NOERR

Cybersecurity in der Praxis

Einführung, rechtliche und technische Perspektiven für sichere Geschäftsabläufe

Eileen Walther (Northwave)

RA Lars Meyer

RA Julian Monschke

27.09.2023

Live-Webinar: Ablauf & Hinweise

Fragen im Chat:

- Sie haben die Möglichkeit, live über den Chat Fragen zu stellen.
- Wenn Sie eine Frage stellen, bleiben Sie gegenüber den übrigen Webinar-Teilnehmern anonym. Nur die Speaker sehen die von Ihnen gestellten Fragen.
- Bitte haben Sie Verständnis dafür, dass wir ggf. nicht jede Frage beantworten können. Sie können gerne im Nachgang auf uns zukommen.

Datenschutzhinweis:

Bitte beachten Sie, dass der Veranstalter Video- und Audioaufzeichnungen des Webinars machen kann und diese ggf. im Internet verbreitet.

Präsentation:

Die Präsentation wird den Teilnehmern des Webinars im Nachgang zur Verfügung gestellt.

Content

NORTHWAVE CYBER SECURITY

NOERR

Bedrohungsszenarien und Perspektiven für sichere Geschäftsabläufe

Eileen Walther, Country Manager Germany, Northwave Cyber Security

27. September 2023

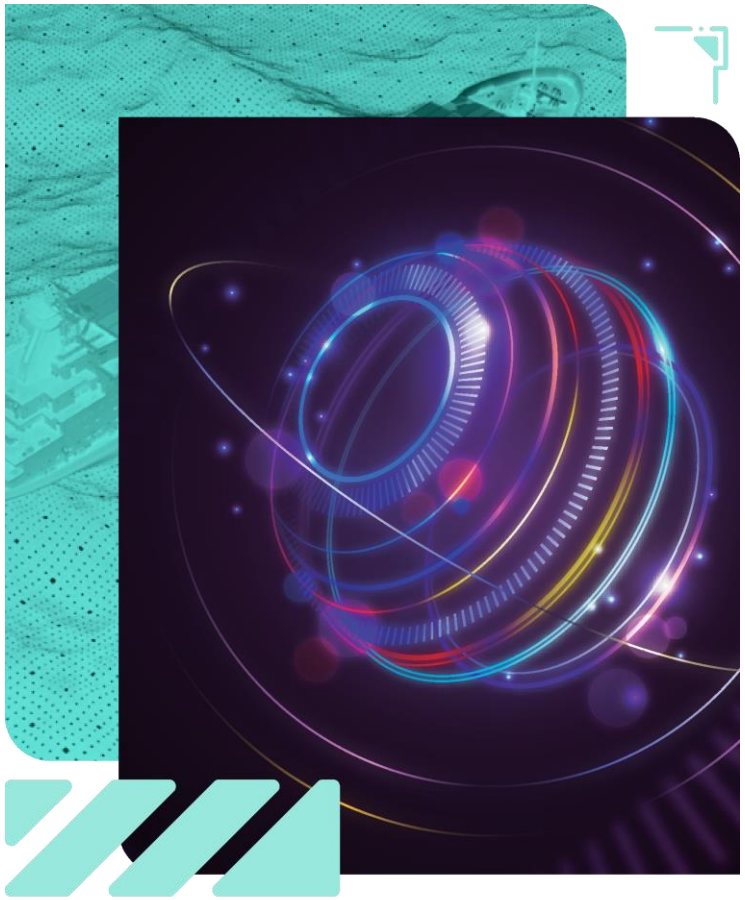
Top Cyberbedrohungen

- Ransomware
- APT’s
- High Volume Cybercrime:

  DDoS, Business-E-mail Compromise, Insider Threat, etc.

Ransomware

Fakten & Erwartungen



Underground-Dynamik der letzten 12 Monate

- Der Rückgang der Angriffe Anfang 2022 (zeitgleich mit der Invasion in der Ukraine) ist vorbei, und die Zahl der Angriffe steigt wieder an.
- Ransomware-Gruppen haben sich im vergangenen Jahr verändert und neu organisiert.
- Führungsebene und Reputation im Fokus der Erpressung.

