KRISENKOMMUNIKATION BEI EINEM CYBERANGRIFF

COMMERZBANK

© REVOLVERMÄNNER GmbH

15+ JAHRE
ERFAHRUNG.

MARKTFÜHRER UND BRANCHENPIONIER FÜR REPUTATIONSMANAGEMENT UND KRISENKOMMUNIKATION 2.0.

© REVOLVERMÄNNER GmbH

Krisenkommunikation 2.0

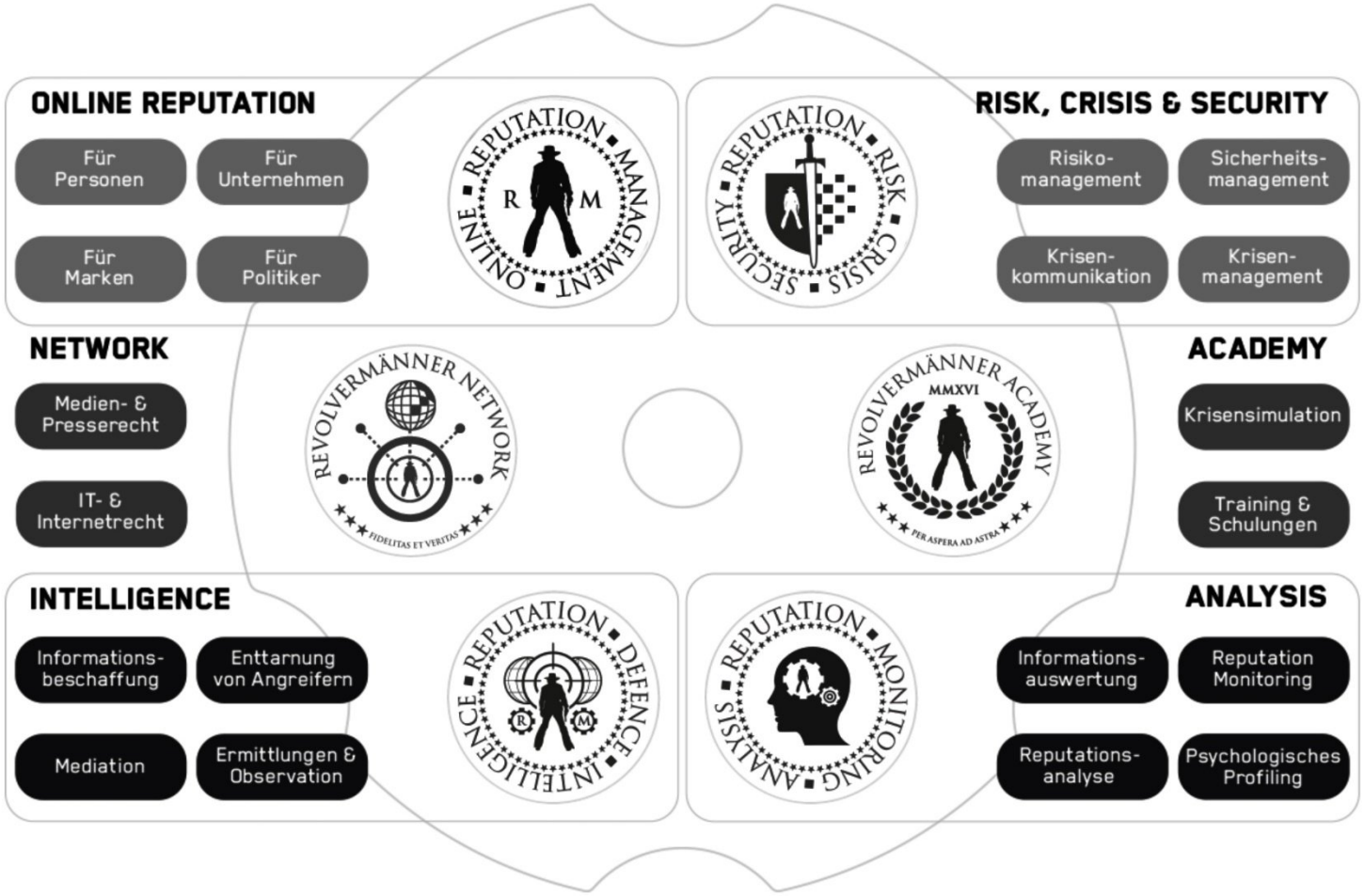
Reputation Management

Monitoring & Analysis

OSINT Analysen

© REVOLVERMÄNNER GmbH

DAS IST UNSER REVOLVER.



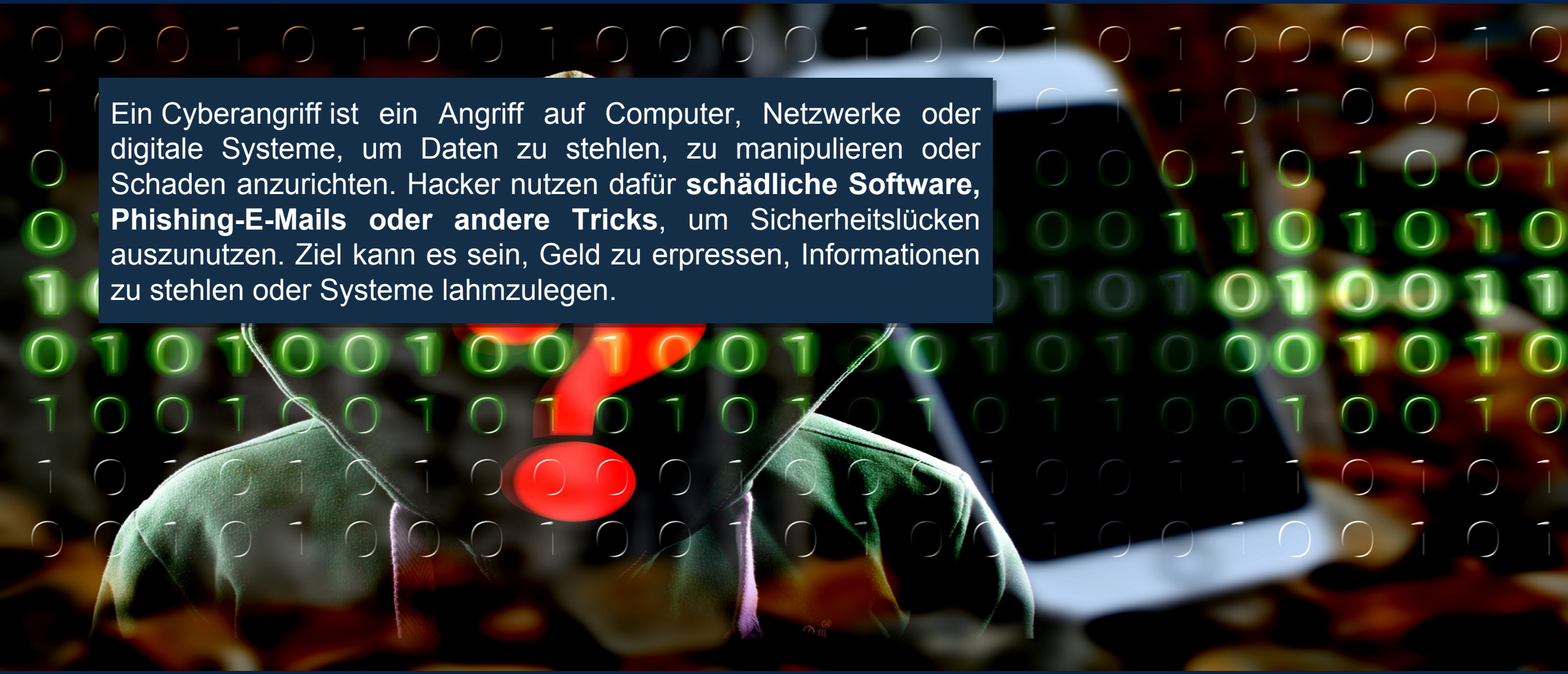
© REVOLVERMÄNNER GmbH

BERND FUHLERT.

