valantic

claranet®

Der Tag wird kommen – Wie Sie aus den Fehlern anderer lernen können

Frankfurt, 3. Juli 2025

Vorstellung

Thomas Lang
Geschäftsführer | Partner

Mitglied im Aufsichtsrat
Volksbank Mittelhessen eG, seit 2024

Partner
valantic GmbH

Geschäftsführer
valantic Management Consulting GmbH,

Landesvorstand Hessen
Wirtschaftsrat Deutschland, seit 2010

verheiratet, 1 Tochter
wohnhaft im Rhein-Main-Gebiet

Bankkaufmann
Ausbildung 1997, Sparkasse Marburg-Biedenkopf

valantic

+4,000
Expert*innen

Ø14
Jahre Projekterfahrung

€ 600mn
Umsatz in 2025e

> 50
Standorte

+500
Blue Chip-Kunden

99%
Kundenbindung

Cyberangriffe zählen – nach wie vor – zu den Top Geschäftsrisiken

Quelle: Allianz Risiko Barometer 2025, Top 10 Geschäftsrisiken für Deutschland

Cybervorfälle wie Ransomware-Angriffe, Datenschutzverletzungen und IT-Ausfälle rangieren im Allianz Risk Barometer (2025) an erster Stelle der globalen Risiken – und das zum wiederholten Male.

Cyber-Angriffe werden sichtbar, passiert sind sie vorher!

CYBERANGRIFF

Hacker legen Autozulieferer EDAG lahm

Der Entwicklungs-Dienstleister aus Fulda hat große Teile seiner IT abgeschaltet, um die sensiblen Kundendaten zu schützen. Die Behörden ermitteln.

Jens Koenen

15.03.2021 · 11:54 Uhr • 11 x geteilt

manager magazin

NEWS

RSS ARCHIV

DFB WURDE OPFER EINES CYBERANGRIFFS

Der Deutsche Fußball-Bund (DFB) ist Opfer eines Cyberangriffs geworden. Der Vorfall ereignete sich am Anfang dieser Woche. Als Sofort- und Vorsichtsmaßnahmen wurden die DFB-IT-Systeme heruntergefahren inklusive aller Netzwerkkomponenten. Betroffen waren lediglich die Office-IT des DFB - weder das DFBnet noch FUSSBALL.DE.

IT-SYSTEME ABGESCHALTET

Cyberangriff auf Deutsche Leasing

VON MAXIMILIAN SACHSE - AKTUALISIERT AM 06.06.2023 - 16:57

Der Leasinganbieter der Sparkassen hat wegen eines Cyberangriffs seine IT-Systeme abgeschaltet. Das Unternehmen ist damit aktuell faktisch lahmgelegt.

Folgen unklar

Cyber-Angriff auf Kupferkonzern Aurubis

Europas größte Kupferhütte Aurubis ist zum Ziel eines Hacker-Angriffs geworden. Die IT- Systeme wurden daraufhin präventiv heruntergefahren und vom Internet getrennt.

ZEIT ONLINE

Politik Gesellschaft Wirtschaft Kultur • Wissen Gesundheit • Digital Campus • Arbeit Sport ZE

Kriminalität

Tegut spürt weiter Folgen von Cyberangriff

5. Mai 2021, 14:57 Uhr / Quelle: dpa /

Fulda (dpa/lhe) - Die Supermarktkette Tegut bekommt die Auswirkungen eines Cyberangriffs auf das IT-Netzwerk des

---

tagesschau Sendung verpasst?

Produktion lahmgelegt

Symrise Opfer von Cyberattacke

Stand: 15.12.2020 12:13 Uhr

Symrise, einer der weltweit größten Hersteller von Geruchs- und Geschmacksstoffen, ist Opfer einer Hackerattacke geworden. Der Anschlag war so heftig, dass die Produktion vorübergehend eingestellt werden musste.

TextilWirtschaft

Business — Fashion

Suchbegriff eingeben

TOP-THEMEN Top-Personalien Chancen in der Krise Online-Plattformen Umsätze TW-Testclub

Home > Business > News

TW+ CYBER-KRIMINALITÄT

Nach Hacker-Angriff: Immer noch kein Normalbetrieb bei Marc O'Polo

Von Jelena Faber
Dienstag, 24. September 2019

Zehn Tage nach dem Cyber-Angriff auf Marc O'Polo ist die Welt in Stephanskirchen noch lange nicht in Ordnung. Immerhin: „Wir sind handlungsfähig und fahren seit einigen Tagen unsere Kernsysteme sukzessive hoch. Die wesentlichen Teile unserer IT-Systeme sind

valantic

Wann werden Cyberangriffe sichtbar – und was passiert davor?

