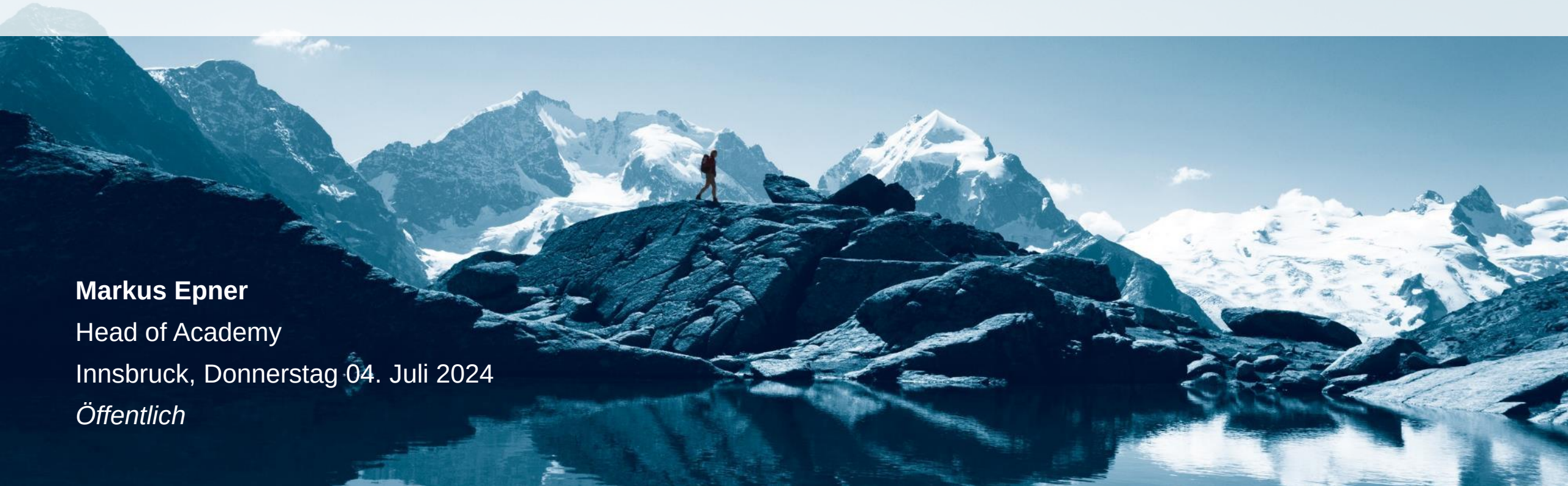
Realistisch trainieren

F24

F24 Cyber-Exit-Game



Markus Epner
Head of Academy
Innsbruck, Donnerstag 04. Juli 2024
Öffentlich

Cyber-Vorfälle*

Entwicklung der Computerkriminalität:

- Bis zum Beginn des nächsten Jahrzehnts wird **erwartet, dass** allein die **Ransomware-Aktivitäten** ihre Opfer **265 Milliarden Dollar pro Jahr kosten werden.**
- Die durchschnittliche Anzahl der Tage, die für die Ausführung eines Auftrags benötigt werden, sinkt von rund 60 Tagen im Jahr 2019 auf vier.
- **Unzureichende Sicherheit** und die **Vermischung** von **persönlichen** und **geschäftlichen Daten** auf mobilen Geräten wie Smartphones, Tablets und Laptops **ermöglichen neue Strategien** für **Cyberkriminelle**.
- Sie zielen nun mit **spezieller Malware** auf mobile Geräte ab, um sich **Fernzugriff zu** verschaffen, Anmeldedaten zu stehlen oder Ransomware einzusetzen.

Wichtigste Risiken für Unternehmen:

1. Datenschutzverletzung: **Verlust** der **Kontrolle** über Ihre **eigenen Daten**
2. Angriffe auf **kritische Infrastrukturen**
3. **Ransomware-Angriffe**
4. Unterbrechung der **digitalen Lieferketten** (Cloud/Dienstleistungsplattformen)

