



# Die 3 Säulen der Cyber-Sicherheit für Ihr Unternehmen

ImmoWebinar der WKO powered by GROSS Versicherungsmakler GmbH  
Mittwoch, 19. Juni 2024

CYBER IS US<sup>®</sup>

# Zu meiner Person

---

**Kurt Kalla, Akad.Vkfm.**

Chief Sales Office Austria

COGITANDA Dataprotect AG  
Niederlassung für Österreich

Über 30 Jahre Berufserfahrung in der  
Versicherungsbranche



# Das erwartet Sie heute

---

1. Zahlen & Fakten zur Bedrohungslage
2. Die 3 Säulen Ihrer Cyber-Sicherheit
3. Was wir für Sie tun können

# Lagebericht des BMI

Auszug aus dem Cybercrime-Report des österreichischen Bundesministerium für Inneres



■ Aufklärungsquote ■ Anzahl der angezeigten Straftaten

Quelle: Cybercrime-Report Bundeskriminalamt, 17. Mai 2023

# Dynamik von Cyber-Vorfällen

## Key-Findings KPMG Cyber Studie Österreich 2023 (Auszug)

- Cyber-Angriffe haben in den letzten 12 Monaten um 201 Prozent zugenommen
- 63% der Unternehmen sind der Ansicht, dass die Cyber-Angriffe auf ihr Unternehmen in den nächsten 12 Monaten zunehmen werden
- 55% der Befragten sagen, dass Cyber-Angriffe ihre geschäftliche Existenz bedrohen
- 33% der Unternehmen berichten von einer Betriebsunterbrechung aufgrund eines Ransomware-Angriffs von rund einer Woche
- 12% der Unternehmen erlitten einen finanziellen Schaden von mehr als 1 Mio. EUR durch Cyber-Angriffe



Quelle: KPMG Cyber Studie 2023 Österreich

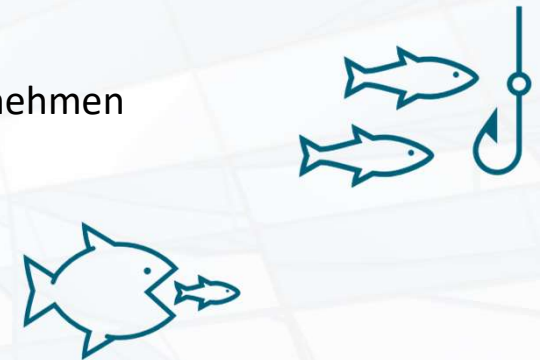
Mittwoch, 19. Juni 2024

COGITANDA GROUP

# Neuer wirtschaftlicher Alltag?

## Key-Findings KPMG Cyber Studie Österreich 2023 (Auszug)

- Bei 63% der Befragten sind Angriffe auf Zulieferer und/oder Kundensysteme normales Tagesgeschäft
- 80% der Unternehmen sehen CEO-Fraud als normales Tagesgeschäft
- 100% haben in den letzten zwölf Monaten Phishing-Attacken erlebt
- 14% der Befragten wissen nicht, ob erfolgreiche Cyber-Attacken gegen ihre Unternehmen stattgefunden haben



Quelle: KPMG Cyber Studie 2023 Österreich

Mittwoch, 19. Juni 2024

COGITANDA GROUP

# Bekannte Cyber-Vorfälle in Österreich

## Auszüge aus der Berichterstattung

### Cyberangriff auf Kärnten: Die wichtigsten Fakten zum aktuellen Fall

Widersprüchliche Aussagen des Landes haben für viel Unsicherheit bei den Betroffenen gesorgt. Nach den Angriffen der Hackergruppe "Black Cat" bleiben viele Fragen offen.

Alexander Amon  
7. Juni 2022, 15:08

Frage: Worum geht es eigentlich?