Wertschöpfungsketten von Cyberkriminellen

Zunehmende **Professionalisierung** von Cyberkriminellen über **Modularisierung** und **Arbeitsteilung**

Forschung & Entwicklung

Schwachstellenforscher: Identifizieren Schwachstellen in Software und Systemen.

Malware-Entwickler: Entwickeln Schadsoftware, die für Angriffe und insbesondere den Initial Access verwendet wird.

Initial Access & Verbreitung

Initial Access Broker: Verkaufen Zugang zu bereits kompromittierten Systemen.

Spammer und Phisher: Versenden schädliche E-Mails oder Nachrichten, um Malware zu verbreiten oder Zugangsdaten zu erlangen.

Ausführung des Angriffs

Exploit-Entwickler: Spezialisieren sich auf die Entwicklung von technischen Exploits

Attack Operators: Führen die Angriffe durch, unter Verwendung von gekauften Exploits oder Zugangsdaten

Datendiebstahl- & Handel

Datenhändler: Spezialisieren sich auf den Kauf und Verkauf gestohlener Daten.

Informationsbroker: Aggregieren und verkaufen spezifische Informationen, die aus verschiedenen Quellen stammen.

Monetarisierung

Ransomware-Operatoren: Verschlüsseln Daten und fordern Lösegelder.

Finanzspezialisten: Spezialisten, die sich mit Geldwäsche und dem Transfer von digitalen Währungen beschäftigen.

