehr, Gesundheitswesen, Post, Abfall, …)

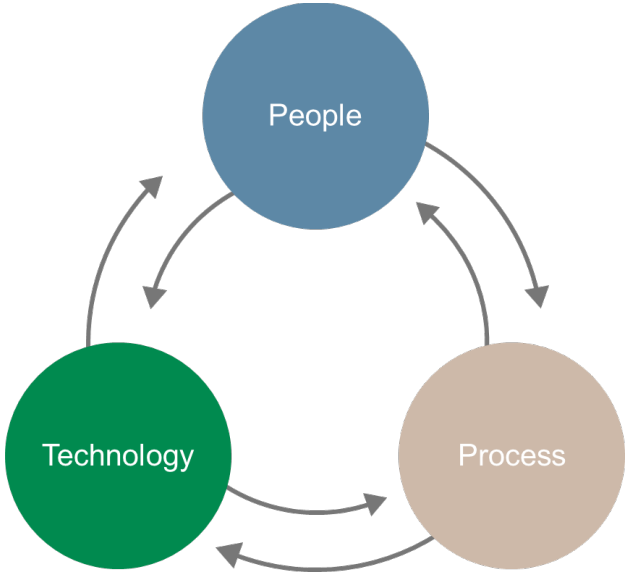
Ziel: Cyberresilienz betroffener Organisationen nachhaltig erhöhen, EU weite Harmonisierung

Wesentliche Elemente

Risikobasierter Ansatz => Informationssicherheitsmanagement einführen, Security als wesentlichen Teil der Unternehmenstätigkeit verstehen, Security als fortlaufender Prozess, SOC für Reaktion und Detektion, Notfallplan, Meldepflichten

Management-Verantwortung

Führungsebene ist persönlich verantwortlich, hohe Strafen möglich, bis zu 10 Mio € oder 2% des Umsatzes



NIS-2 Handlungsphasen und -felder

	S	M	L
Vorgespräch mit Betroffenheits- und Komplexitäts-Einschätzung	✓	✓	✓
Einführungsseminar zu NIS-2	✗	✓	✓
Kick-Off	✓	✓	✓
Datenerfassung	2 Tage Remote	2 Tage vor Ort	mind. 3 Tage vor Ort
Interviews (Organisation, Prozesse, Mensch)	✓	✓	✓
Dokumentationssichtung	✗	✓	✓
System- und Netzwerkanalyse	✗	✓	✓
Richtlinienüberprüfung	✓	✓	✓
Zwischenbericht	✗	✗	✓
Maßnahmenkatalog	✓	✓	✓
Reifegradbestimmung	✓	✓	✓
Lückenanalyse	✓	✓	✓
Kritische Infrastrukturen identifizieren	✗	✓	✓
Risikobewertung	✗	✗	✓
Entwicklung des Aktionsplans	✗	✗	✓
Abschluss-präsentation	✓	✓	✓
Review-Meeting	✗	✓	✓
Begleitende Projektunterstützung	✗	✗	✓

Aus der Standortbestimmung mithilfe eines NIS-2-Assessments leiten sich organisatorische und technische Folgemaßnahmen ab.