Zunehmendes Volumen, wechselnde Taktiken

- Weitere Verlagerung von der Datenverschlüsselung zu (reinen) Datenerpressungsangriffen.
- Größere Wahrscheinlichkeit von Ausfällen bei neuen Opfern in Russland und China betroffen zu sein. China ist ein großer Produzent und Lieferant für Materialien.
- Mehr Regierungen "hacken" aktiv gegen Ransomware-Gruppen.

APT's

Fakten & Erwartungen

Geopolitische Spannungen

- China bereitet sich auf mehr „Abschottung“ und „autonome Beschränkung“ vor.

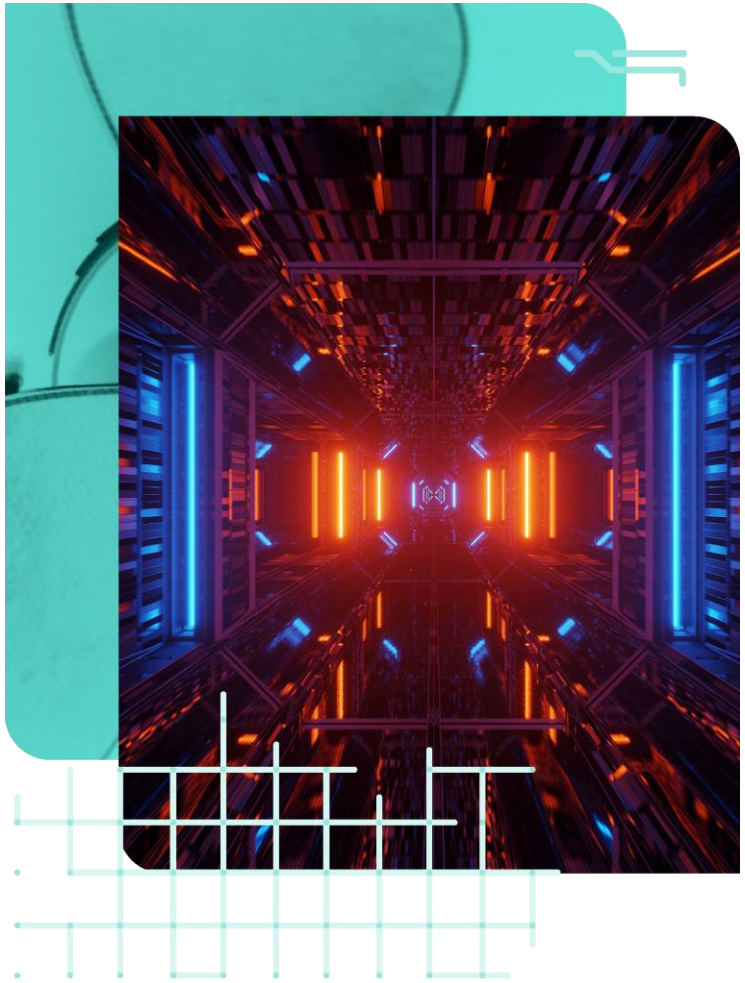
- Geringe Sichtbarkeit, große Menge an Zeit und Ressourcen, die für China’s APT-Aktivitäten zur Verfügung stehen.

Zunehmende Polarisierung

- Die globale IT-Konnektivität von in China tätigen Unternehmen könnte weiter eingeschränkt werden, und es wird mit zusätzlicher Überwachung gerechnet.

- Mögliche neue westliche Sanktionen könnten Unternehmen dazu zwingen, ihre Aktivitäten in China einzustellen/zu beenden.

- Es wird ein verstärkter APT-Fokus auf OT erwartet.