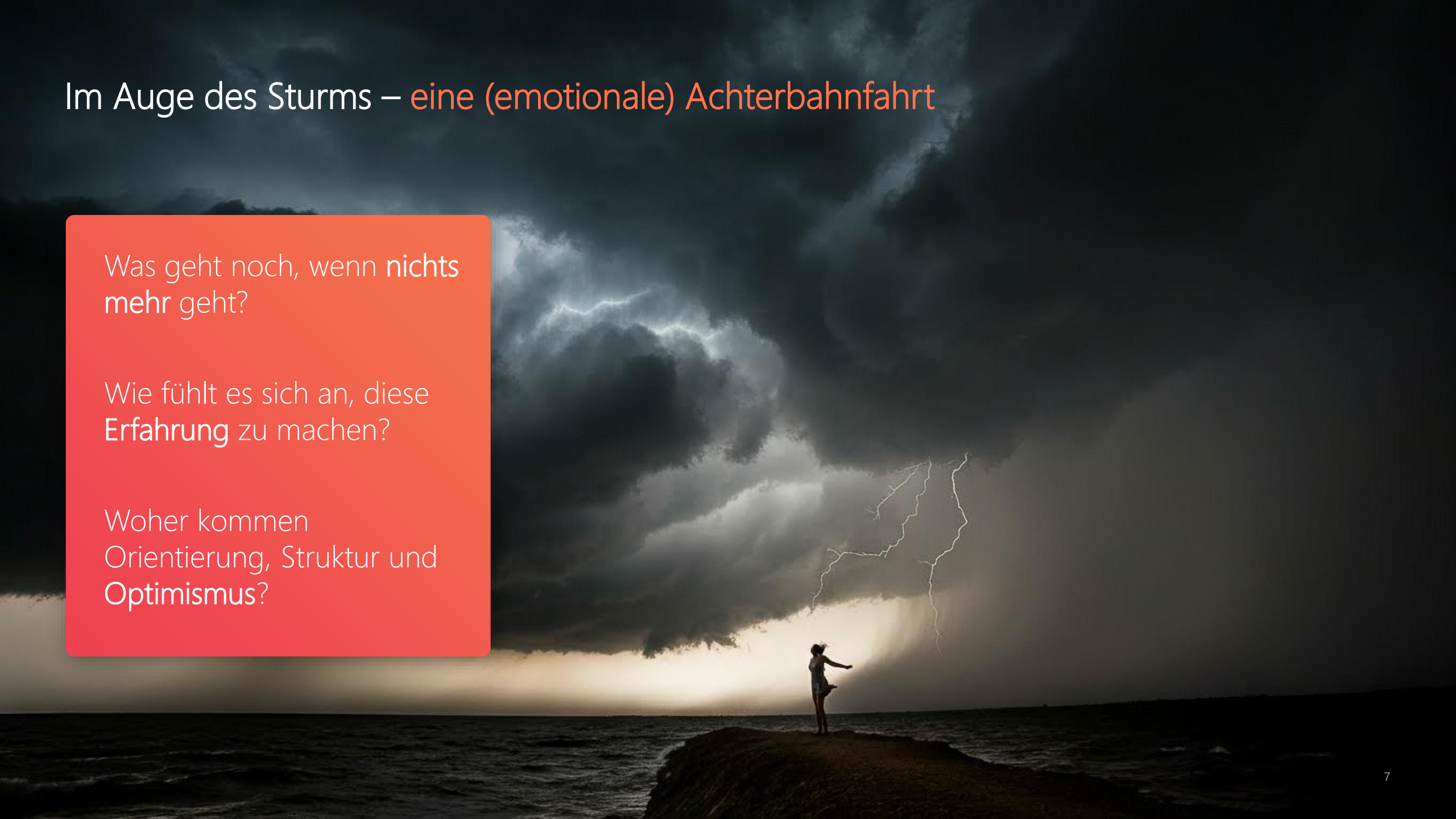
Unterstützende Dienste

Hosting-Dienste: Bieten anonyme Hosting-Lösungen, unteranderem im Darknet an.

Sicherheitsexperten: Bieten Schutzdienste für die Infrastrukturen und Operationen anderer krimineller Akteure.

valantic

Im Auge des Sturms – eine (emotionale) Achterbahnfahrt



Was geht noch, wenn **nichts mehr** geht?

Wie fühlt es sich an, diese **Erfahrung** zu machen?

Woher kommen Orientierung, Struktur und **Optimismus**?

Ein einfaches Beispiel

> Ich sehe was, was Du nicht siehst…


Wo stand noch mal die Palette?

Wie würde sich das für Ihr Unternehmen anfühlen?

Die 3 wichtigsten Geschäftsprozesse

Ich erreiche alle relevanten Personen

Ein Tag Ausfall kostet X

Wir können Y Tage ‘überleben’

