ITEMS FORUM 2023

VOLKER PULSKAMP

SENIOR VICE PRESIDENT & PARTNER

FLEISHMANHILLARD GERMANY

Cyberangriffe auf Stadtwerke

Die Bedrohung ist real

ZfK Zeitung für kommunale Wirtschaft

Stadtwerke Rodgau: Kompletter Systemausfall

Hacker haben die Systeme der Stadtverwaltung und der Stadtwerke von Rodgau lahm gelegt.

NDR

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Stand: 01.10.2021 17:22 Uhr

Cyberkriminelle haben am Dienstag die IT-Systeme der Stadtwerke in Wismar attackiert. Das wurde am Donnerstag bei der Sitzung der Bürgerschaft bekannt. IT-Sicherheitse arbeiten an der Aufklärung.

EUWID

Cyberangriff auf Stadtwerke Langenfeld

EUWID + 12.11.2019 | ca. 1 Min | Erschienen in Ausgabe 46/2019

Donauwörther Zeitung

LANDKREIS DONAU-RIES

Cyberangriff auf die Stadtwerke Donauwörth erfolgreich verhindert

SPIEGEL Netzwelt

IT-Sicherheit

Hacker greifen Stadtwerke Karlsruhe an und spähen Daten aus

Cyberkriminelle haben beim städtischen Ener ausgelesen. Die Kritische Infrastruktur konnte führt nach Russland.

SWR AKTUELL

Radio Dresden. Wir lieben Dresden!

rbb 24

Potsdam

Stadtwerke nach möglichem Cyber-Angriff online nicht mehr erreichbar

Sa 31.12.22 | 17:55 Uhr 3

Cyberangriff bei den Stadtwerken Pirna

Zuletzt aktualisiert: 03.12.2021 | 17:57 Uhr Autor: Redaktion

teilen

Handelsblatt

Auf die IT- gegeben. ten mit Ho

ENTEGA, FES, STADTWERKE MAINZ

Hackerangriff legt Emails und Websites hessischer Versorger lahm

In der Nacht zu Sonntag wurde der gemeinsame IT-Dienstleister der Unternehmen angegriffen. Die kritischen Infrastrukturen sind nicht betroffen.

13.06.2022 • Update: 13.06.2022 - 17:36 Uhr • Kommentieren • Jetzt teilen

INFOBRIEF VERSCHICKT

Mainzer Stadtwerke warnen Kunden nac Hackerangriff

STAND: 29.7.2022, 11:09 UHR

DER TAGESSPIEGEL

Update / Digitale Bedrohungslage in Potsda

Möglicher Cyberangriff weitet sich aus

Nach dem Rathaus trennen sich jetzt die kommunalen Konzerne vom Internet. Betro Stadtwerke, das Bergmann-Klinikum und die Pro Potsdam.

Von Dominik Lenze und Marco Zschieck

30.12.2022, 15:49 Uhr | Update: 31.12.2022, 16:45 Uhr

Arten von Cyber-Angriffen

Methoden und Techniken entwickeln sich ständig weiter

- Spam, Phishing, Spear-Phishing
- Social Engineering
- Malware (Ransomware, Spyware, Trojaner, Würmer etc.)
- Man-in-the-Middle-Angriffe
- DoS- und DDoS-Attacken
- Kennwortangriffe (Brute-Force-Angriffe, Wörterbuchangriffe)
- Botnetze
- Zero-Day-Exploits
- Advanced Persistent Threats (APTs)
- SQL-Injections
- Drive-by-Downloads
- Cross-Site-Scripting (XSS)

…und plötzlich war es dunkel

…nichts geht mehr…

Kein E-Mail……kein Telefon…….kein Netzwerkzugang……..kein Zugriff auf Dateien……..nichts….


Hello……I am here

10.05.2023
14:30

10.05.2023
14:32

10.05.2023
14:35

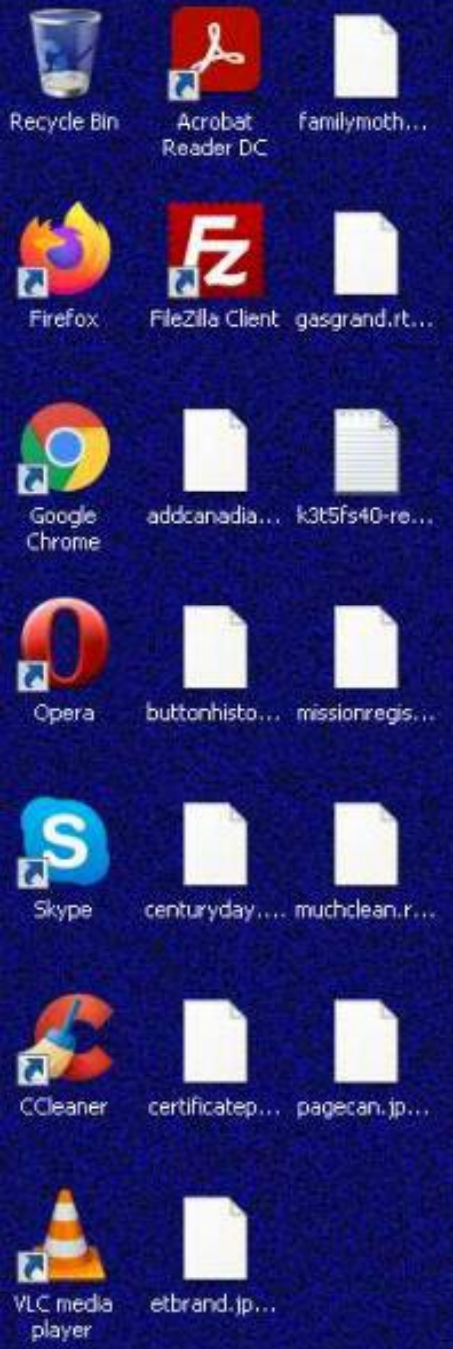
10.05.2023
14:38

error

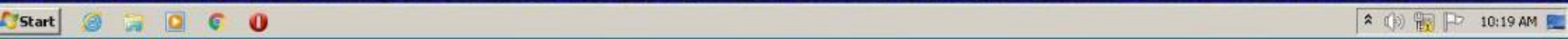

New task
Public tasks
Recycle Bin
Acrobat Reader DC
familymoth...
Firefox
FileZilla Client
gasgrand.rtf
Google Chrome
addcanadia...
missionregis...
Opera
buttonhist...
muchclean.rtf
Skype
centuryday.....
pagecan.jpg
CCleaner
certificatep...
VLC media player
etbrand.jpg
9b11711efed2
4b3c6723521a
7d7eb4a52e4
914db7420e2
78aa36e7274
59d59dd.exe
ANY RUN

All of your files are encrypted!

Find k3t5fs40-readme.txt and follow instuctions



9b11711efed2
4b3c6723521a
7d7eb4a52e4
914db7420e2
78aa36e7274
59d59dd.exe



Your files are encrypted.

All encrypted files for this computer has extension: .0cddd3

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.

Just open our website, upload the encrypted file and get the decrypted file for free.

Additionally, your data have been stolen and if you do not cooperate with us, it will become publicly available on our blog.

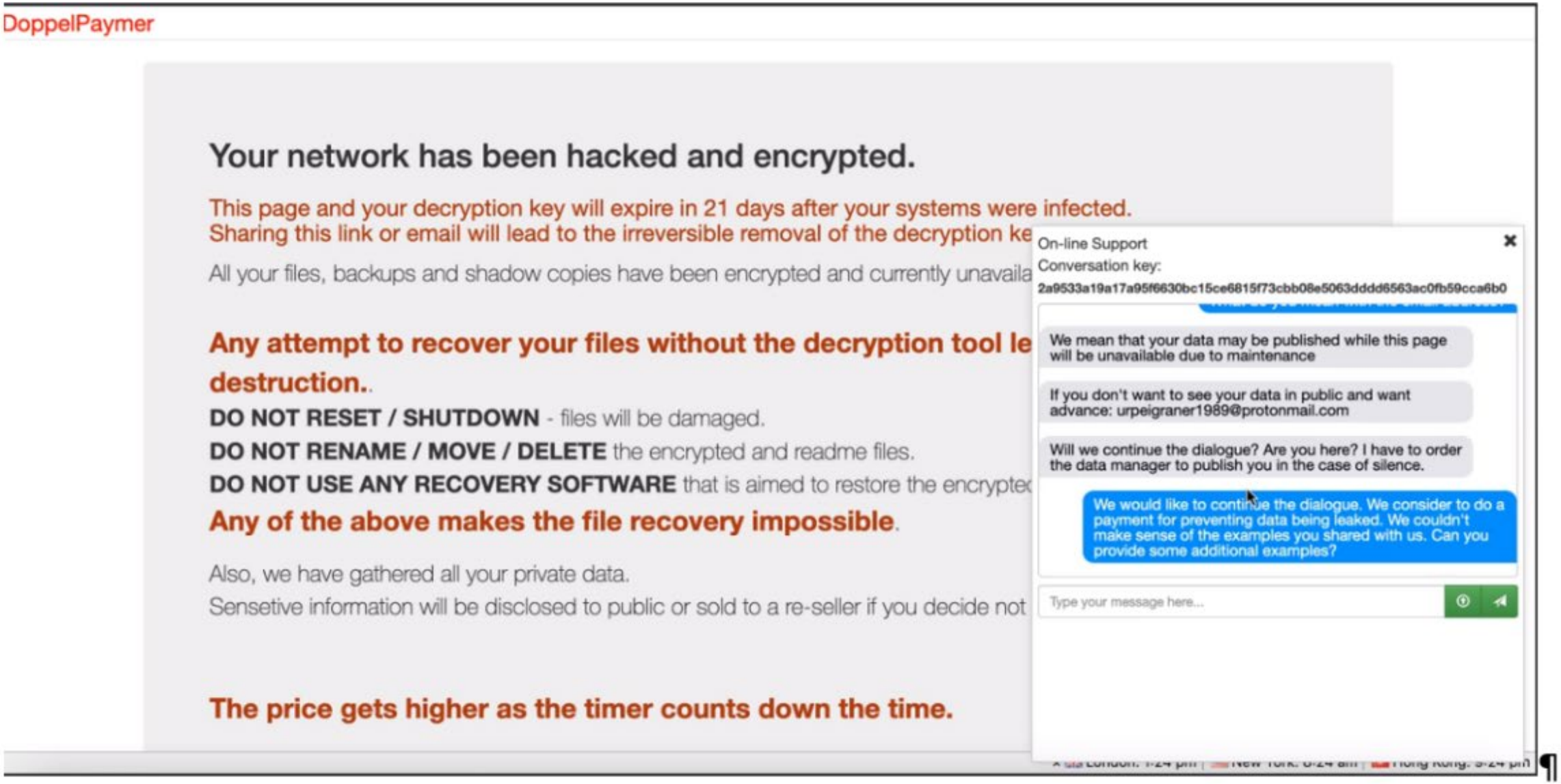
Steps to get access on our website:

