spring EDITION ir 23

Ad-hoc-Pflicht: Ja oder Nein?

Auswirkungen von Cyber-Attacken auf die Finanzkommunikation

SPEAKER:
KATRIN POHL | TIMO HOLZBORN
EQS Group | Orrick

MODERATION:
HENRYK DETER
cometis

PRÄSENTIERT VON:
cometis irclub

Wir danken unseren Hauptsponsoren

Alliance ADVISORS | BAADER | DEUTSCHE BÖRSE CASH MARKET | EQS GROUP | mms solutions | SILVESTER GROUP | TaylorWessing

» Ad-hoc-Pflicht: Ja oder Nein? «

Auswirkungen von Cyberattacken auf die Finanzkommunikation - 28.03.2023

» Agenda «

1. Cyberangriff – Was ist das überhaupt?
2. Motivation, Ziele, Typen & Auswirkungen
3. Bekannte Cyberangriffe auf börsennotierte Unternehmen
4. Impulse für die Finanzkommunikation bei Cyberattacken
5. Ad-hoc-Pflicht: Ja oder Nein?
6. Empfehlungen für die Kommunikation
7. Problemkreise aus Pflichten (Ad-hoc & Datenschutz)
8. Fragen und Antworten

» Cyberangriffe sind unerbetene Versuche, Informationen durch unbefugten Zugriff auf Computersysteme zu stehlen, offenzulegen, zu ändern, zu inaktivieren oder zu vernichten. «

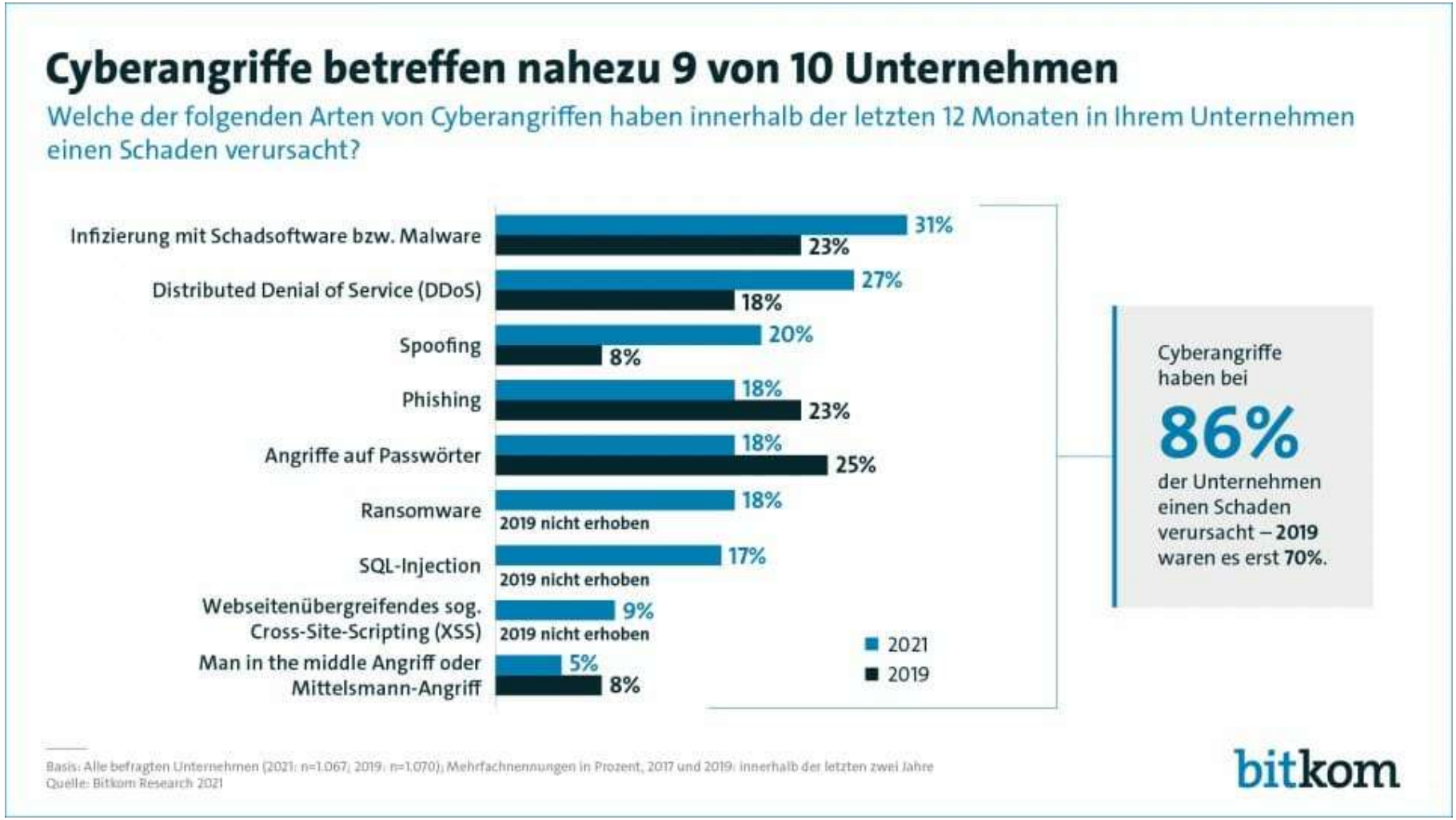
» Motivation – Was steckt hinter einem Cyberangriff