Antwort: Das Land Kärnten hat am 25. Mai – ironischerweise der vierte Jahrestag des Inkrafttretens der Datenschutzgrundverordnung (DSGVO) – publik gemacht, dass man am Vortag von Hackern angegriffen worden sei. Schon damals war bekannt, dass hinter dem Angriff die internationale Hackergruppe Black Cat steckt. Diese forderte ein Lösegeld in Höhe von fünf Millionen Euro in Bitcoin für eine Software, mit der man die verschlüsselten Daten wieder hätte entschlüsseln können. Mehr wurde nicht öffentlich gemacht.

Anfang Juni wurde der Hackerangriff auf Kärnten durch einen auf Twitter veröffentlichten Screenshot konkreter. Der IT-Sicherheitsexperte Sebastian Bicchì behauptete, im Netz aufgetauchte Ordner gefunden zu haben, die Namen wie "Reisepläne", "Impfungen" oder "Cards" trugen. Diese würden von einem Hack gegen das Land Kärnten stammen, schrieb Bicchì, und seien jetzt im Darknet teilweise verfügbar.



Gar nicht so niedlich, sondern immer auf der Sache hoch reiten Ransomware-Opfern: die Hackergruppe Black Cat.  
Foto: Der Standard/Stephan Meyer

### Cyberangriff auf Therme Waltersdorf: Chip-Uhren funktionierten nicht

14.09.2022

Barbara Wimmer

Der Ausfall der IT-Systeme hatten auch Auswirkungen auf die Gäste. Sie brauchten wieder herkömmliche Zimmerschlüssel.



CHRONIK

### Hackerangriff auf Stephansdom

Die Glocken des Wiener Stephansdoms haben in der Nacht auf Mittwoch zahlreiche Bewohner und Bewohnerinnen der Innenstadt aus dem Schlaf gerissen. Ursache war offenbar ein Hackerangriff.

16. März 2022, 9:48 Uhr (Update: 16. März 2022, 15:41 Uhr)



WIRTSCHAFT

### Cyberangriff auf 34 Firmen in Oberösterreich

Insgesamt 34 Klein- und Mittelbetriebe können nach der Attacke nicht mehr auf ihre Computer-Systeme zugreifen.

02.09.2021, 06:24

#### Quellen:

<https://kurier.at/wirtschaft/cyberangriff-auf-34-firmen-in-oberoesterreich/401722080>

<https://futurezone.at/digital-life/cyberangriff-therme-waltersdorf-steiermark-erpresser-ransomware/402146586>

<https://www.derstandard.at/story/2000136355061/cyberangriff-auf-kaernten-die-wichtigsten-fakten-zum-aktuellen-fall>