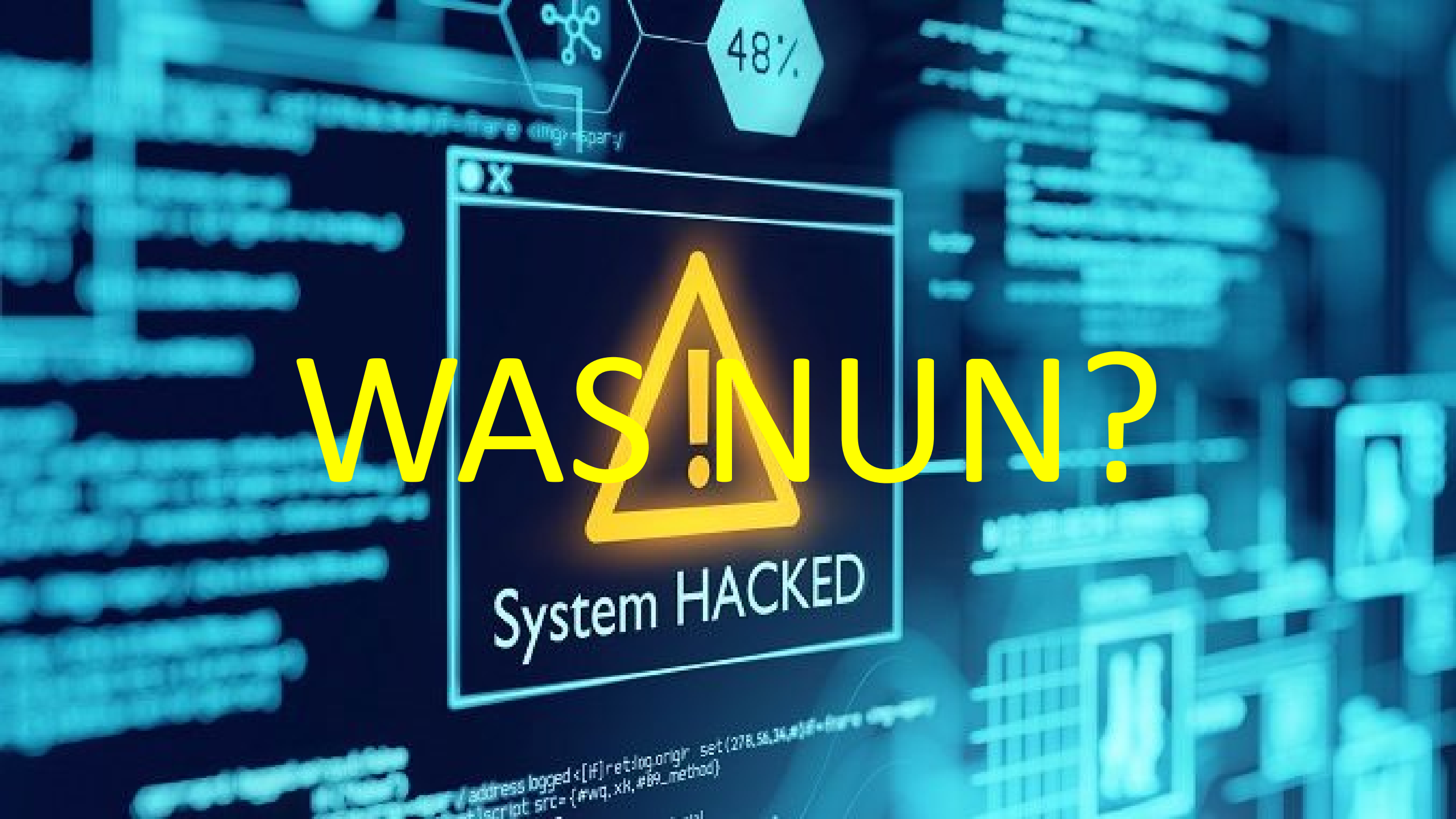
1.Download and install tor-browser: https://torproject.org/

2.Open our website: pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3di.onion

3.Put your personal code in the input form:

{code_0cddd3:
9pWSelA/FIbY6BfjElSjC+M0cXlr5VxCWUfyRwS6XjxphgOafF
rjAFxgHrj5p29x0AqqRzXwdpB/oUqDbTnmjGlKp3PdwHNoCzcO


DoppelPaymer
Your network has been hacked and encrypted.
This page and your decryption key will expire in 21 days after your systems were infected.
Sharing this link or email will lead to the irreversible removal of the decryption ke
All your files, backups and shadow copies have been encrypted and currently unavaila
Any attempt to recover your files without the decryption tool le
destruction..
DO NOT RESET / SHUTDOWN - files will be damaged.
DO NOT RENAME / MOVE / DELETE the encrypted and readme files.
DO NOT USE ANY RECOVERY SOFTWARE that is aimed to restore the encrypte
Any of the above makes the file recovery impossible.
Also, we have gathered all your private data.
Sensetive information will be disclosed to public or sold to a re-seller if you decide not
The price gets higher as the timer counts down the time.
On-line Support
Conversation key:
2a9533a19a17a95f6630bc15ce6815f73cbb08e5063dddd6563ac0fb59cca6b0
We mean that your data may be published while this page will be unavailable due to maintenance
If you don't want to see your data in public and want advance: urpeigraner1989@protonmail.com
Will we continue the dialogue? Are you here? I have to order the data manager to publish you in the case of silence.
We would like to continue the dialogue. We consider to do a payment for preventing data being leaked. We couldn't make sense of the examples you shared with us. Can you provide some additional examples?
Type your message here...



WAS !NUN?


…abtauchen iss nich´…

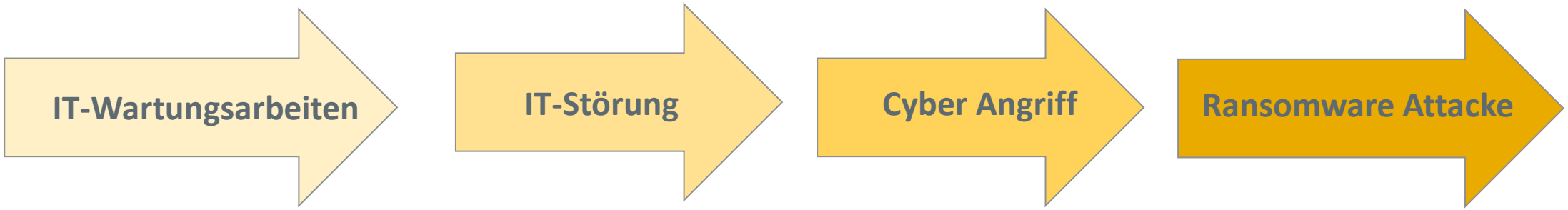
Krisenkommunikation

Grundsätze der Krisenkommunikation

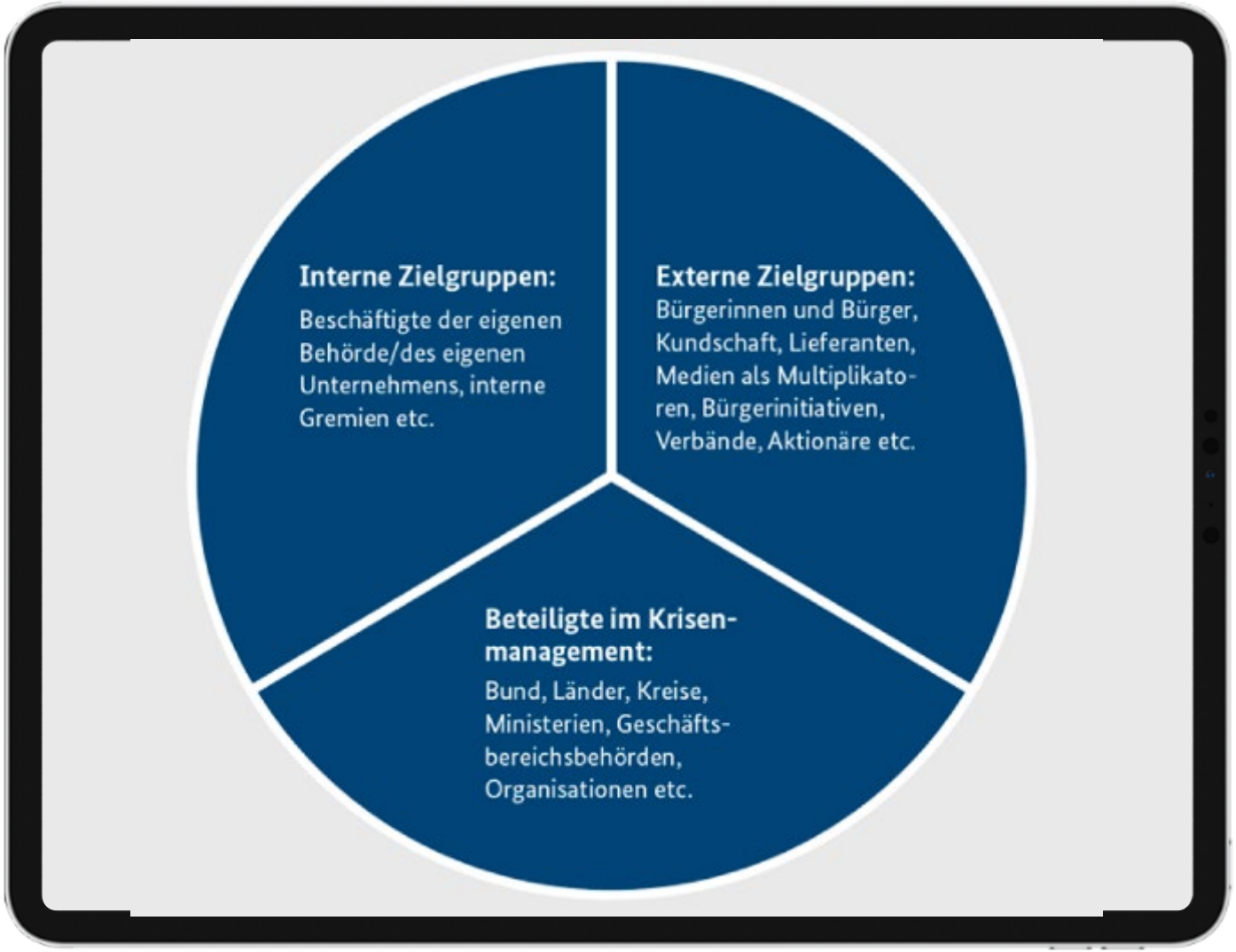
- Schnelligkeit
- Offenheit
- Transparenz
- Glaubwürdigkeit (Immer die Wahrheit sagen – nicht spekulieren)
- Dialogorientierung
- Empathie
- Konsistenz (One Voice)
- Verantwortlichkeit / Konsequenzen professionell tragen
- Vorausschauende Kommunikationsplanung
- Zielgruppen-/Stakeholderanalyse zur zielgerichteten Kommunikation mit Kernbotschaften (Messaging)
- Kontinuierliches Monitoring