- Kriminelle Motivation: finanzieller Gewinn durch Diebstahl von Daten bzw. Geldmitteln, Lösegeldforderung
- Politische Motivation: Aufmerksamkeit für ihre Sache erregen („Hacktivismus“)
- Persönliche Motivation: Geld, Daten oder zur Störung eines Unternehmenssystems („Vergeltung“)
- Spionage: Vorteil ggü. Konkurrenz oder auch politisch motiviert

» Ziele, Typen & Auswirkungen

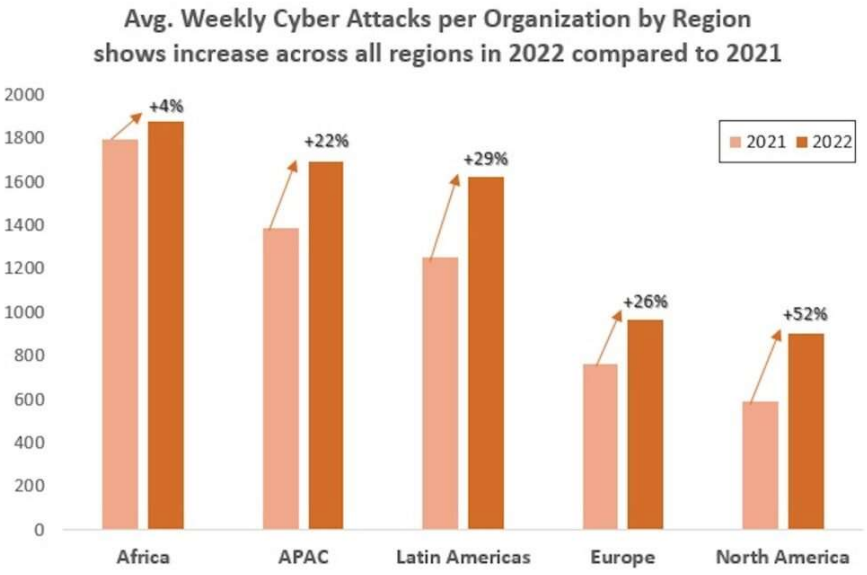
- Finanzdaten von Unternehmen & Kunden
- Kundenlisten, persönliche Kundendaten
- E-Mail-Adressen und Anmeldedaten
- Geistiges Eigentum, wie z. B. Geschäftsgeheimnisse oder Produktdesigns
- Zugriff auf die IT-Infrastruktur
- IT-Services, um Geldzahlungen zu akzeptieren
- Sensible personenbezogene Daten, u.v.m