<https://wien.orf.at/stories/3147683/>

# Die 3 Säulen Ihrer Cyber-Sicherheit



Wir bieten professionelle Cyber-Lösungen für alle Kunden



**RISIKOPRÄVENTION**



**VERSICHERUNG**



**SCHADENMANAGEMENT**

# Kostenrisiko eines Cyber-Angriffs

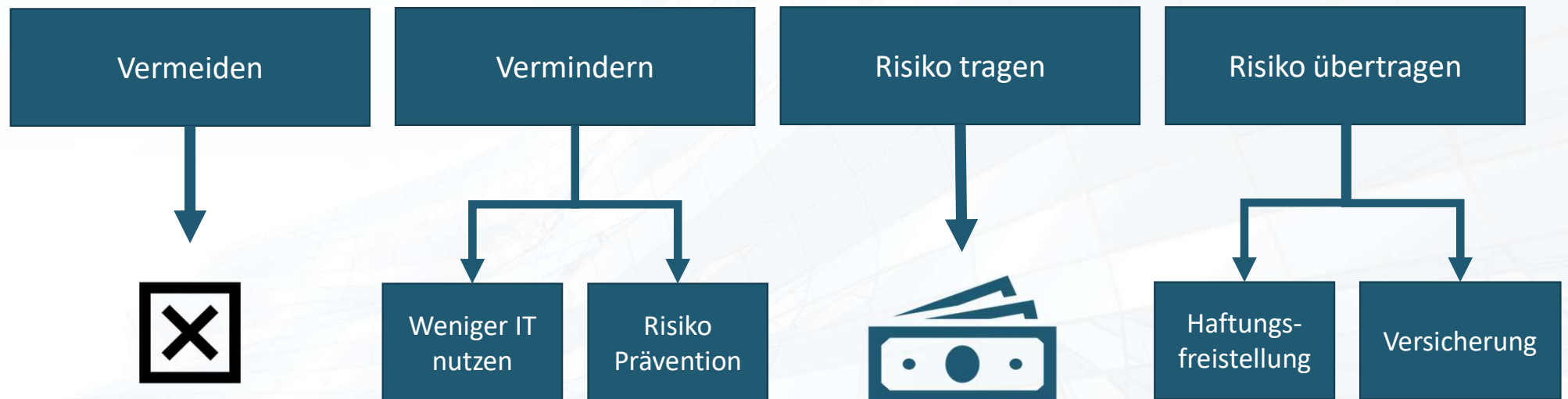
## Das eigene Risiko bewerten



- 🪙 Wer bezahlt die erforderlichen Cyber-Spezialisten?
- 🪙 Wer ersetzt den entgangenen Deckungsbeitrag?
- 🪙 Wer übernimmt die Kosten für die Wiederinstandsetzung der IT?
- 🪙 Wenn beispielsweise Daten gestohlen werden, wie sichern wir uns gegen Haftungsansprüche Dritter ab?

# Kostenrisiken steuern

## Möglichkeiten der Risikobewältigung



# Cyber-Prävention

## Gefahren erkennen



Wir bieten professionelle Cyber Security Services für alle Kunden



COGITANDA®  
CYBER SIND WIR.



### RISIKOPRÄVENTION

- Mitarbeiter-Schulungen
- Phishing-Simulationen
- Schwachstellen-Scans
- Audits



### VERSICHERUNG



### SCHADENMANAGEMENT

# Kostenschutz durch Ihre Cyber-Versicherung



## Die 3 Säulen des Versicherungsschutzes

### Krisenmanagement

- 24/7 Hotline
- Internationales Experten-Netzwerk
- Übernahme der Leistungskoordination

### Eigenschaden

- Betriebsunterbrechung
- Mehrkosten
- Daten-Wiederherstellungskosten
- Geldeswerte auf Konten

### Unternehmerhaftung

- Haftpflichtansprüche
- DSGVO Ansprüche
- Rechtsschutz

# Status-Quo der Cyber-Versicherung

## Zunehmende Spezialisierung des Marktes

- Generalisten -> Spezialisten
- Präventionsdienstleistungen
- Gezielte Risikofragen und Antragsprozesse
- Qualitätslevel Schaden- & Krisenmanagement / Incident Response Management



Wir bieten professionelles Cyber Security Management für alle Kunden



COGITANDA®  
CYBER SIND WIR.