Geschäftsführer der REVOLVERMÄNNER GmbH & TRIARI.US GmbH • Freier Dozent Praxis Campus, IHK Köln sowie weiterer renommierter Institute • Aktives Mitglied und Dozent bundesweit an Schulen für die Sekundarstufe I und II für den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. • Autor zahlreicher Veröffentlichungen, zuletzt des Buches: Datenverarbeitungen in Drittstaaten • externer DSB bei diversen namhaften Unternehmen

© REVOLVERMÄNNER GmbH

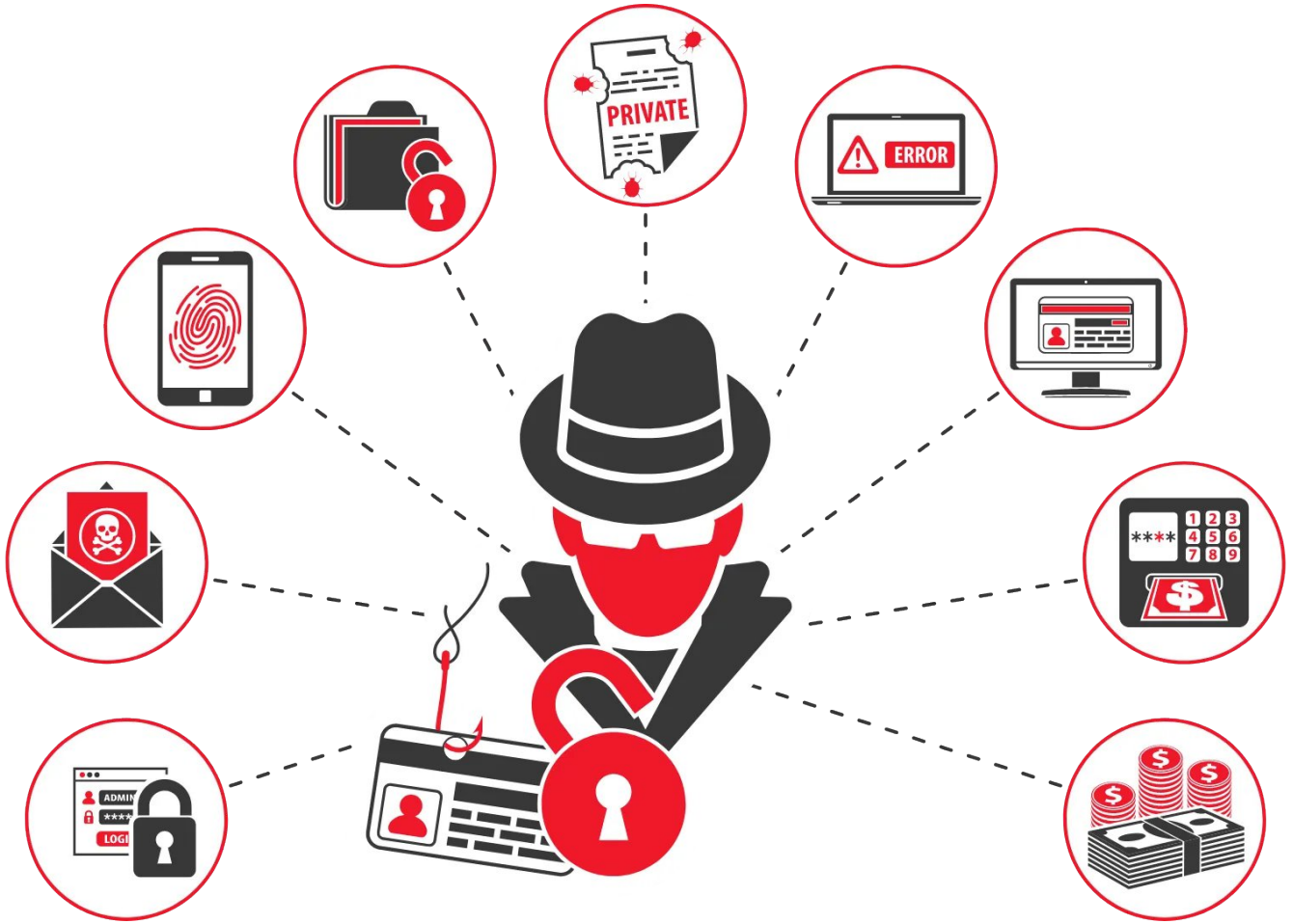
WAS IST EIN CYBERANGRIFF?



Ein Cyberangriff ist ein Angriff auf Computer, Netzwerke oder digitale Systeme, um Daten zu stehlen, zu manipulieren oder Schaden anzurichten. Hacker nutzen dafür **schädliche Software, Phishing-E-Mails oder andere Tricks**, um Sicherheitslücken auszunutzen. Ziel kann es sein, Geld zu erpressen, Informationen zu stehlen oder Systeme lahmzulegen.

© REVOLVERMÄNNER GmbH

ARTEN VON CYBERANGRIFFEN.



© REVOLVERMÄNNER GmbH

BEGRIFFSERLÄUTERUNGEN.

Phishing-Mails
→ Betrügerische E-Mails, die aussehen, als kämen sie von vertrauenswürdigen Absendern. Sie enthalten oft Links oder Anhänge, die dazu dienen, Passwörter, Bankdaten oder andere persönliche Informationen zu stehlen.

Malware
→ Schädliche Software (z. B. Viren, Trojaner, Spyware), die Computer infiziert, Daten stiehlt oder Systeme beschädigt. Malware kann sich über E-Mails, infizierte Webseiten oder unsichere Downloads verbreiten.

Ransomware
→ Eine spezielle Art von Malware, die Daten oder ganze Systeme verschlüsselt und erst nach Zahlung eines Lösegelds (Ransom) wieder freigibt. Häufig wird Bitcoin als Zahlungsmittel gefordert.

© REVOLVERMÄNNER GmbH

BEGRIFFSERLÄUTERUNGEN.

Ein **Advanced Persistent Threat (APT)** ist ein gezielter, langanhaltender Cyberangriff, bei dem Hacker heimlich in ein Netzwerk eindringen, um Daten zu stehlen oder die Kontrolle zu übernehmen. Dieser Angriff kann über Monate oder Jahre laufen und ist oft gut organisiert und schwer zu entdecken.