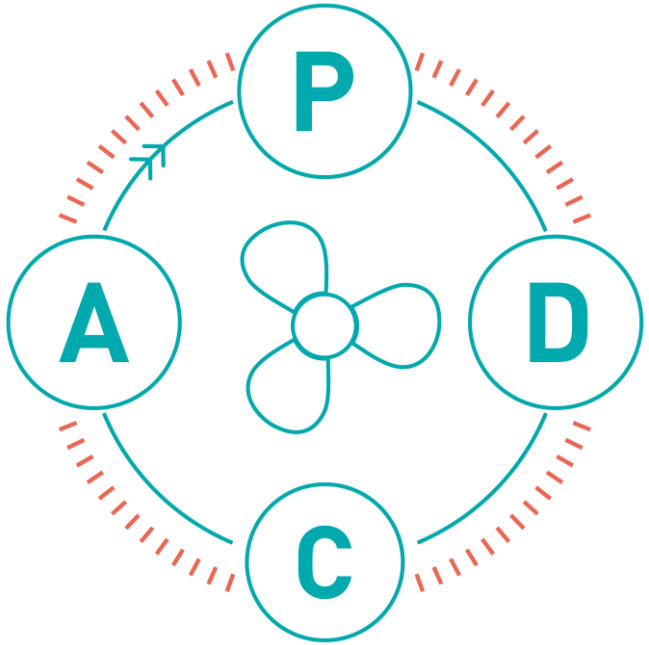
APT's sind das neue Problem

- APT's sind schwierig zu detektieren. Druck auf hochwertiger Intelligence und Analysten.
- APT's haben Zeit. (Sie als/Ihre) Mitarbeiter, telco/ISP's und Lieferanten sind nützliche Sprungbretter.
- APT's treffen Unternehmen im strategischen Bereich (IP). Risiken einschätzen bedarf einer neuen Perspektive.
- Die EU nimmt die NIS2 Direktive sehr ernst.

Intelligent Security Operations

Risk Assessment

Risk Treatment Plan: Taking And Maintaining Security Measures
NIST Framework



NIST Framework

ISO27001 Security Management (ISMS)

Initiate | Prevent | Detect | Respond | Recover

People & Skills Management

NORTHWAVE
CYBER SECURITY

Eileen Walther

Country Manager Germany

info@northwave-security.com

northwave-cybersecurity.com

Rechtliche Rahmenbedingungen

Übersicht über die Pflichten für die Adressaten

IT-Sicherheits-pflichten	Registrierung	Inhaltliche Anforderungen an die Sicherheit	Meldepflichten	Nachweise und Überprüfungen

Überblick über wesentliche gesetzliche Vorgaben

Gesetz	Adressaten
BSI-Gesetz	• Betreiber Kritischer Infrastrukturen • Anbieter digitaler Dienste • Unternehmen im besonderen öffentlichen Interesse
Telekommunika-tionsgesetz	Anbieter von Telekommunikationsdiensten
DS-GVO	Unternehmen, die personenbezogene Daten verarbeiten
EnWG	Energiewirtschaftsgesetz
KWG i.V.m. BAIT/MaRisk	Kreditinstitute *(vergleichbare Vorgaben an andere Unternehmen der Finanzindustrie)*

- Unabhängig von gesetzlichen Vorgaben existieren zahlreiche verwaltungsrechtliche Vorgaben.
- Pflichten der Unternehmensleiter verpflichten Leitungsorgane unabhängig von gesetzlichen Pflichten, IT-Sicherheitsmaßnahmen zu ergreifen
- Hinzu kommen vor allem vertragliche Anforderungen, die häufig auch versteckt sind, etwa in Einkaufs-AGB.

Was tut sich?

Cyberrisikomanagement als Pflicht der Geschäftsleitung (1)

Art. 20 NIS-2-Richtlinie

Die Mitgliedsstaaten stellen sicher, dass die **Leitungsorgane wesentlicher und wichtiger Einrichtungen** die von diesen Einrichtungen zur Einhaltung von **Artikel 21** ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit **billigen**, ihre Umsetzung **überwachen** und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen **verantwortlich gemacht** werden können.