Zusätzliche Herausforderungen

> Als wäre der Stillstand des Unternehmens nicht schon genug

Fokus Ransomware-Attacken

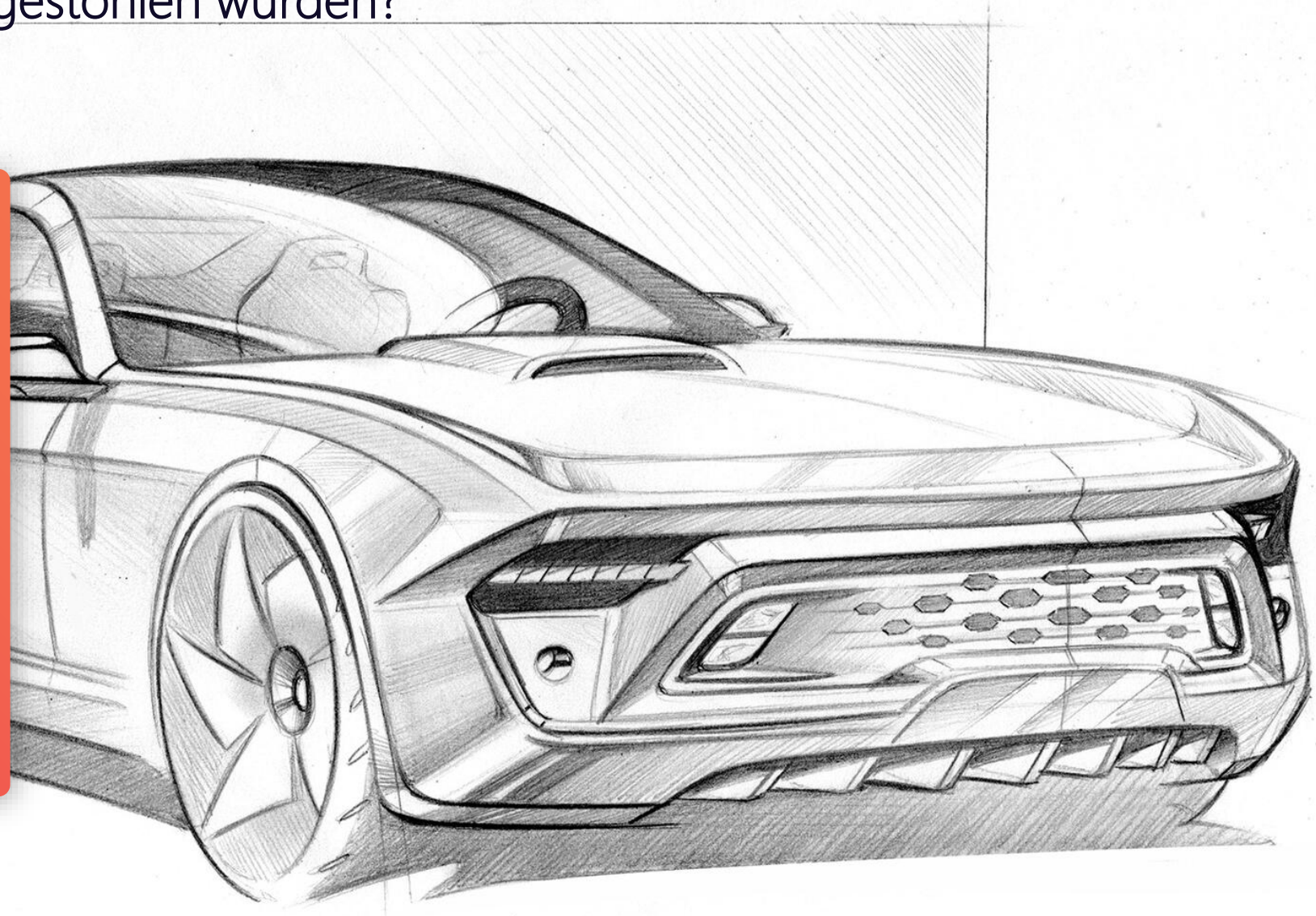
Verschlüsselung und/oder Datendiebstahl – Double- bzw. Triple Extortion

- Eingespielte Schadsoftware
- Anschliessende Erpressung von Lösegeld
- Bei Nichtbezahlung potenzielle Veröffentlichung der Daten im Internet
- Ggfs. Verkauf der Daten

Was, wenn sensitive Daten gestohlen wurden?

Potenziell für Angreifer interessante Daten

- Design-Entwürfe
- Kundendaten
- Das streng geheime Limonadenrezept eines Getränkeherstellers …



valantic

Welche möglichen Rechtsfolgen ergeben sich daraus?

valantic

Fazit

> Die IT ist zwar das Einfallstor, betroffen ist jedoch das gesamte Unternehmen

Die Frage aller Fragen

> (Wie) Gibt es 100%ige Sicherheit?

Beispiel 1: Sicherheit heißt (auch) Ordnung halten

> Wie viele General-schlüssel zu Ihrer IT gibt es?