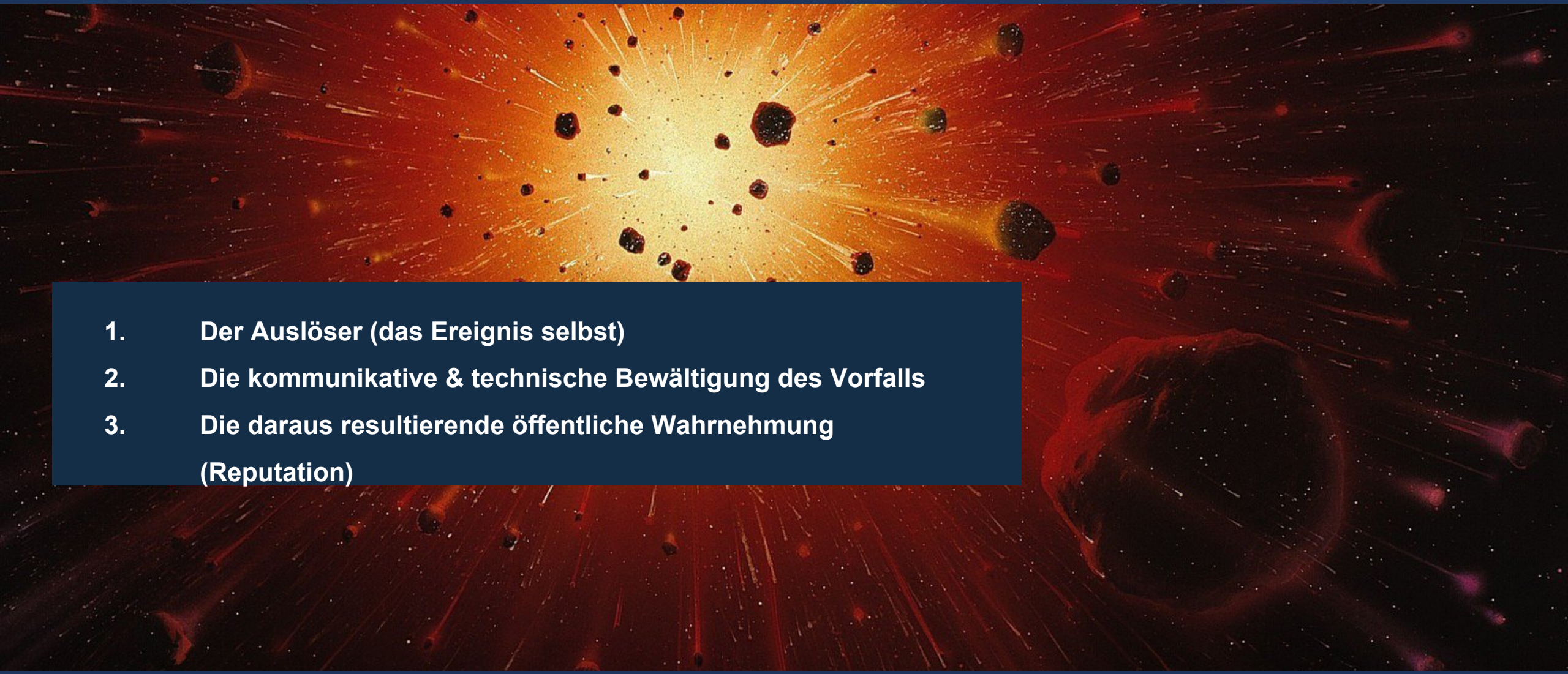
Social Engineering ist eine Methode, bei der Hacker Menschen manipulieren, um an vertrauliche Informationen zu gelangen. Statt technische Schwachstellen auszunutzen, täuschen sie Opfer durch Tricks oder falsche Identitäten, damit diese z. B. Passwörter preisgeben oder schädliche Links anklicken. Ein Beispiel ist eine gefälschte E-Mail, die vorgibt, von der eigenen Bank zu sein.

© REVOLVERMÄNNER GmbH

„DIE FRAGE IST SCHON LANGE NICHT MEHR OB, SONDERN WANN SIE OPFER EINES CYBERANGRIFFES WERDEN.“

© REVOLVERMÄNNER GmbH

DIE DIMENSIONEN EINES CYBERANGRIFFES.



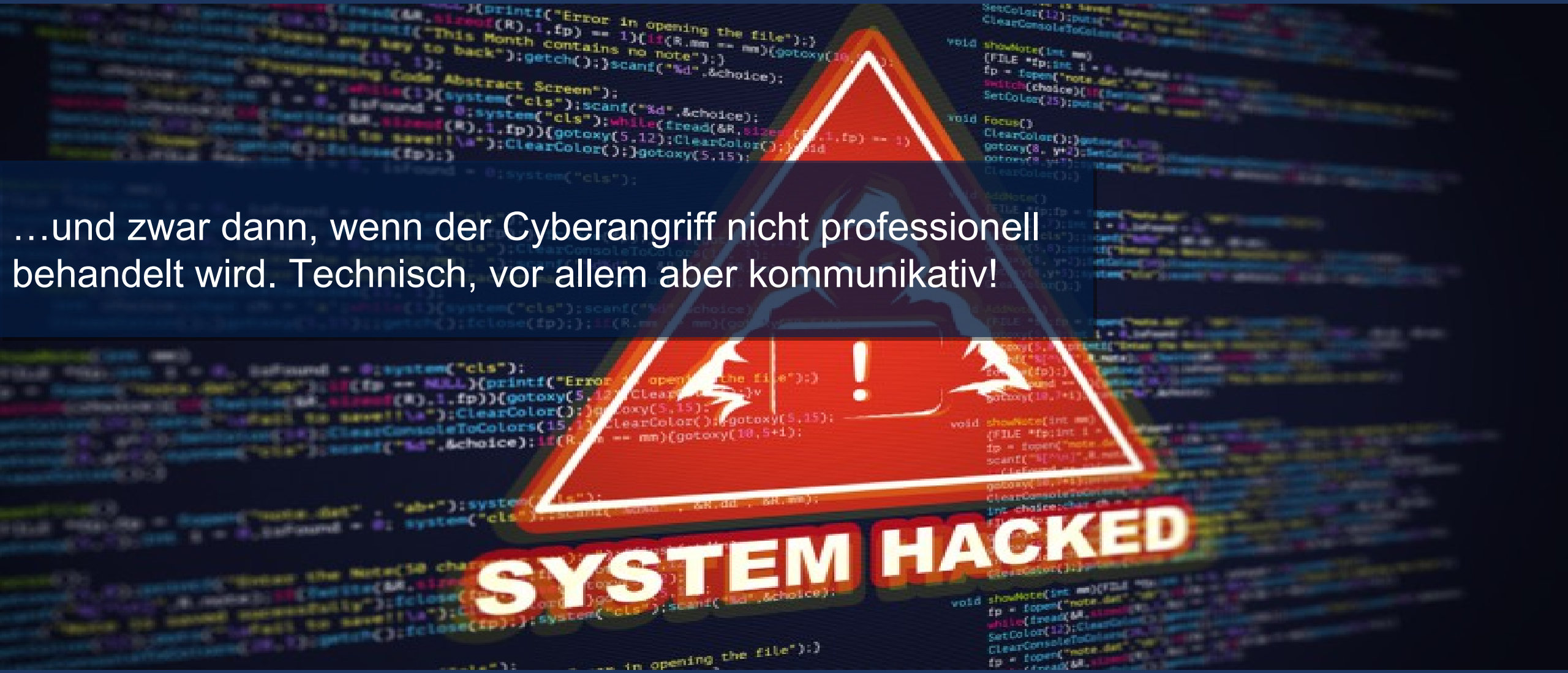
1. **Der Auslöser (das Ereignis selbst)**
2. **Die kommunikative & technische Bewältigung des Vorfalls**
3. **Die daraus resultierende öffentliche Wahrnehmung (Reputation)**

© REVOLVERMÄNNER GmbH

FALSCHE BEWÄLTIGUNG DES CYBERANGRIFFES MÜNDET UNWEIGERLICH IN EINER KRISE!

© REVOLVERMÄNNER GmbH

JEDES UNTERNEHMEN STEHT DAMIT POTENZIELL KURZ VOR EINER KRISE!



…und zwar dann, wenn der Cyberangriff nicht professionell behandelt wird. Technisch, vor allem aber kommunikativ!