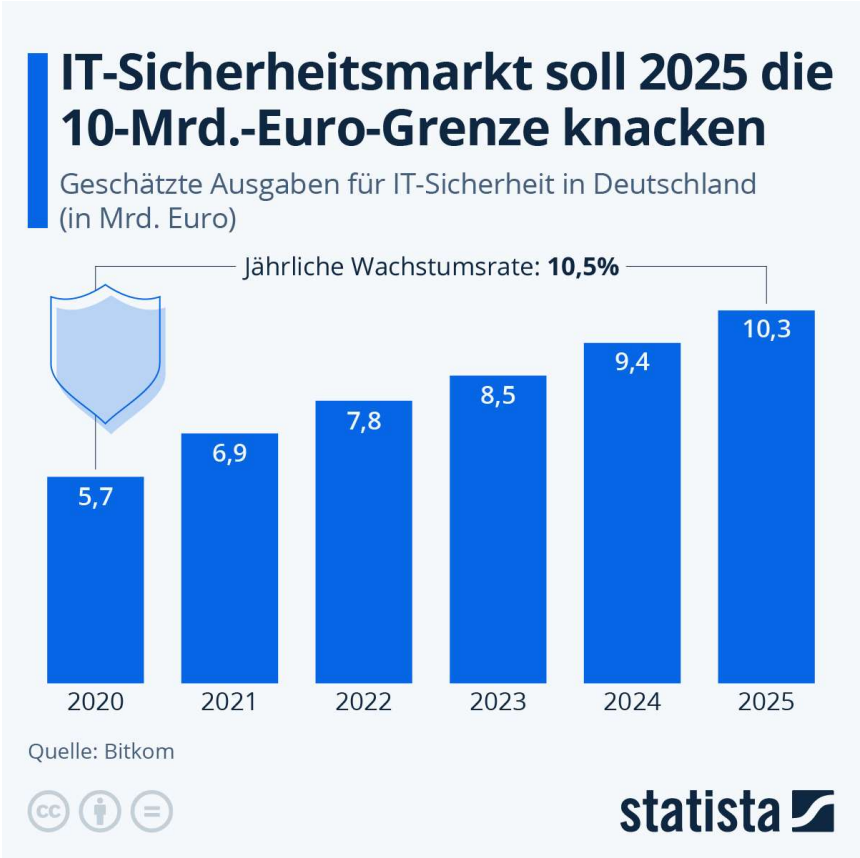
- DoS-, DDoS- und Malware-Angriffe → System- oder Serverabstürze
- SQL-Injection-Angriffe → Datenänderung, Datenklau oder Datenlöschung.
- Phishing → Zugriff auf Systeme oder persönliche Daten
- Ransomware-Angriffe → Verschlüsseln/Lahmlegen des Systems oder Datenklau inkl. Lösegeldforderung



https://www.digitalbusiness-cloud.de/it-sicherheit-cyberangriffe-verursachen-jaehrlich-220-milliarden-euro-schaden/

» Anzahl Cyberattacken vs. Ausgaben für IT-Sicherheit





» Cyberangriffe – Auszug bekannter Fälle

Ransomware-Angriff bei Dax-Konzern

Hacker stehlen offenbar 40 Terabyte von Continental

Die berüchtigte Cybercrime-Gruppe Lockbit hat laut einem Medienbericht den deutschen Autozulieferer Continental erpresst. Die Täter hatten demnach zuvor große Mengen an Unternehmensdaten entwendet.

IT-Sicherheit

Hacker verüben Angriff auf Werkstoffsparte von Thyssenkrupp

Unbekannte haben den Stahlkonzern Thyssenkrupp ins Visier genommen. Die Kriminellen seien aber rechtzeitig erwischt worden, heißt es in Essen.

DDoS-Angriff

Rheinmetall wehrt Cyberattacke weitgehend ab

M-DAX-KONZERN

Hacker-Angriff auf Kupferhütte Aurubis

AKTUALISIERT AM 28.10.2022 - 17:13

Hackerangriff bei Windturbinenhersteller Nordex

Finanzdienstleister Equifax

Hacker erbeuten Daten von bis zu 143 Millionen US-Bürgern

Auf den US-Finanzdienstleister Equifax ist ein Hackerangriff verübt worden, betroffen sind wohl 143 Millionen US-Bürger. In Hunderttausenden Fällen ging es um sensible Daten wie Sozialversicherungs- oder Kreditkartennummern.