Grundsätze der Krisenkommunikation

De-eskalierend agieren – auch kommunikativ – Aufmerksamkeit für Begrifflichkeiten



Krisenkommunikation – Leitfaden des BSI



Jede Krise ist immer auch eine Kommunikationskrise, da die Wahrnehmung der Krise, der Krisenbewältigung und des Managementverhaltens in der Öffentlichkeit ausschlaggebend ist.

- BSI-Standard 100 -4

Leitfaden Krisenkommunikation – BSI, 2014

INFORMIEREN SIE RECHTZEITIG!

- Wer zu lange wesentliche Sachverhalte einer Krise verschweigt, gefährdet seine öffentliche Reputation. Deshalb sollten Sie bereits frühzeitig und ohne unnötige Panik auch über mögliche Risiken informieren, etwa Belastungen für die Umwelt durch Einsickern von Chemikalien in das Grundwasser, gesundheitsgefährdende Ausdünstungen bei einem Brand oder mögliche Datenschutzverletzungen bei einem Informationssicherheitsvorfall.

INFORMIEREN SIE WAHRHEITSGEMÄß!

Sie müssen nicht jedes Detail berichten, aber was Sie berichten, sollte stimmen.

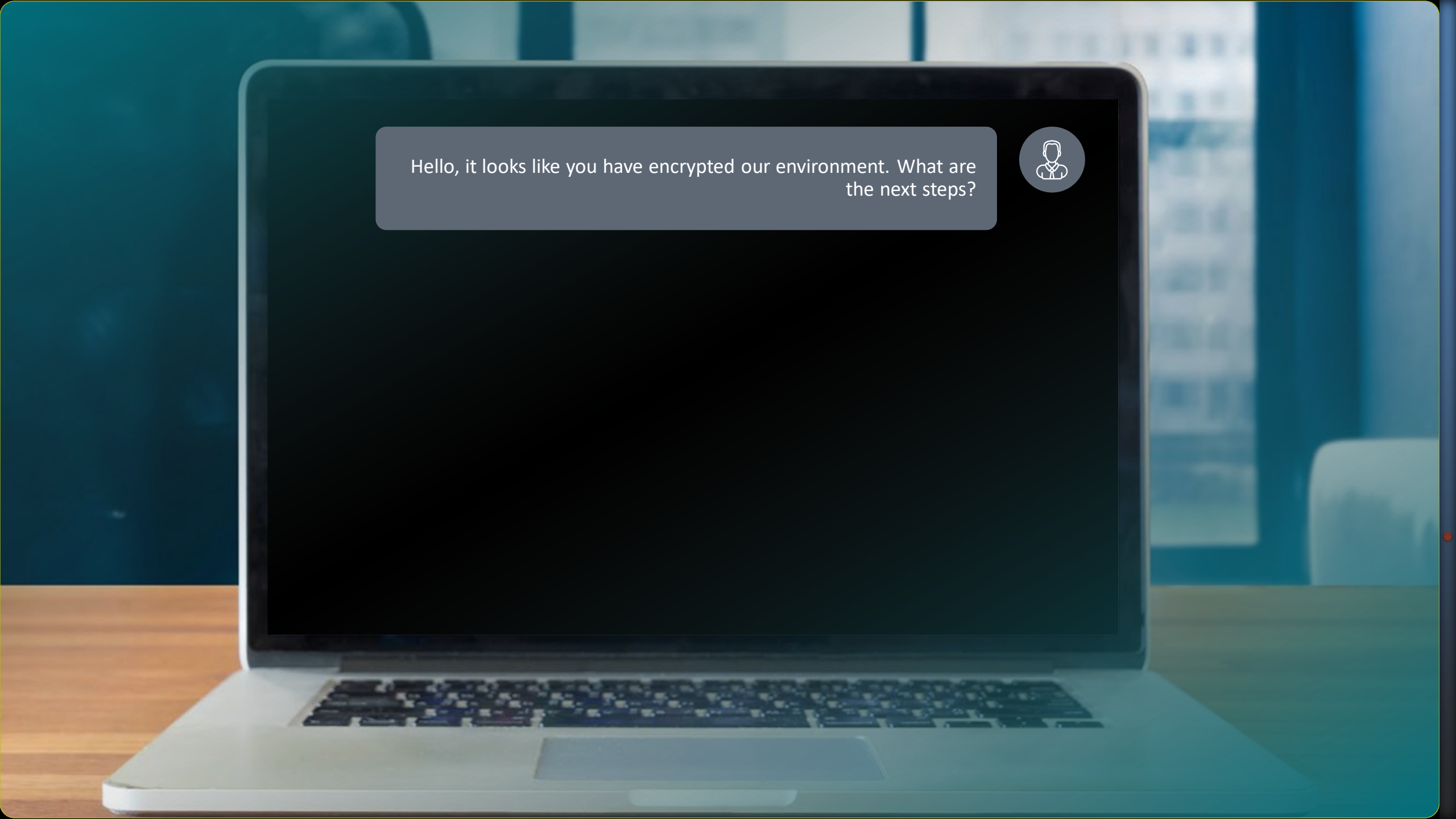
INFORMIEREN SIE SACHLICH UND VERMEIDEN SIE SPEKULATIONEN!

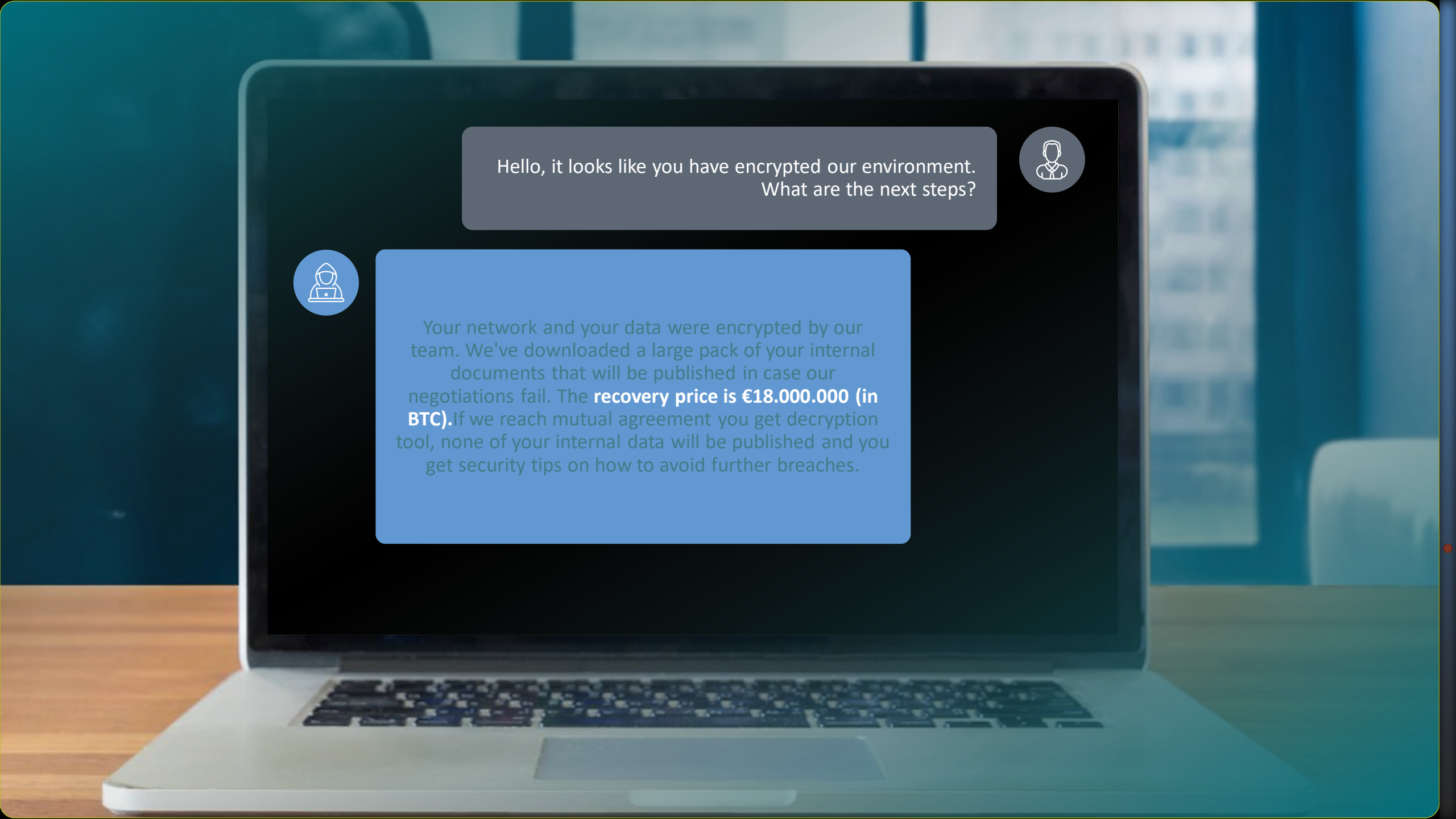
Wenn ein Vorfall Dritte geschädigt hat, sollten Sie gleichwohl das gebotene Einfühlungsvermögen zeigen.