© REVOLVERMÄNNER GmbH

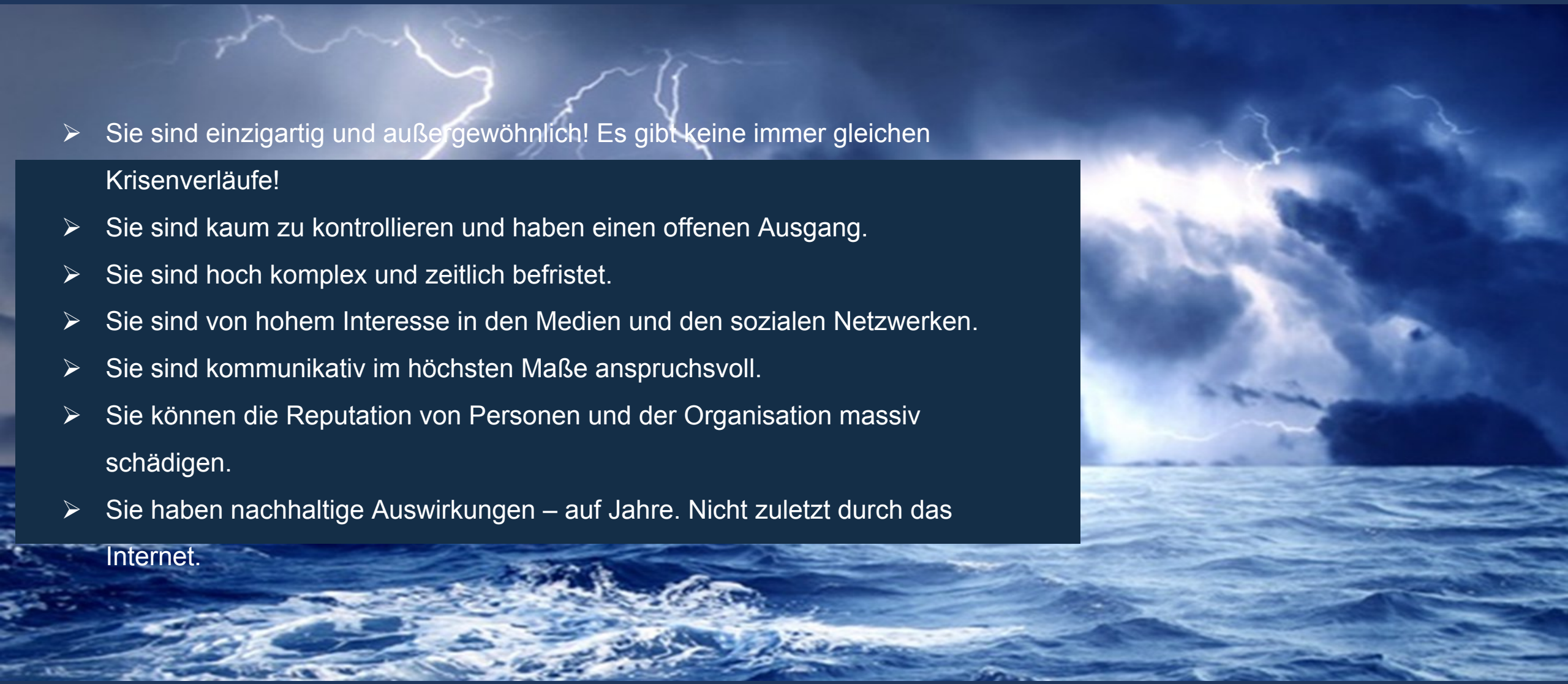
EXKURS: WAS IST EINE KRISE?

Krisen-Definition

„Eine Krise ist ein Bruch in einer kontinuierlichen Entwicklung und bezeichnet eine gefährliche, außergewöhnliche und existenzbedrohende Lage, in der das Management extrem gefordert ist, Schäden für das Leib und Leben von Menschen und/oder für bedeutende Sachwerte zu verhindern."

© REVOLVERMÄNNER GmbH

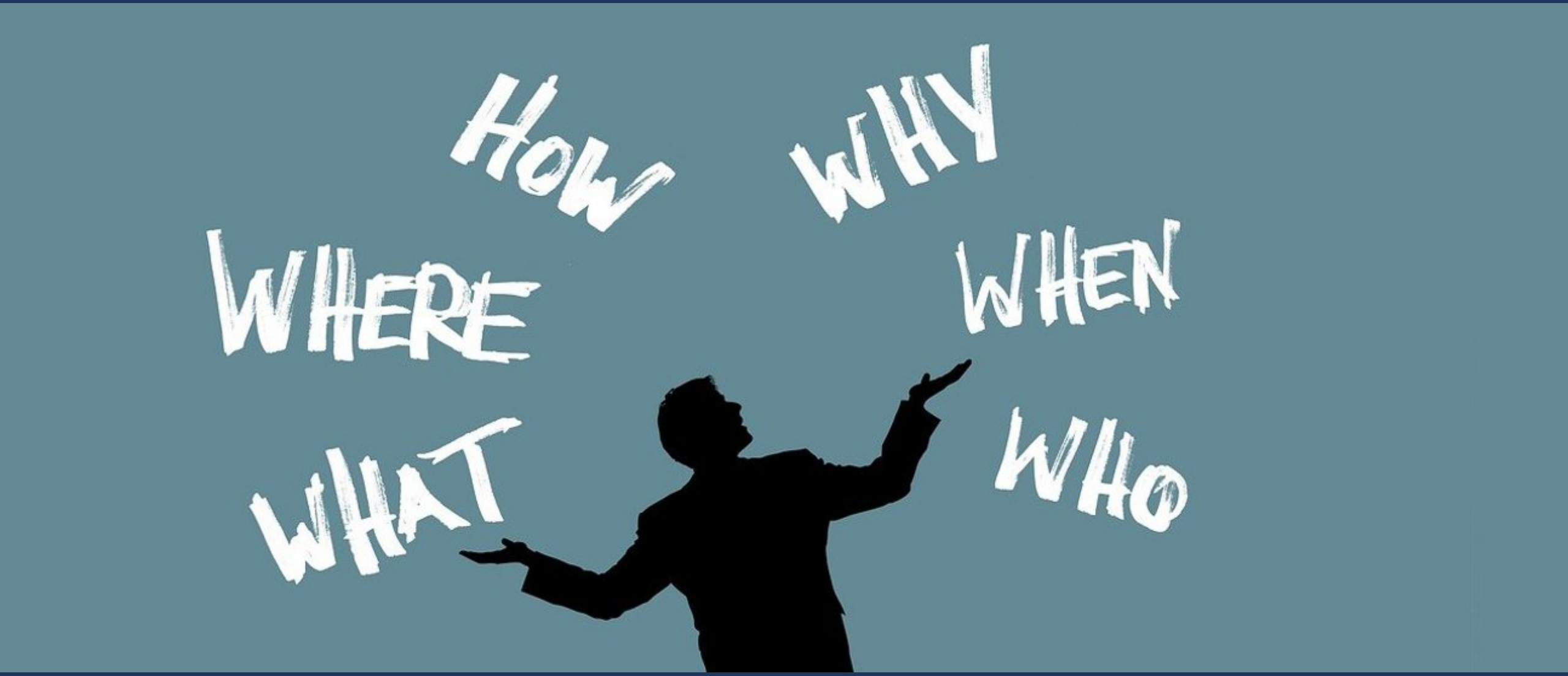
ALLE KRISEN HABEN GEMEINSAM:



- Sie sind einzigartig und außergewöhnlich! Es gibt keine immer gleichen Krisenverläufe!
- Sie sind kaum zu kontrollieren und haben einen offenen Ausgang.
- Sie sind hoch komplex und zeitlich befristet.
- Sie sind von hohem Interesse in den Medien und den sozialen Netzwerken.
- Sie sind kommunikativ im höchsten Maße anspruchsvoll.
- Sie können die Reputation von Personen und der Organisation massiv schädigen.
- Sie haben nachhaltige Auswirkungen – auf Jahre. Nicht zuletzt durch das Internet.

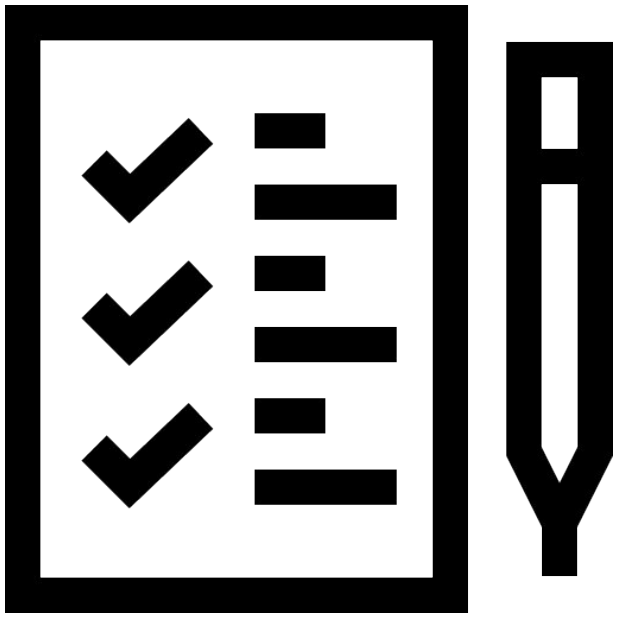
© REVOLVERMÄNNER GmbH

BEREITEN SIE SICH ALSO GRÜNDLICH VOR.