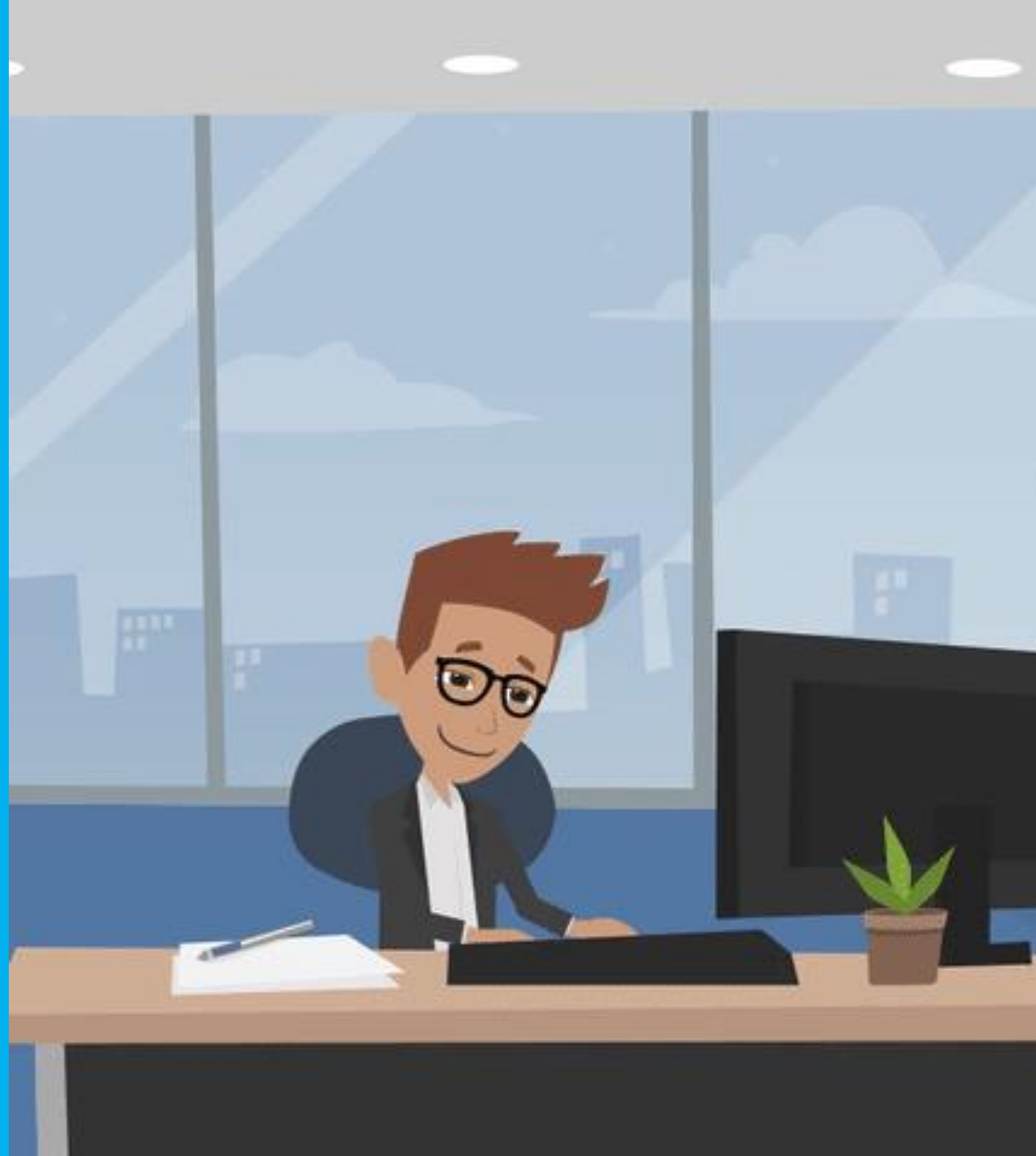
Cyberkriminalität und künstliche Intelligenz:

- Entwicklung eines Marktes für **Ransomware-as-a-Service-Kits** ab **40 $.**
- Mit Hilfe von KI können selbst unerfahrene Personen relativ leicht Ransomware-Angriffe durchführen.

*Allianz Risikobarometer 2024 S.16 - 18

”

Sie arbeiten bei der CRISIX-Gruppe, einem aufstrebenden Maschinen- und Anlagenbauer mit fundierten Kenntnissen in den Bereichen Automatisierung und Digitalisierung. Leider stellen Sie fest, dass Ihr Computer ungewöhnlich langsam hochfährt, und dann erscheint auch noch ein seltsames Pop-up auf Ihrem Desktop. Könnte es sich um einen Ransomware-Angriff handeln?