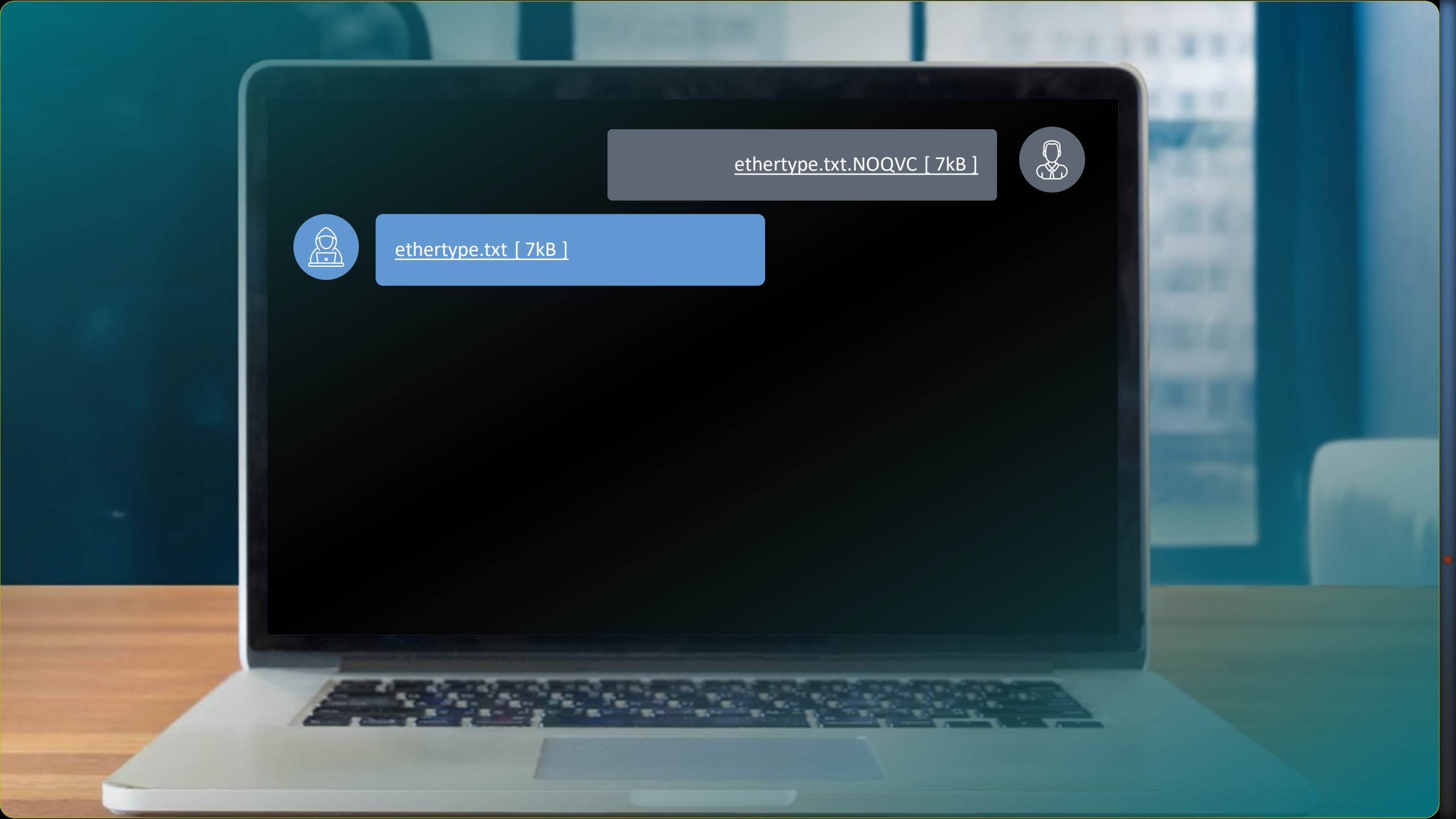
INFORMIEREN SIE VERSTÄNDLICH!

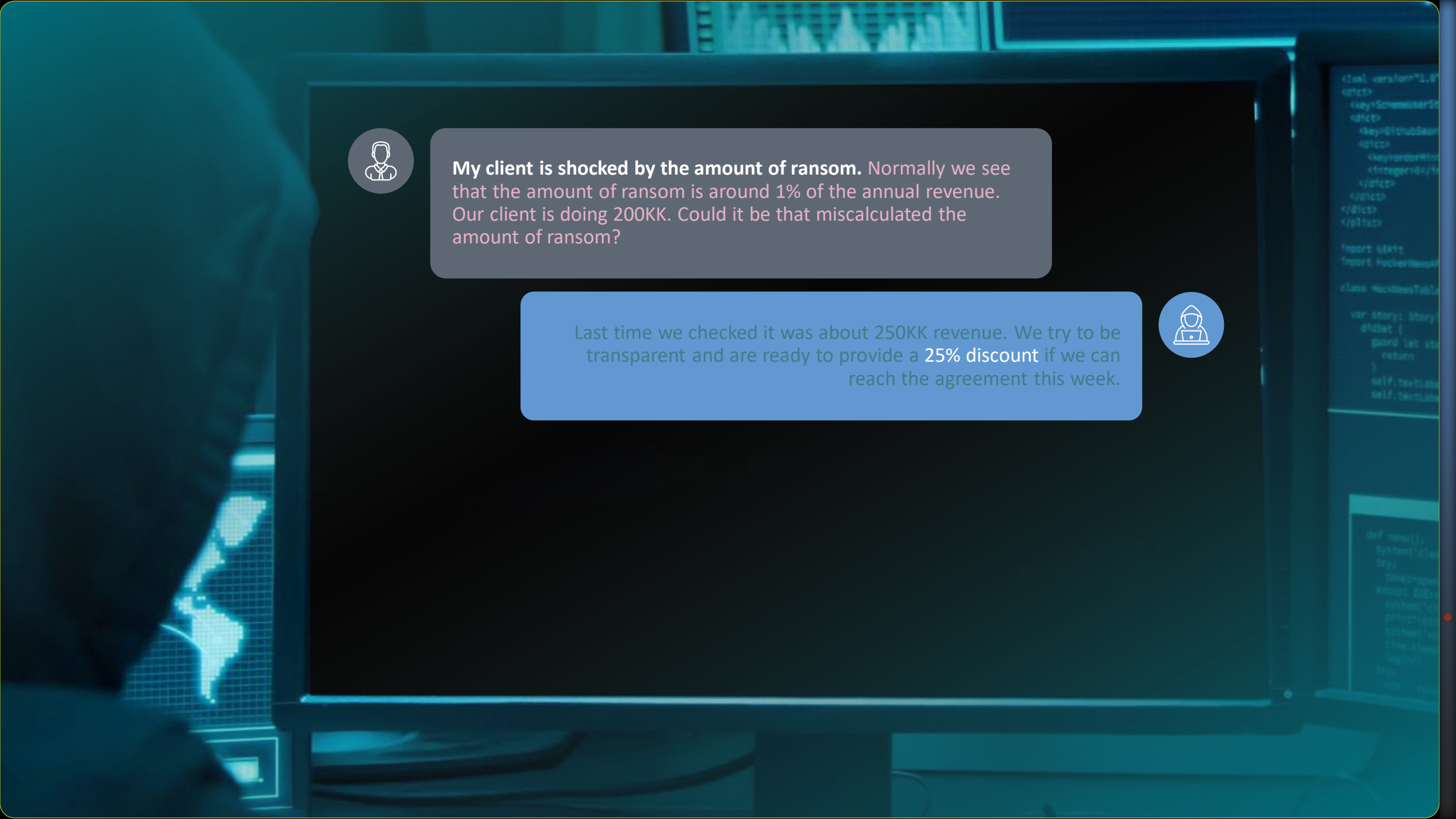
Zu viele Details erschweren das Verständnis und tragen nicht dazu bei, Vertrauen aufzubauen.

Kommunikation mit den Hackern


Hello, it looks like you have encrypted our environment. What are the next steps?


Hello, it looks like you have encrypted our environment.
What are the next steps?
Your network and your data were encrypted by our team. We've downloaded a large pack of your internal documents that will be published in case our negotiations fail. The **recovery price is €18.000.000 (in BTC).**If we reach mutual agreement you get decryption tool, none of your internal data will be published and you get security tips on how to avoid further breaches.


ethertype.txt.NOQVC [7kB]
ethertype.txt [7kB]


My client is shocked by the amount of ransom. Normally we see that the amount of ransom is around 1% of the annual revenue. Our client is doing 200KK. Could it be that miscalculated the amount of ransom?
Last time we checked it was about 250KK revenue. We try to be transparent and are ready to provide a 25% discount if we can reach the agreement this week.