FINANCE ROUNDTABLE

Maßgeschneiderte Risikokategorien für das IT-Security-Konzept

Sophia Eltrop
Vorständin Finanzen, IT und Personal
naturstrom AG

CFO Roundtable zur IT-Security

06.Juni 2024 in Frankfurt

6. Juni 2024

naturstrom
ENERGIE MIT ZUKUNFT

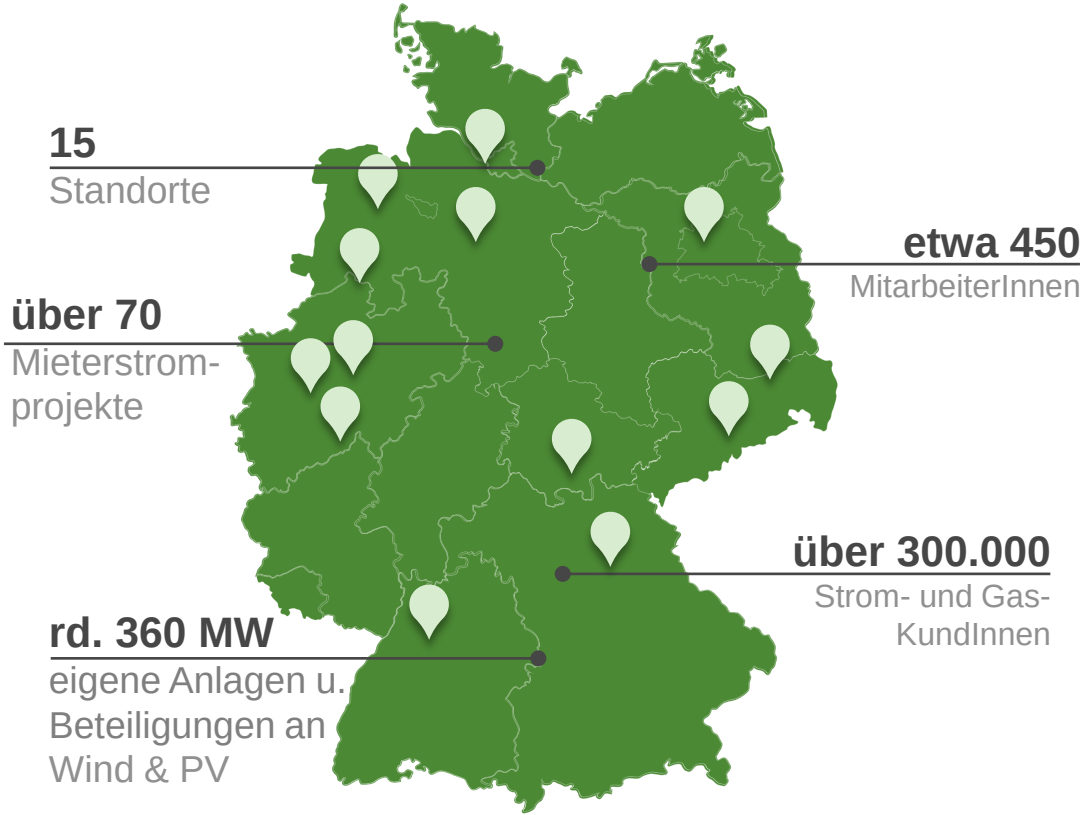
naturstrom ist nachhaltiger Energieanbieter der ersten Stunde

Überblick

- Pionier der Energiewende seit 1998
- 15 Standorte
- über 270.000 Ökostrom-KundInnen
- über 30.000 Biogas-KundInnen
- ca. 740 Mio. Euro Umsatz (2022)
- Mehr als 1 Mrd. kWh Ökostromabsatz

Eigentümerstruktur

- Grundkapital 30,5 Mio. €
- 2,44 Mio. Aktien
- 1.700 Aktionär:innen
- Über 50 % der Aktien in Besitz von privaten Kleinaktionär:innen



Maßgeschneiderte Risikokategorien für das IT-Security-Konzept

OT und IT (operative Technik separat beachten)

Technologie-Einsatz (u.a. Cloud-Strategie etc.)

Fehlerquelle Mensch

Regulatorik, Normen und Patches

Back Ups

Angriffserkennung, Notfall- und Krisenmanagement, (BCM)

FINANCE ROUNDTABLE

Security ist Chefsache – der rechtliche Rahmen für Unternehmensentscheider

Dr. Daniel Pauly
Partner
Linklaters LLP

FINANCE-Roundtable

Security ist Chefsache – NIS-2 nimmt Unternehmensentscheider in die Pflicht

Dr. Daniel Pauly

6. Juni 2024

Anforderungen – Präventiv

Gesellschaftsrecht

Rechtsformübergreifend, im Rahmen der Leitungsaufgaben:

- Umsetzung **spezieller Pflichten** für Unternehmen (z. B. Geheimnisschutz, Datenschutz, IT-Sicherheit)
- **Frühwarnsystem** für den Bestand der Gesellschaft gefährdende Risiken

Börsennotierte Gesellschaften:

Internes **Kontroll- und Risikomanagementsystem** auch für *nicht* bestandsgefährdende Risiken („Wirecard-Paragraph“)

BSI-Gesetz

Im Rahmen der Legalitätskontrollpflicht:

- Organisatorische und technische Vorkehrungen zur **Vermeidung von Störungen** von IT-Systemen und Systeme zur **Angriffserkennung**
- Dokumentations- und **Nachweispflichten**

Anforderungen an Geschäftsleitung:

- Mind. ein **fachkundiges** Mitglied
- **Sorgfaltspflichten** treffen **alle**
  - > Ausreichendes **Verständnis** für digitale Thematiken
  - > Bewusstsein für (aktuelle) **Cyberrisiken**

NIS2

Persönlich für Geschäftsleitung:

- **Schulungsteilnahme**
- Billigung von **Risikomanagementmaßnahmen** und Überwachung der Umsetzung

Im Rahmen der Leitungsaufgaben:

- **Registrierung**
- Dedizierte **Risikomanagementmaßnahmen**
- **Schulungsaufforderung** an alle Mitarbeitenden
- **Kooperation** mit Aufsichtsbehörde
- **Informationsaustausch** mit anderen Einrichtungen

NIS2-Umsetzung (E)

Persönlich für Geschäftsleitung:

- Regelmäßige Teilnahme an **Risikomanagementschulungen**
- Persönliche **Billigung und Überwachung** von Risikomanagementmaßnahmen

Im Rahmen der Leitungsaufgaben:

- **Registrierung** und Änderungsanzeige
- **Risikomanagementsystem** (zahlreiche Mindestinhalte)
- Zukünftige **branchenspezifische** Sicherheitsstandards
- **Nachweispflichten**, regelmäßige **Audits** oder Zertifizierungen
- **Kontinuierliche Verbesserung**

Anforderungen – Nach einem Vorfall

Gesellschaftsrecht

- Risikobewältigung, u.a. mittels:
  - **Versicherung**smeldungen
  - **Rückstellungen**
- Krisenbewältigung:
  - Krisen**eindämmung**
  - **Folgenbeseitigung**
  - **Ex-Post-Analyse**
  - **Optimierung** der Strukturen und Abläufe

BSI-Gesetz

Auf Verlangen des BSI:

Herausgabe notwendiger **Informationen**

NIS2

Gemäß Ausgestaltung der einzelnen Mitgliedstaaten (Unterschiede!):

- Mehrstufiges **Meldesystem** bei „erheblichen Sicherheitsvorfällen“
- **Unterrichtungspflichten** gegenüber Diensteempfängern

NIS2-Umsetzung (E)

Abgesehen von allg. Risiko- & Krisenbewältigung:

- Mind. 3 **Meldungen** über Vorfälle:
  - Erstmeldung (max. 24 Std.)
  - Erstbewertung (max. 72 Std.)
  - Abschlussmeldung (1 Monat)
- **Unterrichtungspflichten** gegenüber Diensteempfängern und BSI, mit Empfehlung von **Abhilfemaßnahmen**
- **Herausgabepflicht** bzgl. notwendiger Informationen (auf Verlangen)

Haftung

Gesellschaftsrecht

- Haftung bei **Pflichtverletzungen**
- **Pflicht** für Unternehmen / Aufsichtsrat, Ansprüche zu verfolgen
- **Gemeinsame Haftung** des Vorstands
- **Entlastung** möglich, aber Beweislast bei Geschäftsleitung

→ **Delegation** von Aufgabenbereichen erst auf Durchsetzungsebene vertretbar (Überwachungspflicht bleibt)

BSI-Gesetz

- Haftung im Rahmen von Pflichtverletzungen aus **Gesellschaftsrecht**
- Erstellte Dokumentationen bieten eine **Chance** für die Entlastung der Geschäftsleistung

NIS2

Gemäß Ausgestaltung der einzelnen Mitgliedstaaten (Unterschiede!):

Verantwortlichkeit von Leitungsorganen für Pflichtverstöße

NIS2-Umsetzung (E)

- **Schadensersatzpflicht** des Leitungsorgans gegenüber der Gesellschaft
- **Hohes Schadenspotenzial**, u.a. wenn das Unternehmen mit Bußgeldern von bis zu 10 Mio. EUR bzw. 2 % des weltweiten Jahresumsatzes belegt wird
- **Kein Verzicht** auf Ersatzansprüche möglich
- **Außergerichtliche Vergleiche** nur unter gewissen Voraussetzungen möglich

Fazit

Die **Anforderungen** an die Geschäftsleitung bezüglich Cybersicherheit werden **konkreter und strenger**

Pflichtverletzungen unterliegen umfassend (bestehenden) **Haftungsregeln** für die Geschäftsleitung

Vorstandsmitglieder sind **gemeinsam letztverantwortlich** und können die Überwachung der Cybersicherheit nicht einmal vorstandsintern vollständig delegieren

Aufgrund der Zunahme des Digitalisierungsgrads, der Wahrscheinlichkeit von Cyberrisiken und der gesetzlichen Sanktionsmöglichkeiten **steigt** das **Schadenspotenzial** (auch) für Vorstände

Linklaters LLP

Dr. Daniel A. Pauly

Partner, Rechtsanwalt, Frankfurt am Main

Tel: +49 69 71003 570

daniel.pauly@linklaters.com

Taunusanlage 8
60329 Frankfurt am Main
Postfach 17 01 11
60075 Frankfurt am Main

Tel: (+49) 69 71003 570
Fax: (+49) 69 71003 333

www.linklaters.com

Gruppenarbeit

FINANCE ROUNDTABLE

Darknet Diggers Coach Mathias Schick

Was ist für Ihr Unternehmen die größte Herausforderung im Zusammenhang mit NIS-2

Phishing Phantoms Coach Michael Beilfuss

NIS-2: Wie kann mein Unternehmen wirklich profitieren? Jenseits der Erfüllung einer (lästigen) Pflicht.

Ransom Raiders Coach David Thornewill

Wissen Sie, was im Cyber-Notfall zu tun ist?

FINANCE ROUNDTABLE

Wrap up & Abschluss

Michael Beilfuss
Head of Customer Success
Bechtle

Martin Schmidl
Geschäftsführer
Bechtle Frankfurt

FINANCE ROUNDTABLE

Herzlichen Dank für Ihre Aufmerksamkeit!