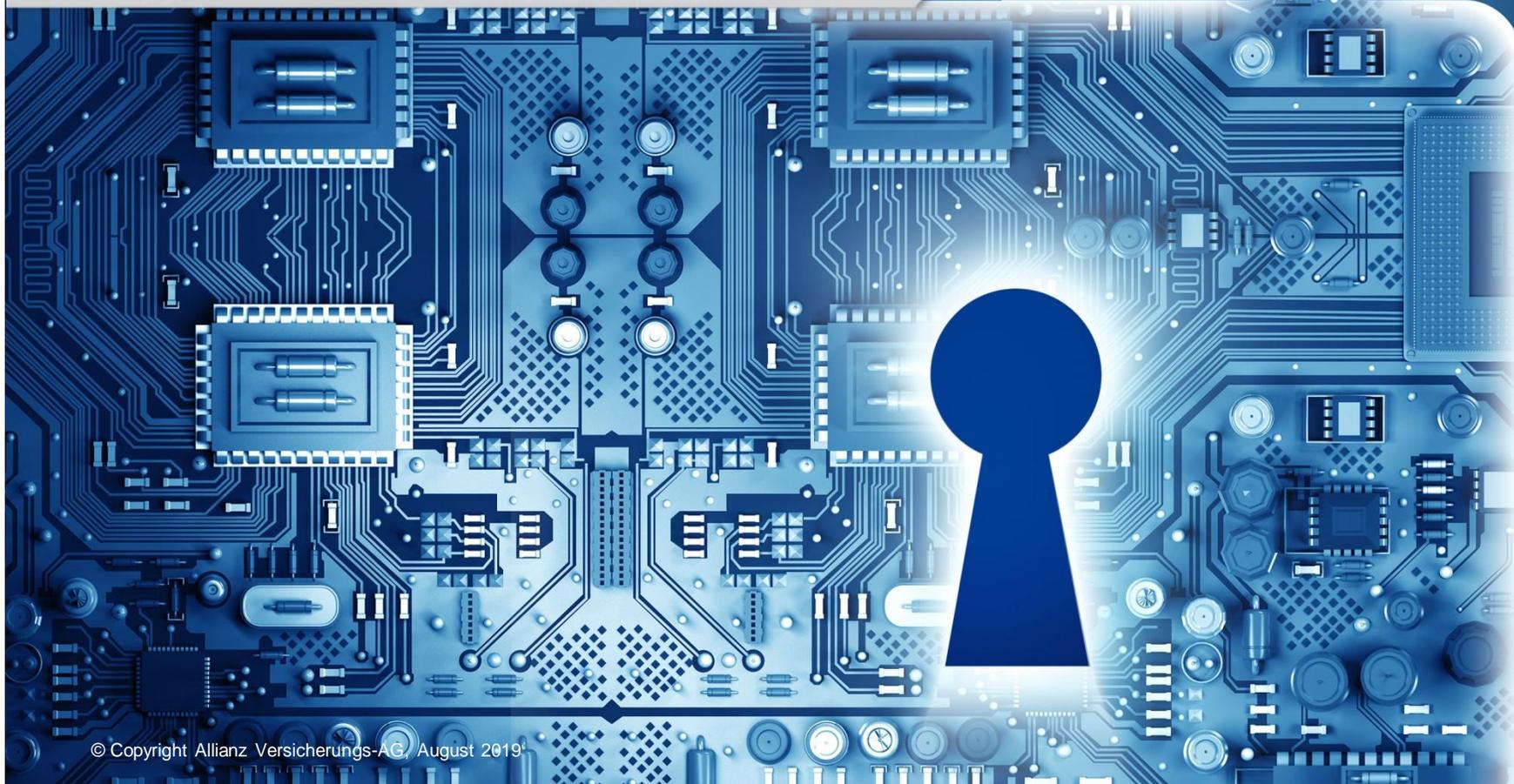


Cyber-Risiken und Bedrohungen in der Praxis aus der Sicht des Versicherers

Wirtschaftsförderung Lübeck 08.08.2019



WELCHEN STELLENWERT NIMMT DAS CYBER-RISIKO BEI DEN UNTERNEHMENSRISIKEN EIN?



Allianz Risk Barometer 2018 TOP 10 UNTERNEHMENSRISIKEN NACH REGIONEN 2018: EUROPA



○ 2017: 35% (1)
Betriebsunterbrechung
(inkl. Lieferkettenunterbrechung)



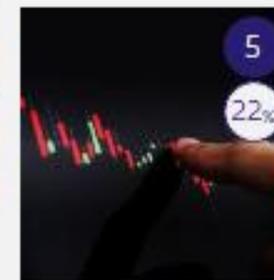
○ 2017: 32% (2)
Cyberfälle
(z.B. Cyberkriminalität, Systemausfall, Verletzung der Datenschutzrechte)



○ 2017: 28% (4)
Rechtliche Veränderungen
(z.B. Wirtschaftssanktionen, Regierungsveränderungen, Protektionismus, Brexit, Zerfall der Euro-Zone)



○ 2017: 21% (6)
Naturkatastrophen
(z.B. Sturm, Überschwemmung, Erdbeben)



○ 2017: 32% (3)
Marktentwicklungen
(z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktfluktuation)

WELCHES SIND DIE HÄUFIGSTEN SCHADENSARTEN

1. Beeinträchtigung des Computersystems 75%
2. Cyber-Erpressung (*Verschlüsselung*)
3. Datenschutzverletzung
4. Datenmanipulation (*Telefonmehrkosten*)

WELCHES SIND DIE MOTIVE WARUM UNTERNEHMEN ANGEGRIFFEN WERDEN

Spaß, Mut, sich selbst und anderen etwas zu beweisen.