Cyberangriff auf deutschen Baustoffproduzent

Der Baustoffhersteller Steico ist Ziel einer Cyberattacke geworden. Sowohl die Produktion als auch die Verwaltung sind betroffen.

» Impulse für Ihre Finanzkommunikation bei Cyber-Attacken «

» Können Sie bestätigen, dass Sie Opfer eines Cyber-Angriffs geworden sind? «

» Fragen zunächst intern stellen und beantworten

- Was wissen wir über Art und Umfang des Angriffs? Besteht Gefahr für Leib und Leben? Gibt es konkrete Einschränkungen oder Unterbrechungen im Geschäftsbetrieb? Sicherheitslücken? Sind Kundendaten betroffen? Seit wann läuft der Angriff?
- Wo stehen wir aktuell? Was haben wir bereits unternommen? Was sind die nächsten Schritte?
- Ist das Thema bereits öffentlich bekannt? Bestehen Gerüchte in den sozialen Medien? Gibt es eine Anfrage dazu von extern? Wie verhält sich der Aktienkurs?
- Welche juristischen Aspekte sind betroffen? Sind wir veröffentlichungspflichtig?

» Ad-hoc-Pflicht: Ja oder Nein? «

» Anknüpfung für Ad-hoc Publizitätspflicht Art 17 MAR

- Insiderinformation Art. 7 (1) MAR: *"Nicht öffentlich bekannte präzise Information, die direkt oder indirekt Emittent oder Finanzinstrument betreffen, und die, wenn öffentlich bekannt, geeignet, den Kurs dieser Finanzinstrumente oder damit verbundener Derivate erheblich zu beeinflussen."*
  d.h. solche , die ein verständiger Anleger wahrscheinlich als Teil der Grundlage seiner Anlageentscheidung nutzen würde.

- BaFin-EmittentenLF 2020: Umfassende Darstellung mit offenen Beschreibungen

- Kursbeeinflussungspotential hängt ab von Markterwartung und Abschätzung der Auswirkungen Finanzieller Schaden und Reputationsschaden

- Ad-hoc Publizität: Art. 17 (1) MAR: Gleichlauf mit Insiderbegriff bei unmittelbarer Betroffenheit

- Informationslecks oder Gerüchte (egal von wem) beenden selbst Aufschub

» Weitere Pflichten aus Datenschutz und Cyber Gesetzen

- **In Deutschland**: Ggf. Informationspflichten aus Datenschutzrecht oder aus Cyber-Gesetzen gegenüber Aufsichtsbehörden und auch Betroffenen zu berücksichtigen.
  Problem: Ad-hoc Pflicht ist nur schwer aufschiebbar, aber nur abgestimmte Kommunikation (Inhalt und Zeitpunkt) vermeidet Probleme mit anderen Aufsichtsbehörden, Öffentlichkeit und Betroffenen (z.B. Kunden, Lieferanten)

- **Bei Aufstellung in mehreren Jurisdiktionen**: Schnelle Verschaffung eines Überblicks über in Betracht kommende Pflichten zur Veröffentlichung aber auch zur Vertraulichkeitswahrung, um widerstreitende Pflichten sachgerecht abwägen zu können.

- **Klageindustrie/Abmahner** suchen nach Datenpannen, kaufen mögliche Schadensersatz-forderungen gegen Unternehmen von Betroffenen auf und machen diese geltend. Denn selbst kleine datenschutzrechtliche Verstöße können zu 2.500 oder 5.000 Euro Schadensersatz führen (immaterieller Schadensersatz): **Beispiel:** Scalable

» ... und dann umsichtig kommunizieren

- Bereiten Sie sich heute bereits vor! Identifizieren Sie Ihre individuellen Top-Risiken. Definieren Sie u.a. die Bagatellegrenze, ab der Sie planen, extern zu kommunizieren
- Verlieren Sie nicht unnötig Zeit! Und managen Sie die Kommunikation aktiv anstatt „es laufen zu lassen“. Sonst überholt Sie ggf. die Gerüchteküche.
- Geben Sie regelmäßige Updates und berichten Sie auch über den Abschluss des Angriffs.
- Quantifizieren und qualifizieren Sie die Auswirkungen des Angriffs und sagen Sie, was Sie getan haben und noch tun werden, damit das nicht wieder passiert.