ALLE IHRE DATEIEN SIND DERZEIT VON DER CONTI-RANSOMWARE VERSCHLÜSSELT.
WENN SIE VERSUCHEN, EINE ZUSÄTZLICHE WIEDERHERSTELLUNGSSOFTWARE ZU VERWENDEN, KÖNNEN DIE DATEIEN BESCHÄDIGT WERDEN ODER VERLOREN GEHEN.
UM SICHERZUSTELLEN, DASS WIR WIRKLICH DATEN WIEDERHERSTELLEN KÖNNEN, BIETEN WIR IHNEN AN, MUSTER ZU ENTSCHLÜSSELN.
KÖNNEN SIE UNS FÜR WEITERE ANWEISUNGEN ÜBER KONTAKTIEREN:
UNSERE WEBSEITE
TOR VERSION:
(SIE SOLLTEN ZUERST DEN TOR-BROWSER HERUNTERLADEN UND INSTALLIEREN HTTPS://TORPROJECT.ORG)
HTTP://CONTIRECJ4HBZMYZUYDYZRVMHOJ2CVF25ZQJ2DWRRQCQ5OAD.ONION/
HTTPS-VERSION :
HTTPS://CONTIRECOVERY.CLICK
SIE SOLLTEN SICH DESSEN BEWUSST SEIN!
NUR FÜR DEN FALL, DASS SIE VERSUCHEN, UNS ZU IGNORIEREN. WIR HABEN IHRE DATEN HERUNTERGELADEN UND SIND BEREIT, SIE AUF UNSERER NACHRICHTEN-WEBSITE ZU VERÖFFENTLICHEN, WENN SIE NICHT ANTWORTEN. ES IST ALSO FÜR BEIDE SEITEN BESSER, WENN SIE UNS SO SCHNELL WIE MÖGLICH KONTAKTIEREN.
ES IST EIN GESCHÄFT!
MacBook
Freitag, 21. Oktober
04:30
FUSION CENTER jetzt
1 Nachricht
PA-Board jetzt
1 Nachricht
IT-Abteilung 1min
1 Nachricht
Ablehnen
Annehmen

Was ist Ihre erste Handlung?

A:
Ich aktiviere unseren BCM-Plan

B:
Ich aktiviere das Krisenmanagementteam

C:
Ich informiere die IT-Abteilung

D:
Ich informiere den CEO

E:
Ich beantworte meine Telefonanrufe und Textnachrichten

Ich aktiviere unseren BCM-Plan

Keine schlechte Idee, ABER bring niemals ein Messer zu einer Schießerei mit!

Sie werden von Kriminellen angegriffen und Ihr gesamtes IT-System ist ausgefallen. Aufgrund der neuesten Gesetzesänderungen müssen Sie die meisten Cyberangriffe innerhalb von 24 Stunden an Ihre nationalen Teams für Computersicherheitsvorfälle melden.

Was wäre also eine bessere Entscheidung?

ZURÜCK

Ich informiere die IT-Abteilung

SORRY! Cybersicherheit kann nicht mehr so sein, dass man zu einem IT-Mitarbeiter sagt: "Okay, wie auch immer, mach du was".

Zwischen 2020 und 2021 haben wir festgestellt, dass Cyberangriffe auf kritische Infrastrukturen weltweit um 45 % und in den EU-Mitgliedstaaten um bis zu 220 % zugenommen haben. Darüber hinaus eröffnete die Umstellung auf Telearbeit während der Pandemie neue Schwachstellen, was dazu führte, dass im Jahr 2020 47 % mehr Menschen auf Phishing-Angriffe hereinfielen.

Und mit der neuen NIS-2-Richtlinie wird das Top-Management in die Pflicht genommen!

Na los! Du kannst es besser!

ZURÜCK

Ich informiere den CEO

Melden macht frei und belastet den Vorgesetzten?

Es besteht ein großer Unterschied zwischen Handeln und Berichten.

Henry Kissinger, der berühmte US-Außenminister, sagte einmal: "Nächste Woche kann es keine Krise geben. Mein Terminkalender ist bereits voll."

Na los! Du kannst es besser!

ZURÜCK

Ich beantworte meine Telefonanrufe und Textnachrichten

WOW!!!!!

Ich dachte, es sei völlig unmöglich, dass jemand diese Antwort wählt.

Natürlich ist Nichtstun auch eine Möglichkeit. In einer Krisensituation ist das meist die schlechteste.

Na los! Du kannst es besser!