Kommunikation der Hacker

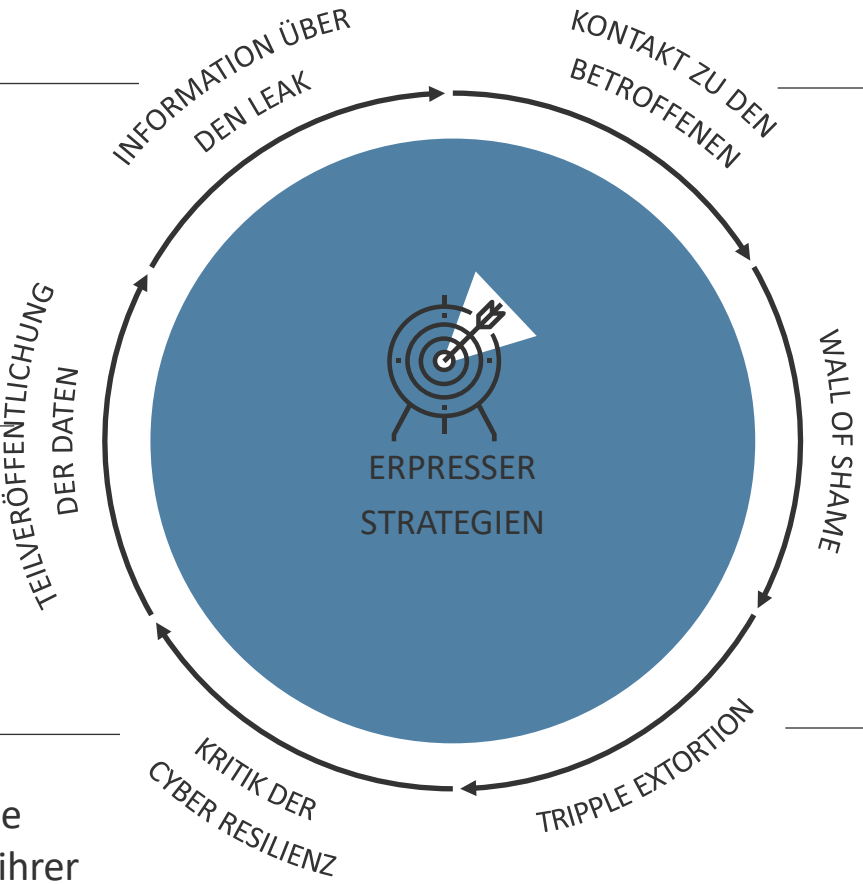
Neuer Trend: Kommunikationsstrategien der Hacker

FÜR DIE SZENARIOPLANUNG KOMMUNIKATIV ZU BERÜCKSICHTIGEN

- Information über den erfolgreichen Datendiebstahl im Dark Web und auf Social Media.

- Teilveröffentlichung der Daten als Beweis für den Datendiebstahl.
- Ziel: Ihre Opfer unter Druck zu setzen.

- Manchmal kritisieren Hacker öffentlich die unzureichenden Sicherheitsmaßnahmen ihrer Opfer.



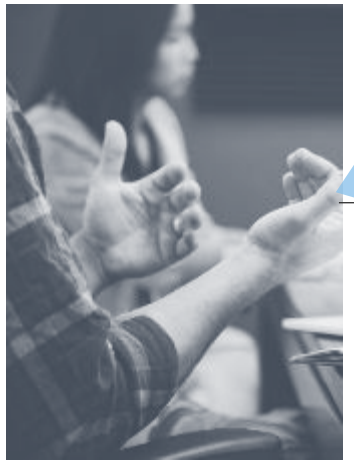
- In einigen Fällen wenden sich Hacker direkt oder über soziale Medien an Betroffene, um zusätzlichen Druck aufzubauen.

- Selten werfen Hacker ihren Opfern vor, im Krisenmanagement die Interessen der betroffenen Stakeholder zu ignorieren (Wall of Shame).

- In seltenen Fällen fordern Hacker nach gescheiterten Verhandlungen Lösegeld direkt von den betroffenen Stakeholdern

Kommunikationsmaßnahmen

ENTSCHEIDUNG ÜBER DIE KOMMUNIKATIONSTAKTIK



AKTIVE / ÖFFENTLICHE KOMMUNIKATION

Beschreibung der Taktik

Die Organisation gibt öffentlich bekannt, dass sie von einem Cyber-Angriff betroffen ist.

Diese Taktik nutzen, wenn:

- Nicht alle Betroffene direkt informiert werden können.
- Öffentliches Interesse am Vorfall ist hoch.

Konsequenzen:

- Größere Kontrolle über das Narrativ.
- Verstärkte Nachfragen durch die Medien.
- Größere Aufmerksamkeit durch den Fall.

REAKTIVE KOMMUNIKATION

Beschreibung der Taktik:

- Informationen über den Vorfall werden den Betroffenen unmittelbar per E-Mail, Telefon oder Brief mitgeteilt
- Auf Nachfrage (z.B. Medien, Kunden) wird kommuniziert

Wichtigste Faktoren:

- Geringe Wahrscheinlichkeit, dass der Vorfall öffentlich bekannt wird.
- Betroffene spezifische Informationen zum Vorfall werden benötigt. (Proof points)

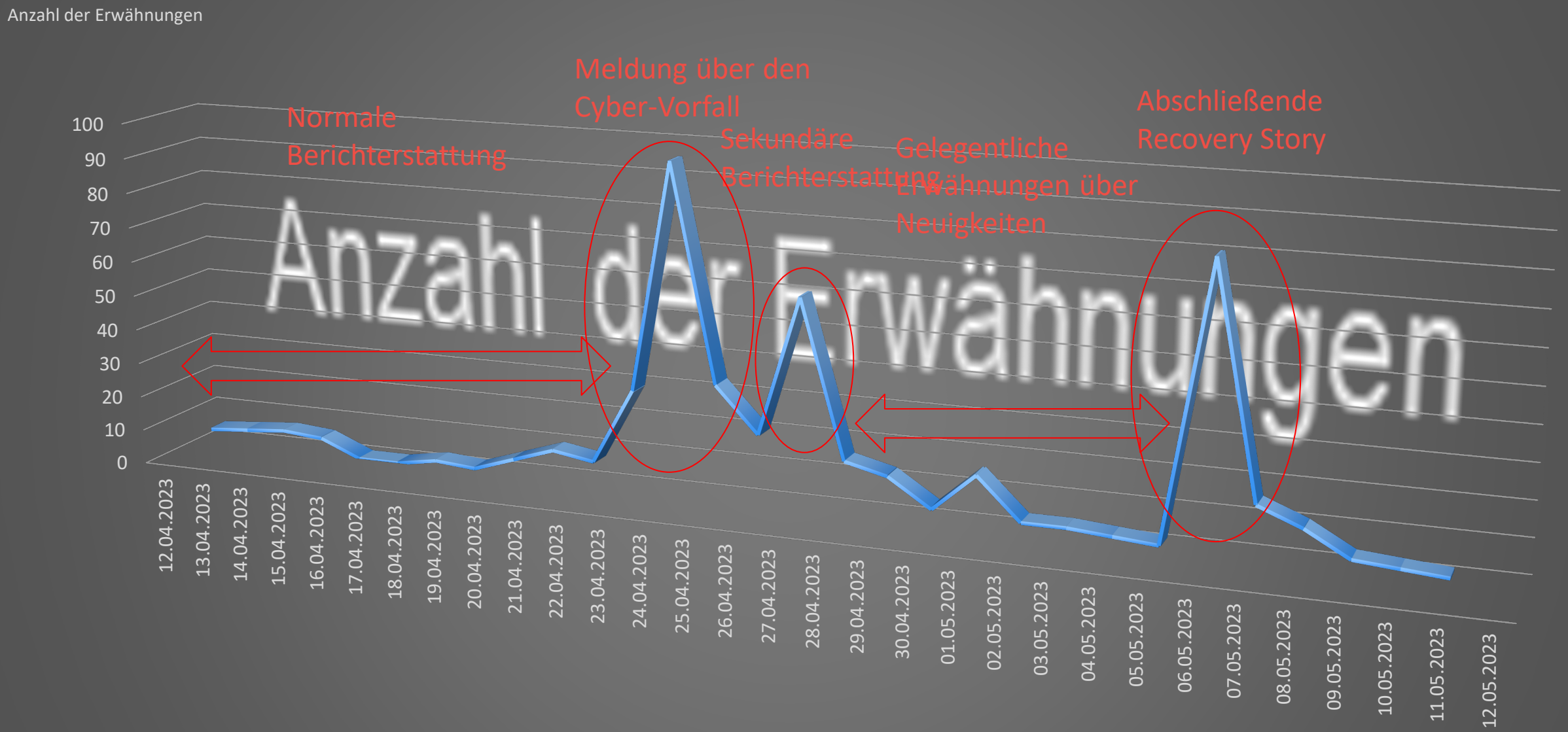
Konsequenzen:

- Größerer Aufwand bei der Umsetzung.
- Geringere öffentliche Aufmerksamkeit.
- Die Möglichkeit, den Vorfall im Rahmen der Wiederherstellung als gelöstes Problem öffentlich zu machen. (Recovery Story)

Professionelle Kommunikationsmaßnahmen im Cyber Krisenfall

- Kommunikative Analyse der Situation inkl. Szenarioplanung (Driver Seat)
- Meldepflicht beachten (Datenschutz/72h)
- Entscheidung Kommunikationsstrategie (Aktive versus reaktive Kommunikation)
- Set-up Social Media Monitoring mit Alertfunktion (Radar)
- Erstellung Q&As und FAQs für konsistente Kommunikation der Sprecher, des Managements, der Mitarbeiter:Innen
- Erstellung Krisen-Kommunikationsplan
- Regelmäßige, vorausschauende Erstellung der internen Kommunikation (ZG Mitarbeiter:Innen)
- Regelmäßige vorausschauende Erstellung der externen Kommunikation (
  ZG Kunden, Geschäftspartner, Behörden, Stakeholder)
- Aufbau und Kommunikation der Recovery Story (Timing)
- Reputation Recovery Programme

Medienanalyse



Die 10 Goldenen Regeln der Cyber Kommunikation

Regel 1

Holen Sie die richtigen Partner an Bord

1. Holen Sie sich die richtigen Partner an Bord – und zwar frühzeitig

Bereits in „Friedenszeiten“ sollten Sie prüfen, ob Sie die notwendigen Ressourcen und die Expertise im eigenen Hause haben, um im Falle eines Cyberangriffs schnell und angemessen reagieren zu können. Dies betrifft nicht nur Ihre IT-Abteilung, sondern auch die Bereiche **Recht, Datenschutz und Krisenkommunikation** sowie die Spezialbereiche **Forensik, Data Security und Recovery**.