» Problemkreise für Ad-hoc Publizitätspflicht Art 17 MAR

- **Gerücht** ist präzise Information i. S. d. Art. 7 (1) a) MAR, muss aber nicht wahr sein. Falsche Gerüchte müssen ggf. korrigiert werden.

- Ggf. kann Information als **Zwischenschritt** in einem Erkenntnis Prozess gesehen werden, aber: "*Kursbeeinflussungspotenzial umso eher anzunehmen, je gewichtiger und wahrscheinlicher das Endereignis ist und eine Gesamtbetrachtung der eingetretenen und zukünftigen Umstände unter Berücksichtigung der jeweiligen Marktsituation nahelegt, dass ein verständiger Anleger bereits diesen Zwischenschritt für sich nutzen werde.*"

- Bei **Ermittlungs-, Verwaltungs- und Gerichtsverfahren** gilt: wenn feststeht, dass Emittent oder für ihn tätige Person Gesetzesverstöße begangen haben, ohne dass eine behördliche Entscheidung vorliegt, spielt bei Beurteilung des Kursbeeinflussungspotenzials wesentliche Rolle, welche rechtlichen und finanziellen Konsequenzen sich aus dem Verstoß für den Emittenten ergeben.

» Aufschub der Ad-hoc Publizität zulässig

- Bei "berechtigten Interessen" des Emittenten, Art. 17(4) (Beeinträchtigung der berechtigten Interessen ist ausreichend, Schaden nicht erforderlich)
- Laufende Verhandlung (insb. finanzielle Überlebensfähigkeit/Vereitelung Abschluss), mehrstufige Entscheidungs-prozesse Art. 17(4), Zwischenschritt gestreckter Vorgang, geistiges Eigentum (Patent/Erfindung); § 6 WpAIV, EG 50 MAR, ESMA 2016/1130 mit nicht abschließendem Katalog
- Unterlassung nicht geeignet, Öffentlichkeit irrezuführen, nicht: Kursschwankungen zu vermeiden oder Veröffentlichung etwaiger negativer Auswirkungen (Reputationsschaden) zu verzögern
- Emittent kann Geheimhaltung sicherstellen (Problem: Offenlegung nach anderen Gesetzen)
- Beschlusserfordernis, mindestens ein Vorstandmitglied (nach BaFin)
- Umfangreiche Dokumentation DelVO (EU) 2016/1055
- Aufschub endet, sobald die Vertraulichkeit, beispielsweise durch Informationslecks oder Gerüchte (egal von wem), nicht mehr gewährleistet, Art. 17(7)

» Problemekreise aus Pflichten aus Datenschutz und Cyber Gesetzen

- (Strafverfolgungs-)**Behörden** verfolgen eigene Interessen, welche nicht unbedingt mit den Interessen der betroffenen Unternehmen übereinstimmen. Das kann zu fehlender Vertraulichkeit, Problemen mit Ransom-Erpressern und der öffentlichen Kommunikation führen.

- Häufig wird übersehen, dass **Kommunikation, die nicht über Anwälte geführt wird**, in Ländern mit Common Law (US/UK/AUS), herausverlangt werden und dann gegen das Unternehmen genutzt werden kann. Um diesem Problem zu begegnen, sollten IT-Forensiker und sonstige Dienstleister über Anwälte beauftragt werden.

» Fragen & Antworten «

» Vielen Dank für Ihre Aufmerksamkeit «

Katrin Pohl
Head of Account Management Investor Relations
katrin.pohl@eqs.com

Dr. Timo Holzborn
Partner Orrick, Herrington & Sutcliffe LLP
tholzborn@orrick.com

Henryk Deter
Vorstand cometis AG
deter@cometis.de

EQS GROUP

Follow us:

www.eqs.com

PRÄSENTIERT VON: cometis irclub