ZURÜCK

Krise - Auslöser

- Politisch
- Wirtschaft
- Soziales
- Technologische
- Umwelt
- Rechtliches

Identifizierung einer potenziellen Krisensituation

- Gefährlich, dynamisch, komplex und schnell eskalierend

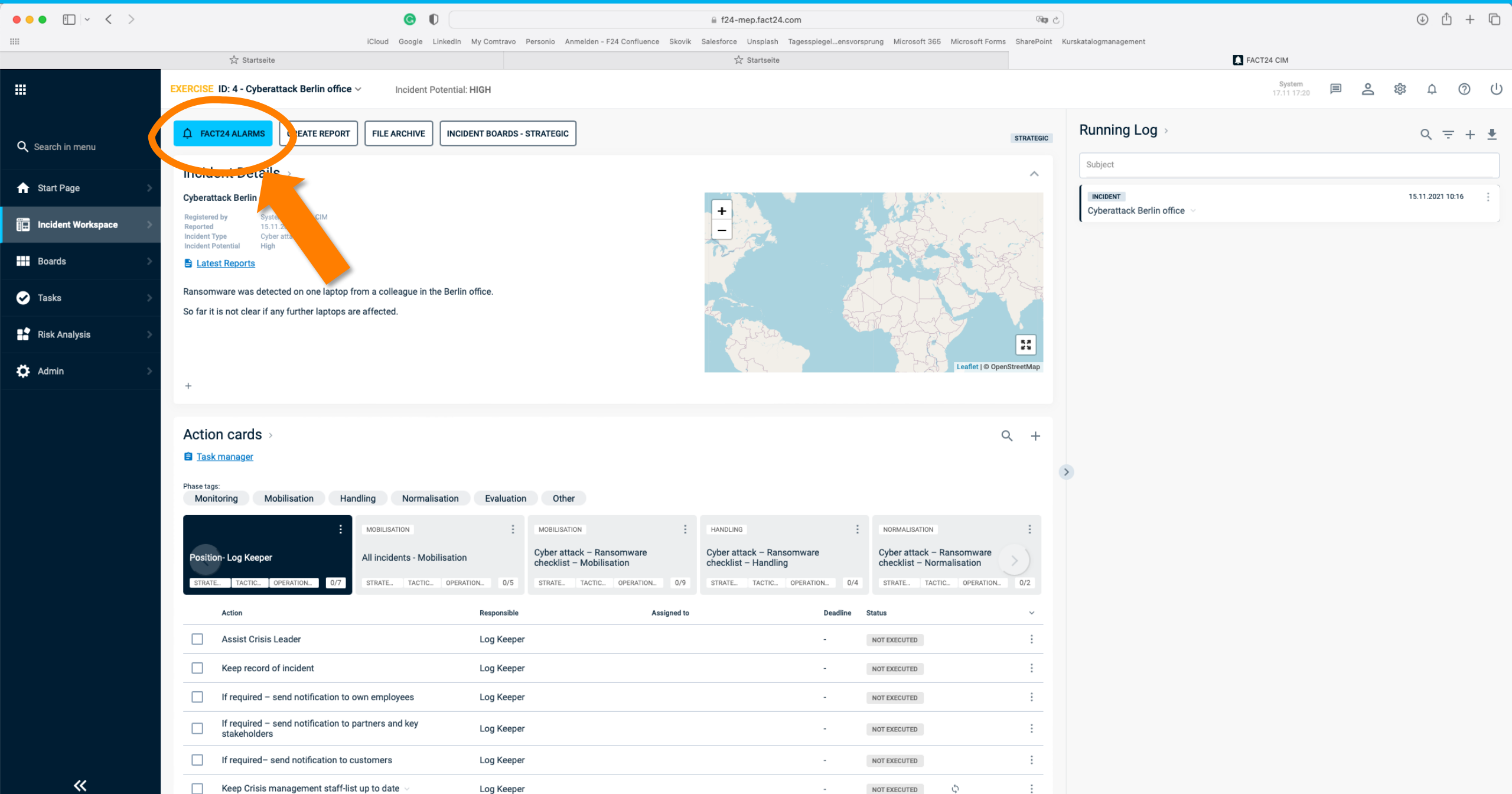
Auswirkungen

- Erfordert sofortige Aufmerksamkeit und Management zum Schutz:
  - Einzelpersonen
  - Umwelt
  - Vermögenswerte
  - Geschäftsbetrieb
  - Ruf und Image

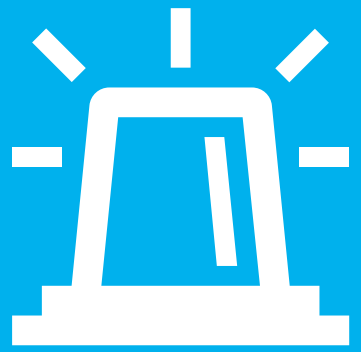
- Kann von der normalen Organisation nicht verwaltet werden

Was sollten Sie tun?