137 - Erwägungsgründe

Die Richtlinie sollte darauf abzielen, auf Ebene der wesentlichen und wichtigen Einrichtungen ein **hohes Maß an Verantwortung** für die Risikomanagementmaßnahmen und die **Berichtspflichten** im Bereich der Cybersicherheit sicherzustellen. Daher sollten die **Leitungsorgane** der wesentlichen und wichtigen Einrichtungen die Risikomanagementmaßnahmen im Bereich der Cybersicherheit **genehmigen** und deren **Umsetzung überwachen.**

IT-Sicherheit als Geschäftsleitungspflicht

§ 43 Abs. 1 GmbHG / § 93 Abs. 1 Satz 1 AktG : „Die Geschäftsführer (Vorstandsmitglieder) haben in den Angelegenheiten der Gesellschaft (bei ihrer Geschäftsführung) die **Sorgfalt** eines **ordentlichen (und gewissenhaften) Geschäftsmannes (Geschäftsleiters)** anzuwenden.“

Kern der unternehmerischen Sorgfaltspflichten ist die **Legalitäts- / Legalitätskontrollpflicht**

Zwar muss die Geschäftsleitung nicht selbst „in den Serverraum“, allerdings muss sie durch angemessene **Steuerung, Organisation** und **Kontrolle** dafür Sorge tragen, dass ein angemessenes Informationssicherheitsniveau im Unternehmen gewährleistet ist.

Vertragsgestaltung in der Lieferkette

Schlaglichter der Vertragsgestaltung

Beispiel:

„Der Dienstleister ergreift angemessene technische und organisatorische Maßnahmen, um bei der Erbringung der vertragsgegenständlichen Leistungen die Verfügbarkeit, Unversehrtheit und Vertraulichkeit jeglicher Informationen aus der Sphäre des Kunden zu gewährleisten. Hierfür setzt der Dienstleister dem Stand der Wissenschaft und Technik entsprechende Mittel ein. Der Dienstleister unterhält während der Vertragslaufzeit ein Informationssicherheitsmanagementsystem auf der Basis von ISO/IEC 27001.“

1. Technikklauseln bringen nicht nur Rechtssicherheit

- Best Practice: Festlegung des einzuhaltenden Informationssicherheitsniveaus mithilfe von Technikklauseln
- Allerdings häufig unklar :
  - Was tatsächlich als Maßstab vereinbart ist
  - Welche konkreten Maßnahmen konkret geschuldet sind
  - Welcher Zeitpunkt maßgeblich ist
  - Wer die Kosten bei Anpassungen trägt

Praxistipp:

- Konkrete Definition, was mit Technikklausel gemeint ist
- Vereinbarung eines Kataloges von konkreten (Mindest-) Maßnahmen
- (Ergänzende) Bezugnahme auf konkrete Standards
- Stichwort „jeweils“ und Kostenregelung nicht vergessen

2. Mangelnde Kontrolle und Anreizsteuerung

- Häufig nicht berücksichtigt:
  - Kontrolle, welche IT-Sicherheitsmaßnahmen der Vertragspartner tatsächlich ergreift
  - Informationspflichten / Abstimmung bei IT-Sicherheitsvorfällen
  - Risikoangemessene Haftungssummen

Praxistipp:

- Vereinbarung von Kontrollrechten und Nachweispflichten (einschließlich Pen-Tests)
- Möglichst präzise Regelung von Informationspflichten und Prozessen für die Bewältigung von IT-Sicherheitsvorfällen
- Informationssicherheit ist Kardinalpflicht: Unbeschränkte Haftung / Super Cap bei Pflichtverstößen

3. Zertifikate – auch ISO 27001 – sind nicht alles

- Regelmäßig: Pflicht zur Vorlage von Zertifikaten/Testaten (etwa gemäß ISO 27001) in Bezug auf die Informationssicherheit
- Zertifikate/Testate sind jedoch für eine effektive Kontrolle i.d.R. allein nicht ausreichend:
  - Beziehen sich teilweise (nur) auf Informationssicherheits-Management-Systeme, Bsp.: ISO 27001
  - Geben nur eine Momentaufnahme wieder
  - Unpassender Geltungsbereich (Scope)
  - Fehlende Spezifität/Aussagekraft, Bsp.: Zertifikat nach ISO 27001 ohne Statement of Applicability (SOA)