### RISIKOPRÄVENTION

- Mitarbeiter-Schulungen
- Phishing-Simulationen
- Schwachstellen-Scans
- Audits



### VERSICHERUNG

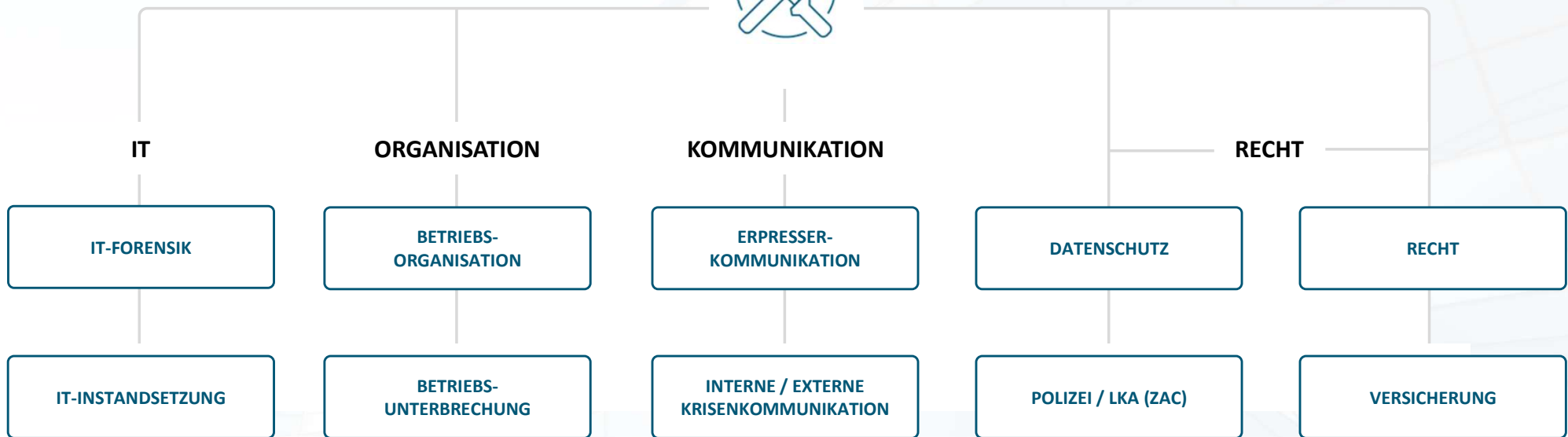
- Maßgeschneiderter Versicherungsschutz
- Optionale Deckungen
- Professionelles Krisenmanagement



### SCHADENMANAGEMENT

# COGITANDA Cyber-Krisen-Management im Einsatz

Cyber-Angriffe erfordern den gezielten Einsatz von Spezialisten



# COGITANDA Cyber Sofort Hilfe



Als vorübergehende Lösung bis zum Abschluss einer Versicherung

## 365/24/7 Notfallhotline

Unsere Hotline steht rund um die Uhr mit unseren Cyber-Experten und IT-Forensikern für Sie bereit.

## Analyse und Sofortmaßnahmen

Spätestens 2 Stunden nach der Meldung des Notfalls beginnen wir mit der konkreten Analyse sowie der Einleitung von Sofortmaßnahmen – GARANTIERTE!

## Einsatz von Netzwerk-Spezialisten

Der Einsatz von Cyber-Spezialisten aus unserem Netzwerk ist in den ersten 48 Std. bis 7.500 € bei der COGITANDA® Cyber Sofort Hilfe inklusive.



Auch ohne Versicherungsschutz buchbar

## Leitung des Krisenstabs

Wir übernehmen die 360°-Steuerung aller Krisenreaktionsmaßnahmen – von der Analyse über das Schadenmanagement bis zur Wiederherstellung Ihres Geschäftsbetriebs.

## Individuelles IT-Spezialisten-Team

Für eine professionelle Reaktion auf den Cyber-Vorfall in Ihrem Unternehmen stellen wir für Sie ein individuelles Team von IT-Spezialisten aus unserem Experten-Netzwerk zusammen.

## Datenschutz und Strafverfolgung

Beratung zu Datenschutzthemen, Kommunikation mit der Datenschutzbehörde, LKA/BKA, Polizei und die Bereitstellung von Fachanwälten werden ebenfalls durch unser Experten-Netzwerk abgedeckt.



Wir bieten professionelles Cyber Security Management für alle Kunden



COGITANDA®  
CYBER SIND WIR.



### RISIKOPRÄVENTION

- Mitarbeiter-Schulungen
- Phishing-Simulationen
- Schwachstellen-Scans
- Audits



### VERSICHERUNG

- Maßgeschneiderter Versicherungsschutz
- Optionale Deckungen
- Professionelles Krisenmanagement



### SCHADENMANAGEMENT

- 24/7 Hotline
- Internationales Experten-Netzwerk
- Übernahme Krisenmanagement

---

---

FRAGEN? GERNE JETZT!



## IT-Sicherheit



© BS Information & Consulting

Gefahren erkennen, Sicherheitsstrategien entwickeln, Maßnahmen umsetzen

Lesedauer: 2 Minuten

05.06.2024



DANKE FÜR IHRE AUFMERKSAMKEIT

CYBER IS US®