Versicherungen mit entsprechenden Cyber-Policen können im Schadensfall in der Regel innerhalb kürzester Zeit ein Expertenteam aus IT-Forensikern, Rechtsberatern und Krisenkommunikationsexperten zusammenstellen.

Diese sind oft als Incident-Team und -Netzwerkpartner bereits eingespielt und bringen sehr, sehr schnell herausragenden Mehrwert und Unterstützung - **365/24/7** für Sie erreichbar sind, national wie international.

1. Holen Sie sich die richtigen Partner an Bord – und zwar frühzeitig

Best-in-Class Partnerschaften für beste Unterstützung

In Zusammenarbeit mit erstklassigen Partnern und gestützt auf die Stärke eines globalen Netzwerks mit nachgewiesener Erfahrung in der Krisenarbeit haben wir zahlreiche Krisenprojekte in verschiedenen Branchen erfolgreich durchgeführt. Zusammen mit unseren Partnern können wir eines der stärksten Krisenteams der Welt anbieten.

RECHT

- Norton Rose Fulbright
- Noerr
- CMS Law.Tax
- DAC Beachcroft
- Kennedys
- Freshfields
- Mayer Brown

FORENSIK/BERATUNG

- National Science Foundation
- Mandiant
- Northwave Intelligent Security Operations
- Grant Thornton
- KPMG
- InfoGuard Swiss Cyber Security
- CyberClan

PARTNERSCHAFTEN

- SmartRiskSolutions Risk & Crisis Management Consultancy
- Crawford
- AFC Consulting Group
- Talkwalker
- moneypenny
- Marsh
- experian
- social simulator

Regel 2

Stellen Sie sicher, dass die Kommunikationsverantwortlichen im Krisenstab mit am Tisch sitzen

2. Stellen Sie sicher, dass die Kommunikationsverantwortlichen im Krisenstab mit am Tisch sitzen

Jedes Unternehmen sollte über ein Cyber Incident Response Team (CIRT) verfügen, dem ein/e leitende/r Kommunikationsverantwortliche/r angehört. Dies hilft dabei, eine Brücke zwischen der IT-Abteilung, der Rechtsabteilung, der Geschäftsleitung sowie externen Partnern zu schlagen und sicherzustellen, dass das Kommunikationsteam in einer dynamischen Situation stets über aktuelle und verlässliche Informationen aus IT-Forensik und -Recovery verfügt. Der schnelle Zugang hierzu ist in der Cyber-Krise essenziell, denn er stellt die Voraussetzung für eine transparente und konsistente Kommunikation nach innen und außen dar inkl. fundierter Kommunikationsplanung

Regel 3

Seien Sie vorbereitet – Prävention und Training sind Key!

3. Seien Sie vorbereitet – Prävention und Training sind Key!

Die drei Geheimnisse einer professionelle Cyber-Krisenkommunikation lauten: Vorbereitung, Vorbereitung, Vorbereitung!

Nutzen Sie die erwähnten „Friedenszeiten“, um alle Vorkehrungen für verschiedene Krisenszenarios bereits jetzt zu treffen.

Dazu gehört auch das intensive Training des Krisenteams oder Krisenkommunikationsteams, z.B. in Form einer Krisensimulation des CIRT: Spielen Sie eine Cyber-Krise komplett durch, machen Sie eine Gap-Analyse, um zu ermitteln, wo noch Lücken bestehen, sei es bezüglich der Kommunikation (zum Beispiel: Welche Sprachen müssen wir abdecken? Existieren Textbausteine für diverse Szenarien und Eskalationsstufen?) oder in Bezug auf die IT – gibt es z.B. für die Systemwiederherstellung eine Priorisierung der Server oder auch extern gelagerte Backups oder Cloud-Lösungen?

Klären Sie Rollen, Aufgabenverteilung und Verantwortlichkeiten innerhalb der Taskforce und üben Sie diese vorab ein.

Regel 4

Seien Sie auf dem neusten Stand hinsichtlich Compliance und Regulierung / Gesetzgebung

4. Seien Sie auf dem neusten Stand der Compliance und Regulierung / Gesetzgebung

Es ist von entscheidender Bedeutung, dass der Chief Communications Officer mit den **aktuellen regulatorischen Anforderungen an Datenschutz und Cyber Security sowie den entsprechenden Berichtspflichten** vertraut ist, ähnlich wie der Chief Compliance Officer. Dies gilt in besonderem Maße, wenn Ihr Unternehmen **international** tätig ist:

Neben der **EU-Datenschutz-Grundverordnung (DSGVO)** oder der **britischen Datenschutzverordnung**, die beide im Falle einer Verletzung des Schutzes personenbezogener Daten eine Berichtspflicht an die zuständigen Datenschutzbehörden innerhalb von **72 Stunden** vorschreiben, können weitergehende Berichtspflichten bestehen.

So sind in den USA beispielsweise börsennotierte Unternehmen von der **Securities Exchange Commission** verpflichtet, ein Formular 8-K einzureichen, um über „wichtige Ereignisse, von denen die Aktionäre wissen sollten“, zu informieren, zu denen auch ein Cyberangriff zählt.

Regel 5

Richten Sie unabhängige Kommunikationskanäle zu Ihren Stakeholdern ein

5. Richten Sie unabhängige Kommunikationskanäle zu Ihren Stakeholdern ein

Haben Sie schon einmal darüber nachgedacht, wie Sie Ihre Mitarbeiter, Kunden und Geschäftspartner erreichen können, wenn Ihr E-Mail-System nicht mehr funktioniert? Wenn Sie nicht mehr auf Adressbücher zugreifen können und auch die Telefonanlage außer Gefecht ist?

Für diesen Fall benötigen Sie alternative Kommunikationskanäle, um mit Ihren Stakeholdern weiterhin Kontakt zu halten und Informationen schnell und effektiv verbreiten zu können – gerade auch in Krisensituationen. Unternehmen sollten daher auch Cloud-basierte, von der eigenen IT unabhängige Plattformen in Erwägung ziehen, die eine Kommunikation in beide Richtungen ermöglichen und im Bedarfsfall schnell per Knopfdruck in Betrieb genommen werden können.

Regel 6

Nutzen Sie digitale Tools – aber behalten Sie analoge Alternativen in der Hinterhand

6. Nutzen Sie digitale Tools – aber behalten Sie analoge Alternativen in der Hinterhand

Erreichbarkeit und Verfügbarkeit sind die Voraussetzung, um im Krisenfall handlungsfähig zu bleiben. Neben separaten E-Mail-Plattformen bieten sich hierfür gerade in der internen Kommunikation auch mobile Mitarbeiter-Apps an, über die sich Mitarbeiter/innen ortsunabhängig mobil erreichen lassen.

Ebenfalls sollten Sie bereits im Vorfeld klären, wie sie Mitarbeiter/innen im Home Office auch abseits der unternehmenseigenen Kanäle per Telefon oder E-Mail erreichen können – hier gilt es, etwaige Betriebsvereinbarungen zu beachten und gegebenenfalls den Betriebsrat frühzeitig für einen etwaigen Krisenfall einzubinden.

Hat Ihr Unternehmen Mitarbeiter/innen in der Produktion, die nicht direkt über Telefon oder E-Mail erreichbar sind, sollten Sie auch über analoge Kommunikationsmittel im Vorfeld nachdenken. Neben (Corona-konformen) Team- und Townhall-Meetings können dies auch schlichte Aushänge oder Kopien aus Papier sein. Auch hier können Templates und Standorte für die Information bereits jetzt definiert werden, um im Krisenfall Zeit zu sparen.

Regel 7

Haben Sie Ihre Botschaften und Textbausteine parat

7. Haben Sie Ihre Botschaften und Textbausteine parat

Ja, jede Krise ist anders.

Dennoch gibt es viele Dinge, die Sie vorbereiten können, um in einer Krisensituation wie einem Cyberangriff schneller reagieren zu können. Vorbereitung ist das A und O – aber haben Sie bereits die Bedürfnisse und Anforderungen aller Ihrer Stakeholder und Hauptzielgruppen bedacht?

Haben Sie Vorlagen für Mitarbeiter- und Kundeninformationen – und wenn ja, auch für verschiedene Eskalationsstufen? Wie steht es mit Pressemitteilungen, Holding- und Leak-Statements – je nachdem, ob Sie sich mit Ihrer Kommunikationsstrategie im reaktiven oder aktiven Modus befinden?

Aus Erfahrung lässt sich sagen: Es ist viel einfacher, mit etwa 70 bis 90 Prozent an bereits vorbereiteten Texten zu beginnen, als mit einem leeren Blatt Papier – insbesondere dann, wenn Sie dafür juristische Beratung oder spezielle, interne Freigaben benötigen, zum Beispiel von Fachabteilungen oder dem Datenschutz.

Auch hier werden Sie schneller durch clevere Vorbereitung.

Regel 8

Achten Sie auf die richtige Sprache – und verhindern Sie „undisziplinierte“ Kommunikation

8. Achten Sie auf die richtige Sprache – und verhindern Sie „undisziplinierte“ Kommunikation

Gerade zu Beginn einer Cyber-Krise kann der weitere kommunikative Verlauf ganz wesentlich davon abhängen, was wie und wann kommuniziert wird. Eine vorschnelle, unüberlegte Kommunikation richtet in aller Regel mehr Schaden als Nutzen an.