Praxistipp:

- Regelung, welche weiteren Dokumente neben dem Zertifikat/Testat offengelegt werden müssen
- Vertragliche Festlegung des Anwendungsbereichs
- Pflicht zur regelmäßigen Vorlage aktueller Zertifikate/Testate
- Enge Abstimmung mit IT-Security-Management, welche Standards geeignet sind

4. Unklare Verantwortungsverteilung und Lücken

- Auftraggeber verlassen sich oft allein auf ihre Dienstleister und allgemeine Informationssicherheitsklauseln in Verträgen
- In vielen Fällen unklare oder fehlende Leistungsbeschreibungen und Verantwortlichkeitsregelungen
- Effektive Informationssicherheit erfordert i.d.R. (abgestimmte) Maßnahmen beider Parteien, insbesondere bei Cloud- und Managed-Services

Praxistipp:

- Informationssicherheit bei Leistungsbeschreibung und vertraglicher Verantwortungsabgrenzung mitdenken
- Bei komplexen Sachverhalten Erarbeitung eines dedizierten Modells für die Verantwortungsverteilung im Bereich der Informationssicherheit (Shared Responsibility-Modell)
- Enge Abstimmung mit IT-Security-Management

Save the date!

NOERR

Digital Talks

Agenda & Anmeldeformular finden Sie in Kürze auf unserer Webseite

17. Oktober 2023, *Webinar*
NIS2 und die Auswirkungen auf die Medienbranche

14. November 2023, *Präsenz*
Data & AI Summit, München

21. November 2023, *Webinar*
Cybersecurity und Versicherung

Wenn Sie auch weiterhin Einladungen zu unseren Webinaren, Veranstaltungen und für Sie relevanten Rechtsthemen erhalten möchten, registrieren Sie sich bitte auf www.noerr.com/noerr-news, soweit Sie dies noch nicht getan haben.

FRAGEN UND ANTWORTEN

NOERR

Ihre Noerr Referenten

Lars Meyer (geb. Powierski)
Rechtsanwalt
Senior Associate

+49 40 300397140
lars.meyer@noerr.com

Kompetenzen

- IT-Recht
- Cloud Computing
- Datenschutz
- Softwarelizenzen
- IT-Compliance

Lars Meyer ist auf die rechtliche Beratung im IT-Recht und im Datenschutzrecht spezialisiert. Insbesondere unterstützt er Unternehmen bei der rechtskonformen Umsetzung innovativer Geschäftsmodelle (u.a. KI, DLT, datengetriebene Geschäftsmodelle) sowie im Zusammenhang mit Digitalisierungs- und Outsourcingprojekten, vor allem im Bereich Cloud Computing. Ein weiterer Schwerpunkt seiner Tätigkeit liegt in der Beratung zu IT-Compliance (u.a. Informationssicherheit, KRITIS) sowie der datenschutzrechtlichen Begleitung interner Untersuchungen.

Julian Monschke
Rechtsanwalt
Senior Associate

+49 69 971477 241
julian.monschke@noerr.com

Kompetenzen

- IT-Recht
- IT-Sicherheit
- Datenschutz
- Outsourcings
- Cloud Computing

Julian Monschke berät zu Rechtsfragen des IT-, Cybersecurity- und Datenschutzrechts. Dies umfasst die Vertragsgestaltung und -verhandlung bei allen Formen der Überlassung von Soft- und Hardware. Ein Schwerpunkt von Herrn Monschke ist das Cloud Outsourcing (insbesondere im Sinne der MaRisk) von Unternehmen regulierter Branchen, insbesondere des Finanzsektors. Er berät regelmäßig als Mitglied der Cyber Risks-Gruppe bei aufgetretenen Cybervorfällen sowie zu Fragen des BSIG und der KRITIS-VO. Dabei berät er sowohl präventiv als auch repressiv.