© REVOLVERMÄNNER GmbH

VORBEREITUNG.



- Entwicklung eines Krisenkommunikationsplans & -handbuchs
- Definition von Rollen und Verantwortlichkeiten
- Schulung und Sensibilisierung von Mitarbeitenden
- Testen von Reaktionsstrategien (Simulationen)

© REVOLVERMÄNNER GmbH

DAS KRISENHANDBUCH. IHR HANDLUNGSLEITFADEN.

Krisenkommunikationshandbuch

Workflow
(Organisation)

- Ressortspezifische Abläufe
- Ansprechpartner
- Aufgabenzuweisung
- Verantwortlichkeiten
- Informationsgeber
- Meldeformulare
- Meldeprozesse
- Erreichbarkeiten

Basisinformationen
(nach Szenarien)

- Q&A
- Botschaften für alle Szenarien
- Argumentarium
- Hintergrundinfos
- Szenariengebundene und szenarienunabhängige Textbausteine

Aktionsplan
(nach Zielgruppen/ Szenarien)

- Medien
- Informationszeiten
- Meldeverpflichtungen
- Kanäle
- Multiplikatoren

© REVOLVERMÄNNER GmbH

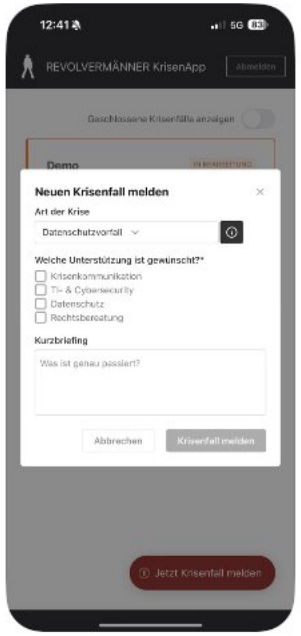
SCHNELLE REAKTION SICHERSTELLEN!

CrisisApp

Revolvermänner KrisenApp

Laden

Entwickelt für iPhone. Nicht für macOS überprüft.



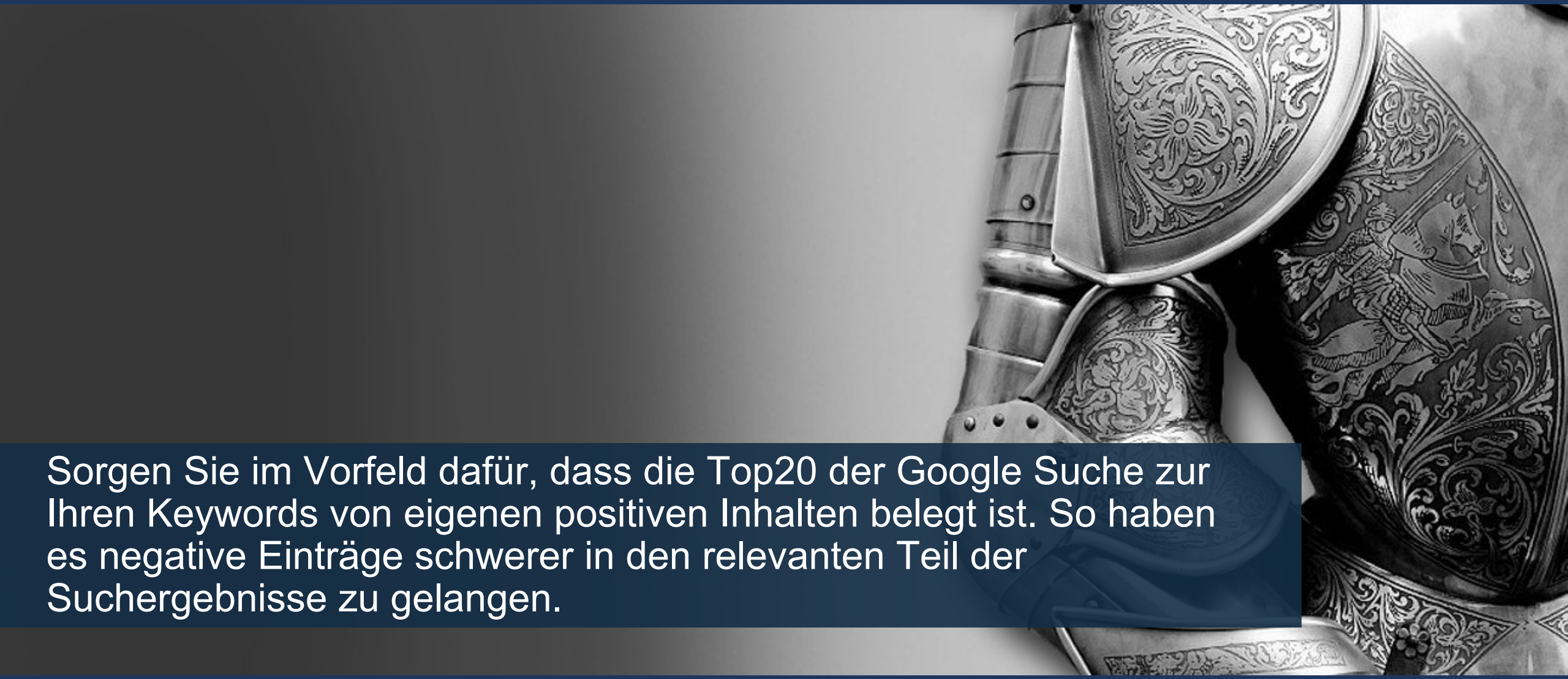
© REVOLVERMÄNNER GmbH

SCHNELLE REAKTION SICHERSTELLEN!

Scannen Sie den QR-Code oder öffnen Sie krisenapp.com. Erstellen Sie Ihren persönlichen Account.
Im Google Play Store auch kurzfristig verfügbar.

© REVOLVERMÄNNER GmbH

DER SCHUTZPANZER.



Sorgen Sie im Vorfeld dafür, dass die Top20 der Google Suche zur Ihren Keywords von eigenen positiven Inhalten belegt ist. So haben es negative Einträge schwerer in den relevanten Teil der Suchergebnisse zu gelangen.