Es macht einen riesigen Unterschied, ob ein CEO direkt über Twitter veröffentlicht „Wir wurden gehackt – ich stehe bereits in Kontakt mit den Erpressern“, oder ob die Firmen-Website vermeldet „Es gibt derzeit eine IT-Störung aufgrund von Wartungsarbeiten“.

Regel 9

Bestimmen Sie das Narrativ – Sitzen Sie „im Driver Seat“ der Kommunikation

9. Bestimmen Sie das Narrativ – Sitzen Sie „im Driver Seat“ der Kommunikation

Bei einem laufenden Cyberangriff gibt es mehr unbekannte als bekannte Variablen.

Als Kommunikationsverantwortliche/r sind Sie die zentrale Informationsquelle nach innen und außen – nutzen Sie diesen Vorteil, um sich in den „Driver Seat“ der Kommunikation zu setzen. Jeder wird auf Ihre Botschaften zur aktuellen Entwicklung und zum Status hören, seien sie positiv bei voranschreitender Wiederherstellung der Betriebsabläufe oder negativ bei neuen Eskalationen – aber Sie sollten die Geschichte in der Hand haben, steuern und navigieren.

Umso wichtiger ist es, dass Sie stets über die neusten Erkenntnisse und aktuellen Informationen zur Lage in Forensik und IT-Recovery verfügen.

Regel 10

Lernen Sie aus der Krise

10. Lernen Sie aus der Krise

Nach der Krise ist vor der Krise. Ist der Cyberangriff erfolgreich abgewehrt oder beendet und sind die IT-Systeme wieder hergestellt, sollte der Krisenstab bzw. das CIRT direkt die wichtigsten Lehren und Erkenntnisse aus allen Bereichen ziehen, um nachhaltig gestärkt aus der Krise hervorzugehen.

Oftmals können Unternehmen sogar aus der Not eine Tugend machen und den „Schwung“ der Krise nutzen, um weitere, häufig längst überfällige Maßnahmen in Angriff zu nehmen. Dazu kann die Einführung zusätzlicher IT-Sicherheitsmaßnahmen wie Multi-Faktor Authentifizierungen, IT-Sicherheits- und Datenschutz-Schulungen für Mitarbeiter/innen, die Erstellung bzw. Aktualisierung von Krisenhandbüchern, Medien- und Krisentraining für Pressesprecher/innen ebenso zählen wie die Erstellung von Social-Media- oder Kommunikations-Guidelines.

….und zum guten Schluss noch eine Frage an Sie…

Lösegeld zahlen oder nicht zahlen?

„Trusted Criminals“?


DISKUSSION


FRAGEN

Vielen Dank für Ihre Aufmerksamkeit

VOLKER PULSKAMP

Head of Corporate Communications &
Crisis Lead Germany (A.R.C. Certified)
Global and EMEA Crisis Team

+49 (0)173 8998 739
volker.pulskamp@fleishman.com

VOLKER PULSKAMP IS A VERSATILE A.R.C.-CERTIFIED CRISIS CONSULTANT WHO BRINGS MORE THAN 26 YEARS OF GLOBAL EXPERIENCE IN ORGANIZING AND MANAGING COMMUNICATIONS PROGRAMS AND PROCESSES. AS A MEMBER OF THE MANAGEMENT TEAM OF FLEISHMANHILLARD GERMANY AND HEAD CORPORATE COMMUNICATIONS, HE SPECIALIZES IN THE CONCEPTION AND IMPLEMENTATION OF COMMUNICATION PROGRAMS IN A WIDE VARIETY OF FACETS.

AS CRISIS LEAD GERMANY AND PART OF THE EMEA CRISIS TEAM FOR FLEISHMANHILLARD, CRISIS COMMUNICATION, CRISIS PREVENTION, CRISIS TRAINING, AND CRISIS SIMULATIONS MAKE UP A LARGE PART OF HIS WORK. HE HAS EXTENSIVE EXPERIENCE IN ISSUES AND CRISIS MANAGEMENT AND HAS MANAGED NUMEROUS CRISES FOR VARIOUS COMPANIES. IN NUMEROUS CASES, HE HAS BEEN BOTH THE MAIN CONTACT PERSON AND COMPANY SPOKESPERSON. AS A CRISIS AND MEDIA TRAINER, HE HAS TRAINED MORE THAN 250 PEOPLE (CEOS, TOP MANAGEMENT, MID-LEVEL MANAGEMENT TEAMS) IN INDIVIDUAL OR TEAM TRAININGS DURING HIS CAREER.

AS A FORMER NEWS AGENCY JOURNALIST AND PRESS OFFICER FOR LEADING GLOBAL COMPANIES, VOLKER PULSKAMP IS THE PERFECT COMMUNICATIONS CONSULTANT AND COACH FOR TOP MANAGEMENT AND LEADERSHIP TEAMS WHO NEED TO GET MESSAGES ACROSS AND APPEAR CONFIDENT IN CRISIS AND INTERVIEW SITUATIONS - EVEN UNDER PRESSURE.

APPENDIX

Meldepflichten

Art. 33 DSGVO

Verantwortliche im Sinne der DSGVO

§ 8b BSIG

Betreiber von Kritischer Infrastruktur

§ 8c BSIG

Anbieter Digitaler Dienste (etwa Online-Marktplätze oder Cloud Dienste)

§ 8f BSIG

Unternehmen im besonderen öffentlichen Interesse

§ 168 TKG

Betreiber öff. TK-Netze oder TK-Dienste

§ 54 ZAG

Zahlungsdienstleister

§ 24 KWG

Auslagernde Institute

§ 6 AtSMV

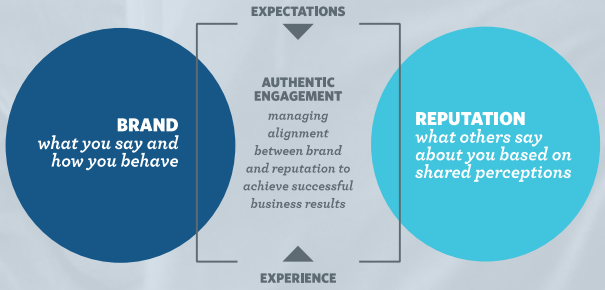
Inhaber von atomrechtlichen Genehmigungen

- In Europa: Starke Orientierung an NIS-Richtlinie (ggf. Kooperation über BSI suchen)
- Weltweit:
  - Sehr heterogenes Feld, insbesondere in China; in USA Ebene der Bundesstaaten prüfen
  - Teilweise sind Verträge mit Regierungsorganisationen ausschlaggebend

FLEISHMANHILLARD

UNSERE DNA

Wir sind überzeugt, dass die Reputation eines Unternehmens und seine positive Rolle, die es in einer Gesellschaft spielen kann, untrennbar miteinander verbunden sind. Deshalb helfen wir Organisationen dabei, ihre Reputation zu schützen und zu stärken – durch einen kanalübergreifenden authentischen Dialog mit allen Anspruchsgruppen. Unsere Teams verwandeln datenbasierte Insights in strategisch zielgerichtete und kreativ begeisternde Kommunikations-kampagnen, die sich von der Masse abheben – und damit das Marktpotenzial jeder Marke freisetzen.



FLEISHMANHILLARD IN DEUTSCHLAND

+100
Berater:innen in Deutschland

WIR SIND DORT, WO SIE UNS BRAUCHEN

Wir haben mehr als 2.200 Kolleg:innen an 80 Standorten in mehr als 30 Ländern. Und wir sind so strukturiert, dass wir fast überall auf der Welt schnell die richtige Expertise und Erfahrung für unsere Kunden bereitstellen können.

UNSERE LEISTUNGEN

- Brand Positioning
- Change & Transformation
- Content Development & Storytelling
- Design & Creative
- ESG & Sustainability Consulting
- Government Relations, Policy & Advocacy
- Internal Communications & Employer
- Branding
- Issues & Crisis Management
- Media & Influencer Relations
- Product Marketing
- Reputation Management
- Research, Analytics & Measurement
- Strategic & Creative Planning