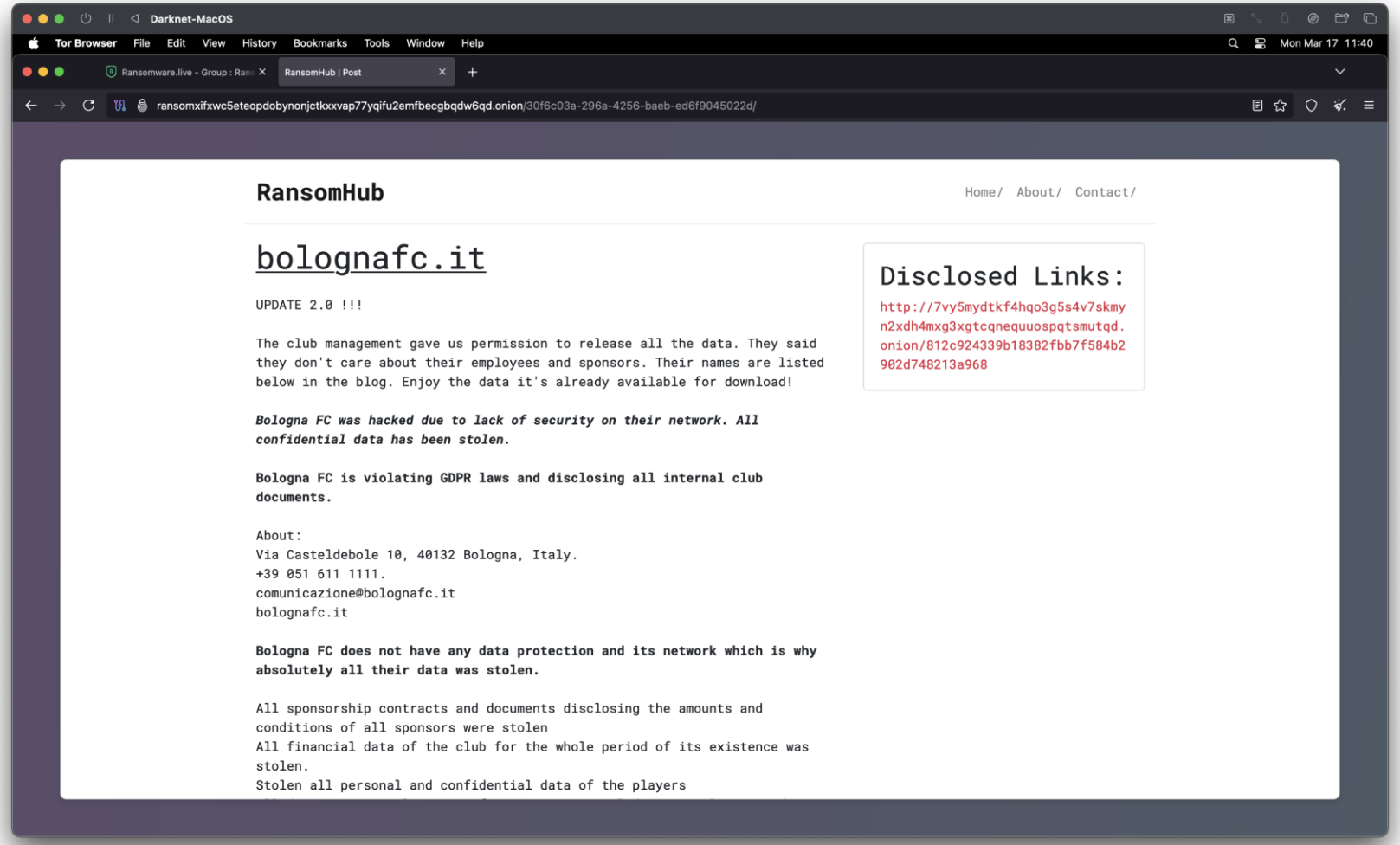
Beispiel 2: Sicherheit heißt (auch) vorbereitet sein

> Gibt es ein erprobtes Business Continuity Management?

Beispiel 3: Wissen Sie, was (im Darknet) über Sie gesprochen wird?

Im November 2024 wird Bologna FC gehackt und interne Daten werden veröffentlicht:

- Die Gruppe RansomHub nutzt den sogenannten Double Extortion Mechanismus, wobei Systeme verschlüsselt werden und parallel sensitive Daten abgegriffen werden.
- 200 GB gestohlene Daten werden Angeboten. Unter anderem die Reisepässe des Trainers, Sponsorenverträge, sowie vertrauliche Daten von Spielern, Mitarbeitern und Fans.
- Die Gruppe droht auch zu veröffentlichen, dass der Verein FIFA und UEFA-Richtlinien bricht. Dieses "Aufdecken von Missständen" ist typisch für Ransomware Gruppen.



valantic

Drei wichtige Fragen …

1. Wo steht Ihre IT in Bezug auf das Thema Cybersecurity wirklich?
2. Gibt es Notfallprozesse, die den Namen verdienen?
3. Haben Sie die Partner unter Vertrag, die in der Krise helfen oder fangen Sie dann an, in Telefonbüchern und Erinnerungen zu graben?

valantic

… und drei konkrete Empfehlungen

1. Machen Sie das Thema zur Chef-Sache
2. Bauen Sie Steuerungssysteme für das Thema Cybersecurity auf (wenige, nicht-technische KPIs).
3. Stellen Sie Transparenz her und etablieren Sie Frühwarnsysteme.

Herzlichen Dank

THOMAS LANG

Geschäftsführender Partner

+49 171 680 4635

thomas.lang@mc.valantic.com

valantic