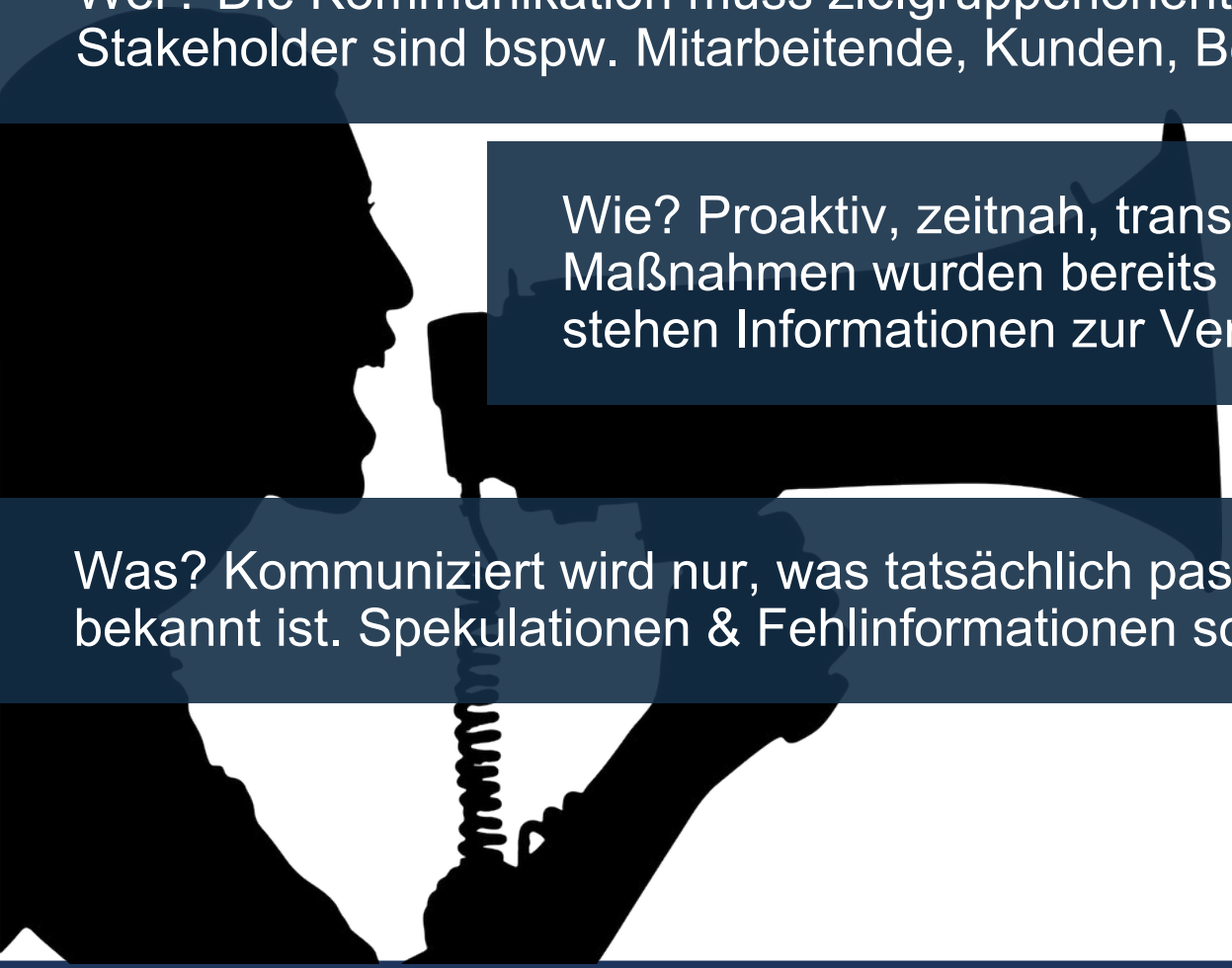
© REVOLVERMÄNNER GmbH

SOFORTMASSNAHMEN IM AKUTEN FALL.

- 1. Bestätigung des Angriffs an Behörden (Meldefristen) und Kunden
- 2. Aktivierung des Krisenreaktionsteams
- 3. Information der relevanten Stakeholder
- 4. Sicherung und Untersuchung der betroffenen Systeme

© REVOLVERMÄNNER GmbH

WER, WIE, WAS …
KOMMUNIKATION IM AKUTEN FALL.



Wer? Die Kommunikation muss zielgruppenorientiert stattfinden. Relevante Stakeholder sind bspw. Mitarbeitende, Kunden, Behörden, Medien, etc.

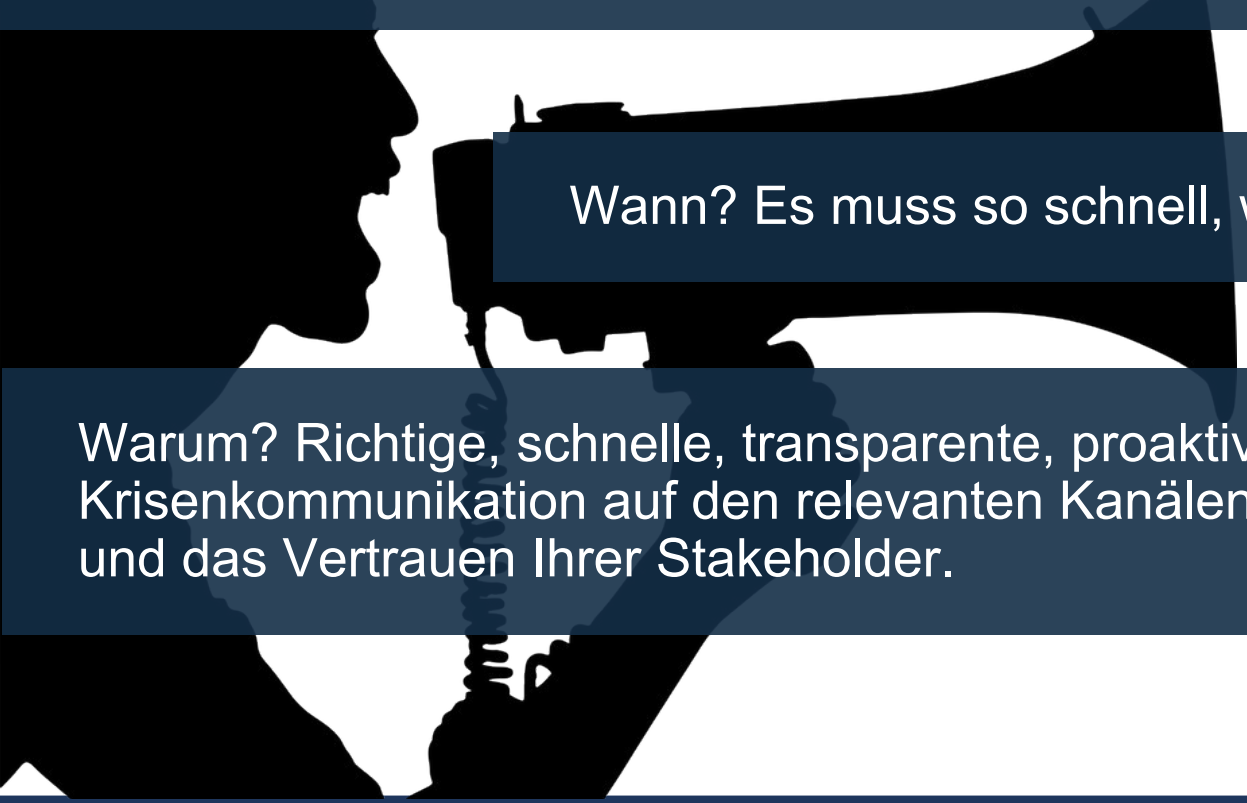
Wie? Proaktiv, zeitnah, transparent. Welche Daten sind betroffen, welche Maßnahmen wurden bereits ergriffen, welche Auswirkungen hat die Attacke, wo stehen Informationen zur Verfügung.

Was? Kommuniziert wird nur, was tatsächlich passiert ist und was wirklich bekannt ist. Spekulationen & Fehlinformationen sollten vermieden werden.

© REVOLVERMÄNNER GmbH

…WO, WANN, WARUM?
KOMMUNIKATION IM AKUTEN FALL.

Wo? Jeder Stakeholder sollte auf dem jeweiligen, relevanten Kanal informiert werden, wie bspw. Pressemitteilung, eigene Webseite, Social Media, direkte E-Mail. Achtung: behördliche Meldewege sind unbedingt einzuhalten!



Wann? Es muss so schnell, wie nur möglich kommuniziert werden.

Warum? Richtige, schnelle, transparente, proaktive und zielgruppenorientierte Krisenkommunikation auf den relevanten Kanälen sichert die Deutungshoheit und das Vertrauen Ihrer Stakeholder.

© REVOLVERMÄNNER GmbH

WENN SIE ALLES RICHTIG MACHEN.