FLEISHMANHILLARD WORLDWIDE

OUR PHILOSOPHY

"To make ourselves as valuable to our clients as they are to us…"®

100+
industry accolades
In the past year,
Including

Cannes Festival of Creativity

ICGO Global Awards

Global Sabre Awards

PRWeek Award

Silver Anvil Awards

Shorty Awards

2010-2017 NAFE TOP COMPANIES FOR EXECUTIVE WOMEN

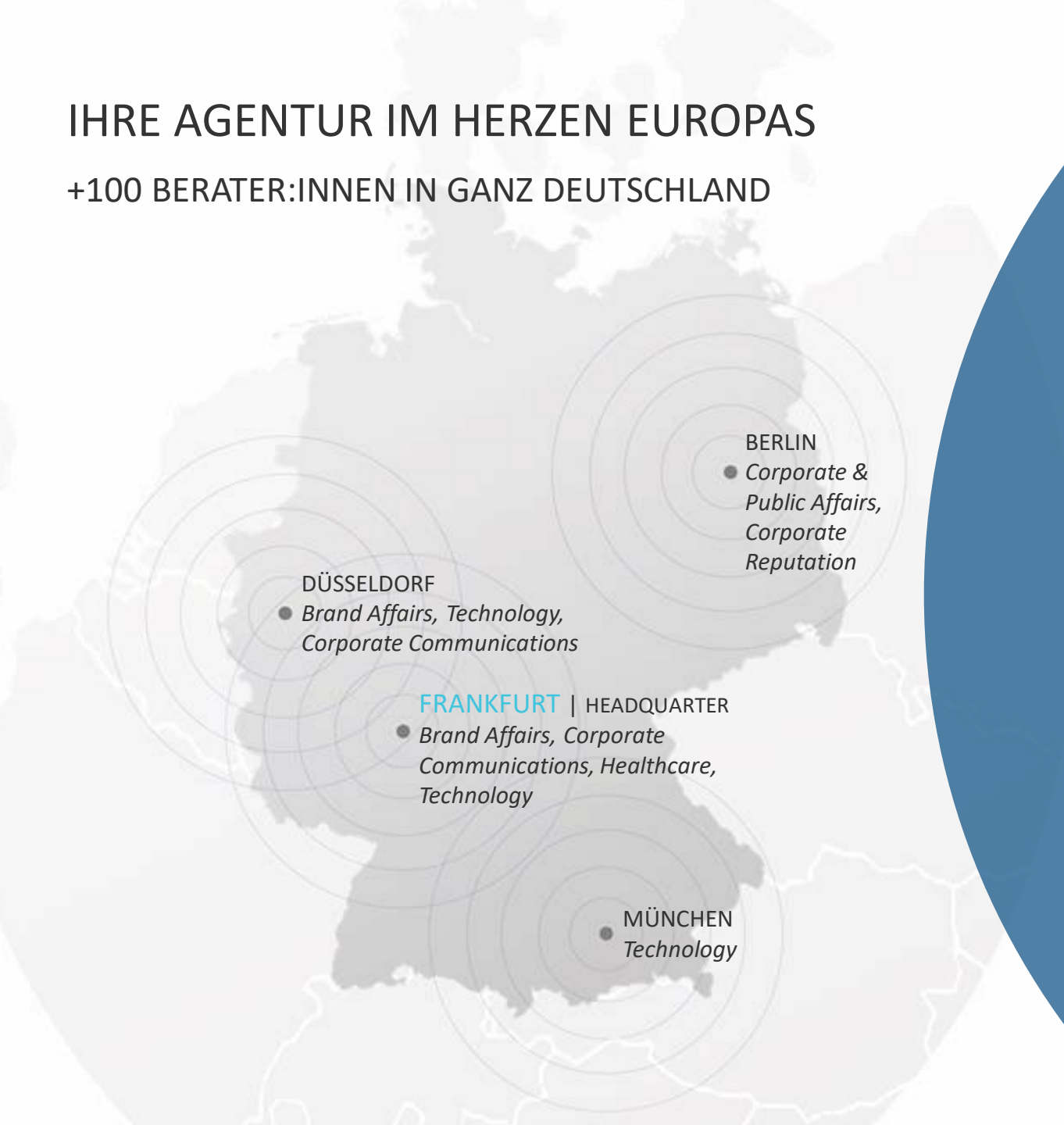
PRNEWS' CSR A-LIST 2013-2017

Long-standing
Client
Relationship

63 years	28 years	28 years	27 years	26 years	24 years	22 years	19 years	19 years	14 years	14 years
EMERSON	AT&T	Hallmark	BOY SCOUTS OF AMERICA	P&G	Johnson&Johnson	Lilly	BAYER	PHILIPS	ENTERPRISE HOLDINGS	PEPSICO

IHRE AGENTUR IM HERZEN EUROPAS

+100 BERATER:INNEN IN GANZ DEUTSCHLAND



BERLIN
Corporate & Public Affairs, Corporate Reputation

DÜSSELDORF
Brand Affairs, Technology, Corporate Communications

FRANKFURT | HEADQUARTER
Brand Affairs, Corporate Communications, Healthcare, Technology

MÜNCHEN
Technology

AUSWAHL CYBER-KRISENKUNDEN

KURZ UND BÜNDIG: UNSER ANGEBOT

KRISENMANAGEMENT

24/7/365 KRISEN-SUPPORT

Das 24/7/365 Ad-hoc-Beratungs- und Serviceangebot von FleishmanHillard Germany sowie den mehr als 80 internationalen FH-Büros mit mehr als 200 spezialisierten Krisenkommunikations-berater:innen und über 2.700 Mitarbeiter:innen. Je nach Situation und den erforderlichen Kommunikations-aufgaben/-dienstleistungen stellt FH das Krisenkommunikationsteam national oder international zusammen.

KRISEN-HOTLINE

Entwicklung und Durchführung eines individualisierten Krisenhotline-Trainings zur Beantwortung externer Anfragen an das Unternehmen im Falle einer aktuellen oder potentiellen Krise. Simulation aller Hotline-Prozesse im Krisenfall, Training von Melde- und Informationsketten inkl. Vermittlung von Basiswissen zur Beantwortung kritischer Fragen am Telefon.

KRISEN-MONITORING

Entwicklung und Erstellung eines kundenspezifischen Social- und Online-Medien-Monitorings inkl. Dashboard mit Alert-Funktion. Jederzeitige Aktivierung für den Kunden innerhalb einer Stunde nach Alarmierung, um die aktuellen Diskussionen und Medienbeiträge zur akuten Krise in Echtzeit 24/7/365 online scannen zu können, in bis zu 26 Sprachen.

KURZ UND BÜNDIG: UNSER ANGEBOT

KRISENPRÄVENTION

ASSESSMENT

Bewertung der bestehenden Krisenprozesse und -materialien, Analyse der Kommunikationsstruktur, der Fähigkeiten und der Krisenerfahrung des Kommunikationsteams des Kunden mit Empfehlungen zur Optimierung (Gap Analysis).

KRISEN-MEDIENTRAINING

Entwicklung und Durchführung eines maßgeschneiderten Krisenmedientrainings für zwei bis vier Teilnehmer:innen zur Vorbereitung von Kommunikationsverantwortlichen/ Sprecher:innen auf relevante Krisensituationen. Die Teilnehmer:innen werden in Theorie und Praxis intensiv auf mögliche Krisensituationen vorbereitet und im richtigen Umgang mit Medien inkl. Videoaufzeichnung und Feedbackanalyse geschult.

CRISIS COMMUNICATION PLAYBOOK / CRISIS POCKET GUIDE

Entwicklung eines maßgeschneiderten Krisenkommunikations-Playbooks zur Unterstützung und Vorbereitung auf mögliche Krisenkommunikationsszenarien, einschließlich Darstellung der relevanten Krisenkommunikations-prozesse, Berichtsketten, Verantwortlichkeiten, Aufgaben-verteilung, Mitgleider des Krisenteams, Kontaktdaten interner/externer Stakeholder /Kernbotschaften des Unternehmens, Vorlagen für Krisenreaktionsmaterialien

KRISENSIMULATION

Entwicklung und Durchführung einer individuellen, halbtägigen Krisensimulation für das Krisenteam des Auftraggebers inkl. Konzeptentwicklung. Training von zuvor definierten Krisenszenarien sowie Simulation aller Krisenprozesse im Krisenfall, Training von Berichts- und Informationsketten; Training zur Entwicklung von Krisenkommunikations-materialien.

AUF JEDES ISSUE VORBEREITET

UNSER BEWÄHRTER ANSATZ FÜR ISSUES & CRISIS MANAGEMENT

Die Berater:innen von FleishmanHillard haben eine Vielzahl von Unternehmen beim Aufbau und Schutz ihrer Reputation begleitet. Reputationsmanagement erfordert proaktiven Schutz. Wir antizipieren die Risiken, die potenziell negative Auswirkungen auf Ihre Reputation haben können und entwickeln Programme, die diese Risiken minimieren. Und gemeinsam mit Ihnen bewältigen wir im Ernstfall Krisensituationen, um Ihre Marke und Ihre Organisation zu schützen.

Unser Engagement für bewährte Methodiken in Krisensituationen spiegelt sich in unserem einzigartigen Zertifizierungsverfahren für Krisenberater:innen wider - das mit seiner Einführung im Jahr 2013, unserer Meinung nach, das erste Programm seiner Art war.

Die A.R.C.™ Methodologie

Mithilfe unseres erprobten A.R.C.™ Prozesses (Assess – Resolve – Control) managen wir Issues und Krisen. Durch das planvolle und schrittweise Vorgehen in einer brenzligen Situation helfen wir unseren Kund:innen in unterschiedlichsten Kontexten, ihre Organisation zu schützen und die Unternehmensreputation zu wahren oder wiederherzustellen.

ASESS
Einordnung des Sachverhalts, der Begleit-umstände, Einstufung des Bedrohungsgrades und Einleiten der sofort erforderlichen operativen Maßnahmen.

RESOLVE
Bestimmung einer geeigneten Strategie und transparente Einbeziehung aller Beteiligten während des gesamten Prozesses.

CONTROL
Ständige Kommunikation mit allen Beteiligten, Zuhören und Reagieren auf alle Fragen und Anliegen. Wir arbeiten in Echtzeit und über alle traditionellen und digitalen Kanäle. So stellen wir sicher, dass keine fehlerhaften Informationen unwidersprochen bleiben.

UNTERSTÜTZUNG, DA WO SIE SIE BRAUCHEN

A.R.C. PROZESS & SERVICE OFFERING

PHASE	ASSESS	RESOLVE	CONTROL
UNSERE SERVICES	*Audit & Gap-Analysis:* [Review vorhandener Prozesse & -materialien; Identifizierung möglicher Lücken und Schwachstellen] *Crisis Response Materials* [Krisenhandbuch inkl. Prozessen & Templates; Crisis Pocket Guide; Crisis Service Card…] *Ausarbeitung der wichtigsten Krisenszenarien* *Third-Party Education*	*365/24/7 Crisis Support* *Crisis Hotline & Call Center* *Crisis Response Materials* [Q&As, FAQs, Krisenstatements/Holding Statements] *Briefing-Materialien / Leadership Packages*	*Key Learnings Workshop* *Management Summary / Optimierungsvorschläge* *Kontinuierliche Erfolgsmessung & Optimierung*
UNSERE TOOLS	*Risk Radar* *Stakeholder Mapping* *Krisensimulationen* *Media & Crisis Trainings*	*A.R.C Certified Crisis Counselors* *Crisis Monitoring & Dashboard*	*Crisis Response Audit* *Crisis Recovery Plan*
TIMING	2-4 WOCHEN	8-12 WOCHEN	KRISENHOTLINE