Sabotage (Produktionsausfall) oder Rache auch durch ehemalige Mitarbeiter

Know-how erwerben durch gezielte Spionage.

Geld, z.B. durch:

- Auftragsprogrammierung für Dritte,
- Vermietung von Botnets, damit Dritte D-Dos Attacke durchführen können.
- Lösegelder durch Verschlüsselungstrojaner, Verkauf von Zugangsdaten, Passwörtern, Pay-Pal Guthaben etc.

WIE KANN DER VERSICHERER BEIM RISIKOMANAGEMENT HELFEN?

Durch Formulierung von IT Mindeststandards für die Versicherbarkeit

Existiert ein Datenschutzbeauftragter?

Existiert eine IT-Sicherheitsorganisation mit definierten Rollen und Verantwortlichkeiten?

Erfolgt eine Sensibilisierung der Mitarbeiter zur Informations- und Cyber-Sicherheit?

Werden durch Sie oder einen IT-Dienstleister nicht zwingend notwendige Softwarebestandteile und Funktionen des Computersystems entfernt bzw. deaktiviert (Härtung)?

Gibt es einen Schutz vor Schadcodes (Virens Scanner)?

WIE KANN DER VERSICHERER BEIM RISIKOMANAGEMENT HELFEN?

Durch Formulierung von IT Mindeststandards für die Versicherbarkeit

Existieren Verfahren zum Patch- und Schwachstellenmanagement?

Werden regelmäßig Backups durchgeführt?

Werden Wiederherstellungstests von Backups regelmäßig durchgeführt?

Wie werden externe Zugänge abgesichert?

Sind Vorgaben zur Passwortqualität umgesetzt?

Gibt es einen Zutrittsschutz zu Gebäuden oder IT-Sicherheitszonen?

AKTUELLE SCHADENFÄLLE

Crypto-Miner Systemauslastung

Crypto Miner sind Softwareanwendungen zur Erzeugung von Crypto Währungen.

Durch den Angriff auf einen Server kam es zu Systemauslastungen mit der Folge, dass Websites nicht mehr erreichbar waren.

Es sind forensische Untersuchungen erforderlich um festzustellen, wer der Eindringling ist, wie und wo dies erfolgt ist, wie die Schadsoftware endgültig entfernt werden kann, ob der Server zusätzlich in anderer Weise missbraucht wurde (z.B. Spaming) bzw. allgemein um weiteren Schaden abzuhalten.

Erste Rechnungen des Forensik-Unternehmen i.H.v. 74.244,38 EUR liegen vor.

AKTUELLE SCHADENFÄLLE

VERSCHLÜSSELUNGSVIRUS- KRYPTOTROJANER

Angriff durch einen Verschlüsselungstrojaner auf einen Dienstleister im internationalen Warenverkehr/Spedition/Handelsunternehmen

Betroffen bzw. beeinträchtigt sind Datenbanken, Laufwerke und Computer. Betriebsunterbrechung ca. 3 Stunden.

Es wurde unverzüglich der IT-Dienstleister eingeschaltet, der Sofortmaßnahmen durchgeführt hat (Löschen der Festplatten, Neuaufspielen des Systems und Rekonstruktion von Daten aus Backup)
Schadenaufwendungen rd. 10.000 EUR

AKTUELLE SCHADENFÄLLE

HACKER ERPRESSEN DEUTSCHE FIRMA MIT GESTOHLLENEN DATEN

Hacker sind in ein großes deutsches Internetinfrastrukturunternehmen eingebrochen, das Dienstleistungen für Dutzende der größten und wertvollsten Unternehmen der Welt anbietet.

Dabei seien Daten von Kunden erbeutet worden. Die Hacker versuchten nun das Unternehmen zu erpressen. Die Angreifer haben demnach gedroht, Daten von den betroffenen Kunden zu veröffentlichen. Eine entsprechende Meldung an die Datenschutzbehörde ist erfolgt und die Kunden wurden umgehend über den Cyberangriff sowie den Datenabfluss informiert und es herrschte von Anfang an volle Transparenz.

AKTUELLE SCHADENFÄLLE

Telefonmehrkosten – IP Telefonie gehackt.

In der Nacht von Freitag auf Samstag wurde die Telefonanlage einer Hochschule gehackt und für massenhaftes Absetzen von Telefonanrufen (überwiegend nach Albanien) missbraucht.

Der Telefonanbieter bestreitet ein Mitverschulden.

Geltend gemacht werden 5.833,96 EUR Telefonmehrkosten, die der Hochschule vom Telefonanbieter in Rechnung gestellt wurden.

Vielen Dank!

Carsten Hoffmann
Fachreferent Haftpflicht- und Cyberversicherung
Allianz Deutschland AG
Tel: 040-69469-27021
Mobil: 0152- 09018433