Published **29. März 2019**

Großflächige und massive Cyber-Attacke auf Aluminiumkonzern Norsk Hydro

Der norwegische Konzern Norsk, einer der größten Aluminium-Hersteller weltweit, ist am 19. März zum Ziel einer großflächigen Cyberattacke geworden. Am vergangenen Dienstag meldet sich der Konzern zuerst über Facebook und andere Nachrichtenkanälen, da die eigenen Webserver auch betroffen waren:

> *IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation. (Q: hydro.com / Kopie)*

Einen Tag später wurde darüber informiert, dass die Ursache des Problems identifiziert worden sei und man dabei sei die betroffenen und ursächlichen Systeme zu isolieren, während die Produktionssysteme weiterhin manuell betrieben werden. Eine knappe Woche später, am 26.3. waren laut Pressemitteilung nahezu alle Systeme wieder hergestellt, obgleich es mit einigen wenigen Produktionszweigen noch Schwierigkeiten geben soll. Zu den Ursachen der Attacke gibt es bislang wenige öffentliche Informationen:

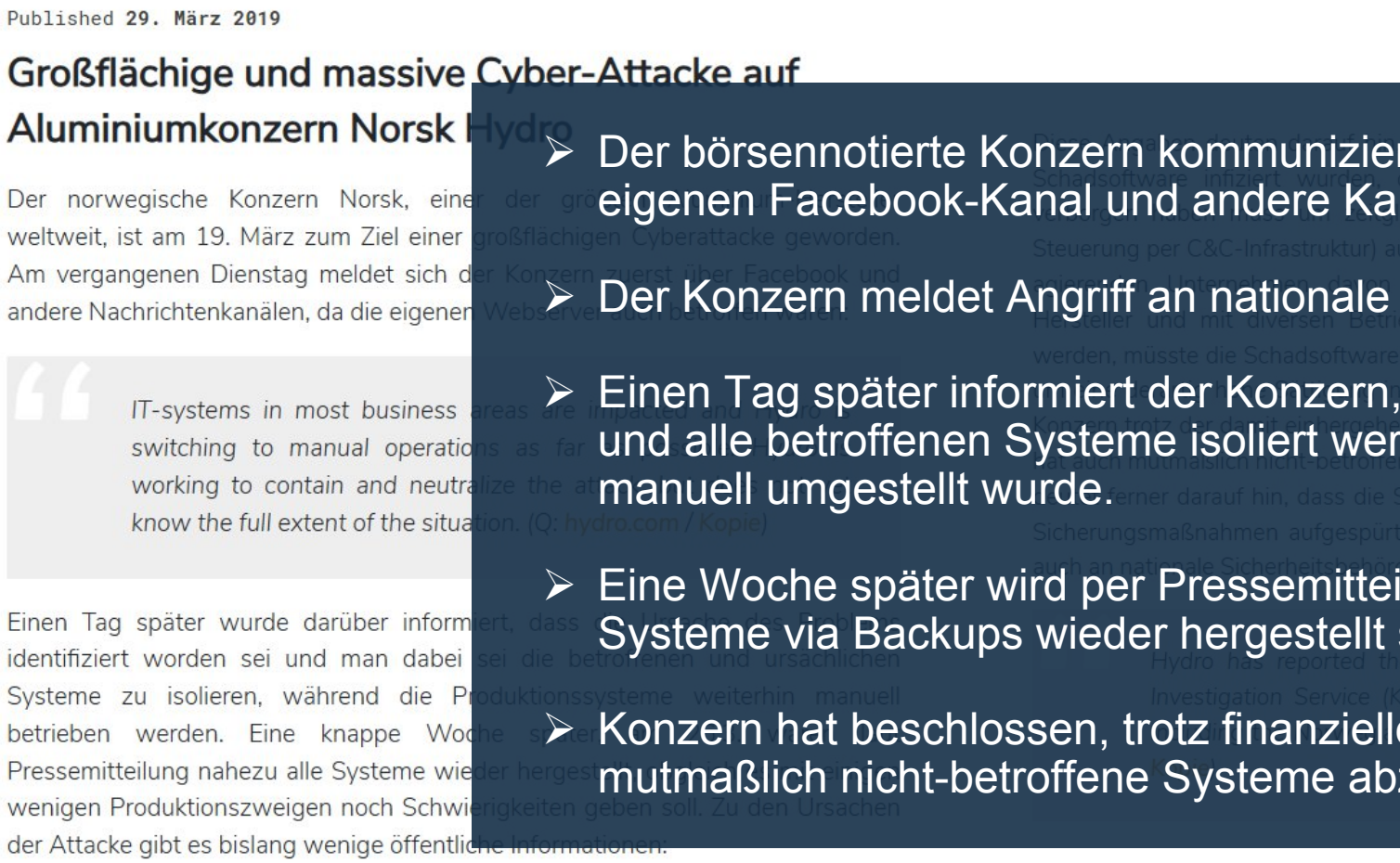
Diese Angaben deuten darauf hin, dass die IT-Systeme des Konzern großflächig mit einer Schadsoftware infiziert wurden, die sich bis zum 19.3. verdeckt in den IT-Systemen verborgen haben muss um zeitgleich (entweder per „eingebautem Timer“ oder externe Steuerung per C&C-Infrastruktur) ausgelöst zu werden. Da bei einem derart großen, weltweit agierenden Unternehmen davon auszugehen ist, dass IT-Systeme unterschiedlichster Hersteller und mit diversen Betriebssystemen und Software-Versionsständen eingesetzt werden, müsste die Schadsoftware sehr breitflächig und universell in der Lage gewesen sein um eine derartig hohe Sättigung innerhalb der Konzern-IT-Systeme zu erzielen. Da sich der Konzern trotz der damit einhergehenden finanziellen und produktiven Einbußen entschlossen hat auch mutmaßlich nicht-betroffene Systeme als Vorsichtsmaßnahme vom Netz zu nehmen deutet ferner darauf hin, dass die Schadsoftware maßgeschneidert und nicht mit Standard-Sicherungsmaßnahmen aufgespürt werden kann. Der Konzern hat den Vorfall demzufolge auch an nationale Sicherheitsbehörden gemeldet:

> *Hydro has reported the sophisticated cyber attack to Norway's National Investigation Service (Kripos) and is cooperating with relevant authorities, including the Norwegian National Security Authority (NSM). (Q: Hydro.com / Kopie)*

Text-Auszug aus dem Artikel

© REVOLVERMÄNNER GmbH

WENN SIE ALLES RICHTIG MACHEN.



Published **29. März 2019**

Großflächige und massive Cyber-Attacke auf Aluminiumkonzern Norsk Hydro

Der norwegische Konzern Norsk, einer der größ… weltweit, ist am 19. März zum Ziel einer großflächigen Cyberattacke geworden. Am vergangenen Dienstag meldet sich der Konzern zuerst über Facebook und andere Nachrichtenkanälen, da die eigenen Webserver […]

> *IT-systems in most business areas are impacted and […] switching to manual operations as far […] working to contain and neutralize the at… know the full extent of the situation. (Q: hydro.com / Kopie)*

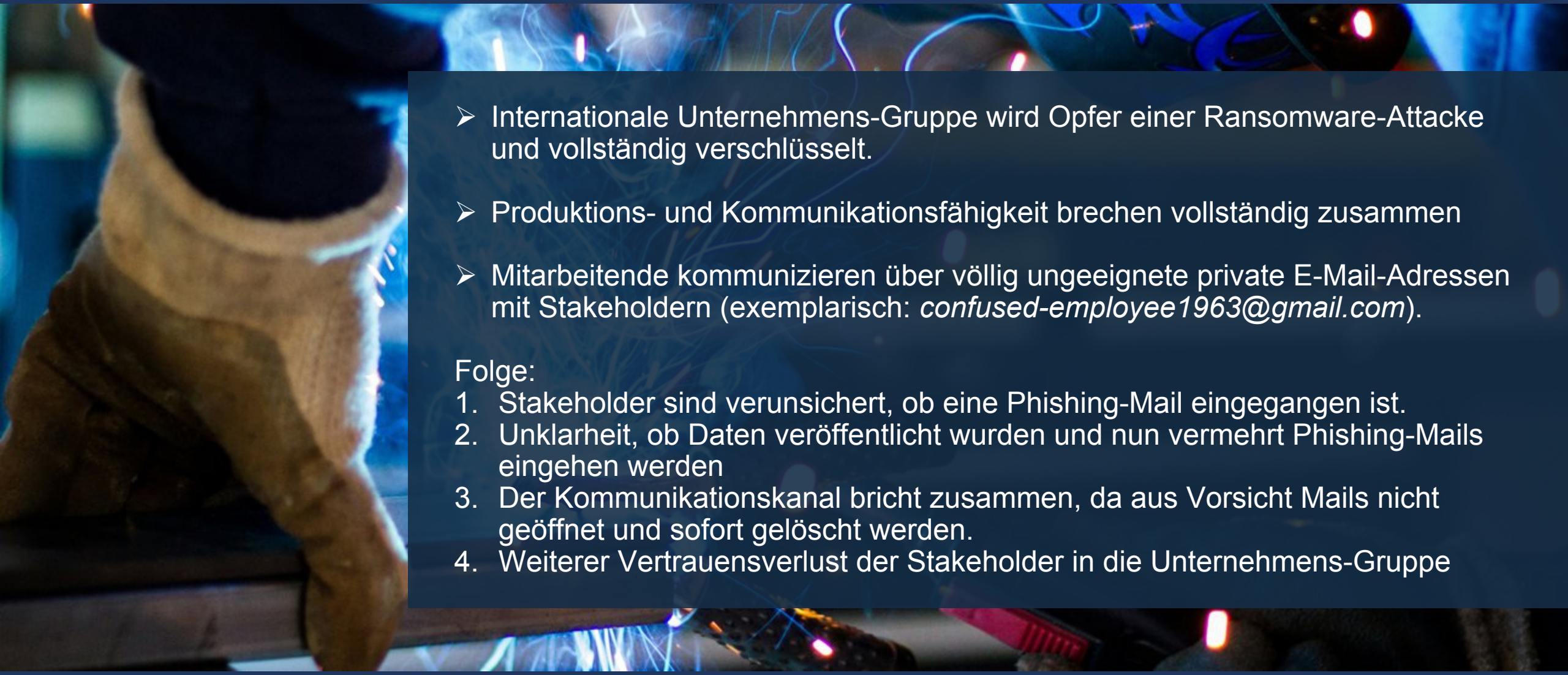
Einen Tag später wurde darüber informiert, dass … identifiziert worden sei und man dabei sei die betroffenen und ursächlichen Systeme zu isolieren, während die Produktionssysteme weiterhin manuell betrieben werden. Eine knappe Woche … Pressemitteilung nahezu alle Systeme wieder herges… wenigen Produktionszweigen noch Schwierigkeiten geben soll. Zu den Ursachen der Attacke gibt es bislang wenige öffentliche Informationen.

- Der börsennotierte Konzern kommuniziert transparent die Cyberattacke über eigenen Facebook-Kanal und andere Kanäle.
- Der Konzern meldet Angriff an nationale Sicherheitsbehörden.
- Einen Tag später informiert der Konzern, dass die Ursache identifiziert wurde und alle betroffenen Systeme isoliert werden, während die Produktion auf manuell umgestellt wurde.
- Eine Woche später wird per Pressemitteilung kommuniziert, dass nahezu alle Systeme via Backups wieder hergestellt sind.
- Konzern hat beschlossen, trotz finanzieller und produktiver Einbußen, auch mutmaßlich nicht-betroffene Systeme abzuschalten.

Text-Auszug aus dem Artikel

© REVOLVERMÄNNER GmbH

WAS HINGEGEN PASSIERT, WENN SIE NICHT RICHTIG HANDELN.



- Internationale Unternehmens-Gruppe wird Opfer einer Ransomware-Attacke und vollständig verschlüsselt.
- Produktions- und Kommunikationsfähigkeit brechen vollständig zusammen
- Mitarbeitende kommunizieren über völlig ungeeignete private E-Mail-Adressen mit Stakeholdern (exemplarisch: *confused-employee1963@gmail.com*).

Folge:

1. Stakeholder sind verunsichert, ob eine Phishing-Mail eingegangen ist.
2. Unklarheit, ob Daten veröffentlicht wurden und nun vermehrt Phishing-Mails eingehen werden
3. Der Kommunikationskanal bricht zusammen, da aus Vorsicht Mails nicht geöffnet und sofort gelöscht werden.
4. Weiterer Vertrauensverlust der Stakeholder in die Unternehmens-Gruppe

© REVOLVERMÄNNER GmbH

WAS HINGEGEN PASSIERT, WENN SIE NICHT RICHTIG HANDELN.

Start › Alles& › Massive IT-Datenpanne bei der Unimedizin Main

Alles& | Rathaus & andere Skandale

Massive IT-Datenpanne bei der Unimedizin Mainz: Emails im Darknet gelandet, 280.000 Adressaten betroffen

Von **Gisela Kirschstein** - 3. Mai 2024 846 0

Der Haupteingang der Universitätsmedizin Mainz: Die Uniklinik ist von einem massiven Datenklau betroffen. – Foto: Universitätsmedizin Mainz/ Peter Pulkowski

„Informationen zu einem Datenschutzvorfall" – Überschrift zu einer E-Mail, die derzeit zahlreichen Patienten und anderen Kontaktleuten der Mainzer Universitätsmedizin ins Email-Postfach flattert. Hinter der harmlosen Überschrift verbirgt sich ein handfester Datenskandal: Bei einem Hackerangriff wurden ausgelagerte Protokollierungsdaten des E-Mail-Servers der Universitätsmedizin Mainz entwendet – und die Daten anschließend im Darknet veröffentlicht.

Wann genau der Datenklau geschah, teilte die Mainzer Nachfrage nicht mit – dabei wäre dies natürlich eine wichtige ebenfalls nicht gesagt. „Der IT-Dienstleister hat den Vorfall mit Strafverfolgungsbehörden aufgearbeitet und die Universitätsmedizin Mail an Betroffene lediglich. Die Email liegt Mainz& vor, die betroffene

Erpresser-Virus auf einem Computer: Durch geklaute Daten kann es nun zu vermehrten

Text-Auszug aus dem Artikel

- Stakeholder der Unimedizin Mainz erhalten eine Informations-Mail, dass ein IT-Dienstleister Opfer einer Cyberattacke wurde und Daten geklaut sowie veröffentlicht wurden.
- Keine Information, wann der Datenklau geschah und wann Daten im Darknet veröffentlicht wurden.
- Informationen legen nahe, dass der Datenklau bereits einige Tage vor der Information der Stakeholder geschah.
- Es wurde lediglich mitgeteilt, dass „ein potentielles Risiko vorliege". Was das für die Stakeholder konkret bedeutet, wurde nicht mitgeteilt.
- Informationsmails an Betroffene kommen teilweise mit Tagen Verzögerung.
- Keine Information, welcher IT-Dienstleister betroffen war, wie es zu dem Vorfall kam und welche künftigen Sicherheitsmaßnahmen die Unimedizin Mainz künftig ergreift.

© REVOLVERMÄNNER GmbH

FAZIT.

PROFESSIONELLE KOMMUNIKATIVE UND TECHNISCHE VORBEREITUNG, KLAR DEFINIERTE ABLÄUFE UND EIN STETIGER AUSTAUSCH SIND ENTSCHEIDEND, OB SIE GUT DURCH DIE KRISE KOMMEN UND KEINE BLEIBENDEN SCHÄDEN ERLEIDEN.

© REVOLVERMÄNNER GmbH

REVOLVERMÄNNER® GMBH
BURGUNDERSTR. 29
40549 DÜSSELDORF

TEL +49 (0) 211 52 06 36 – 0
FAX +49 (0) 211 52 06 36 – 15

WWW.REVOLVERMAENNER.COM

Bernd Fuhlert
bernd.fuhlert@revolvermaenner.com

© REVOLVERMÄNNER GmbH