F24



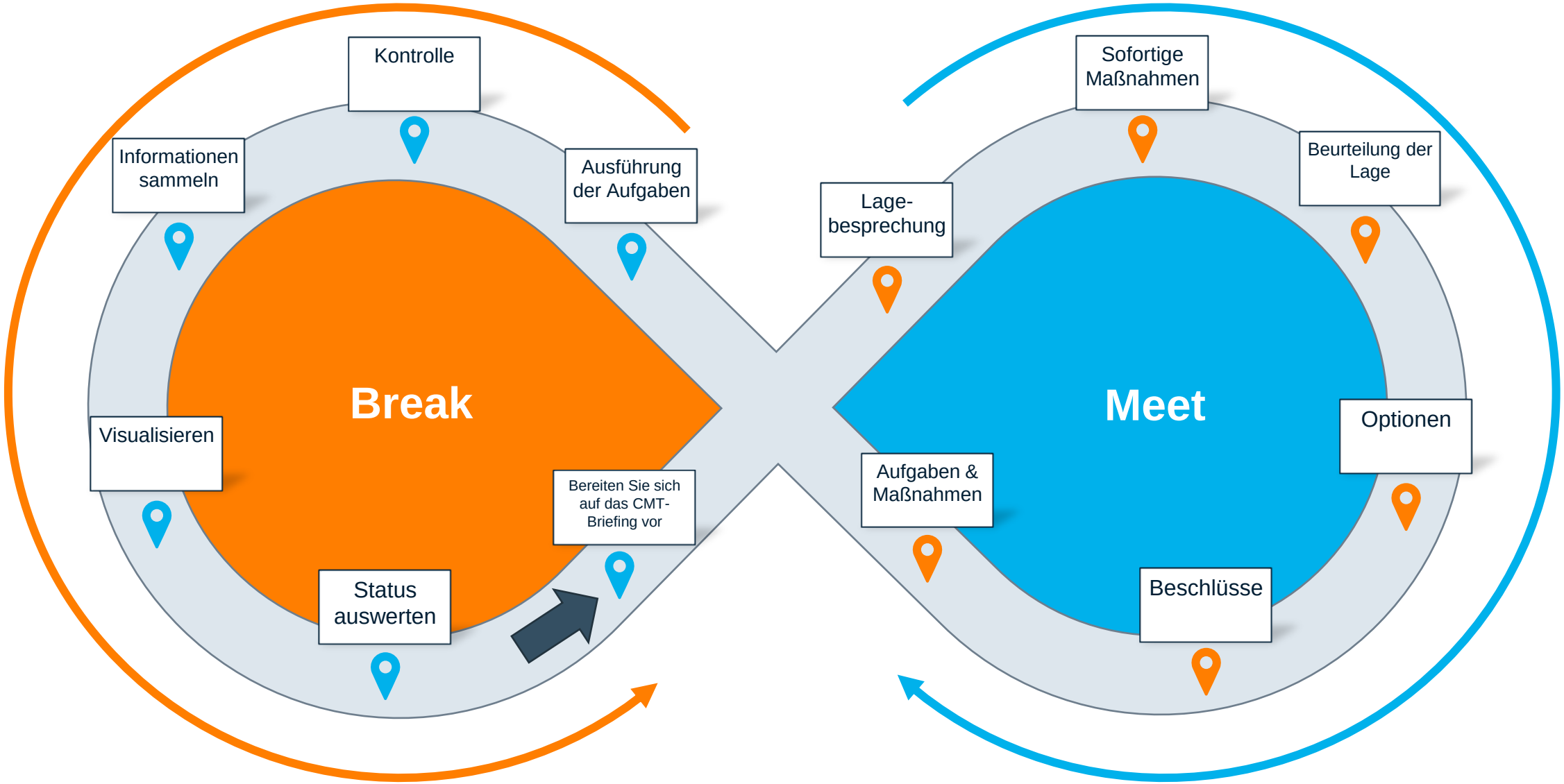
F24



Es hat einen Cyberangriff auf CRISIX gegeben. Sie sind nun Mitglied des aktiven Krisenmanagementteams. Bitte begeben Sie sich in den virtuellen CMT-Raum. Drücken Sie 1, um den Raum zu betreten, drücken Sie 2, um diese Nachricht an Ihren Stellvertreter weiterzuleiten.

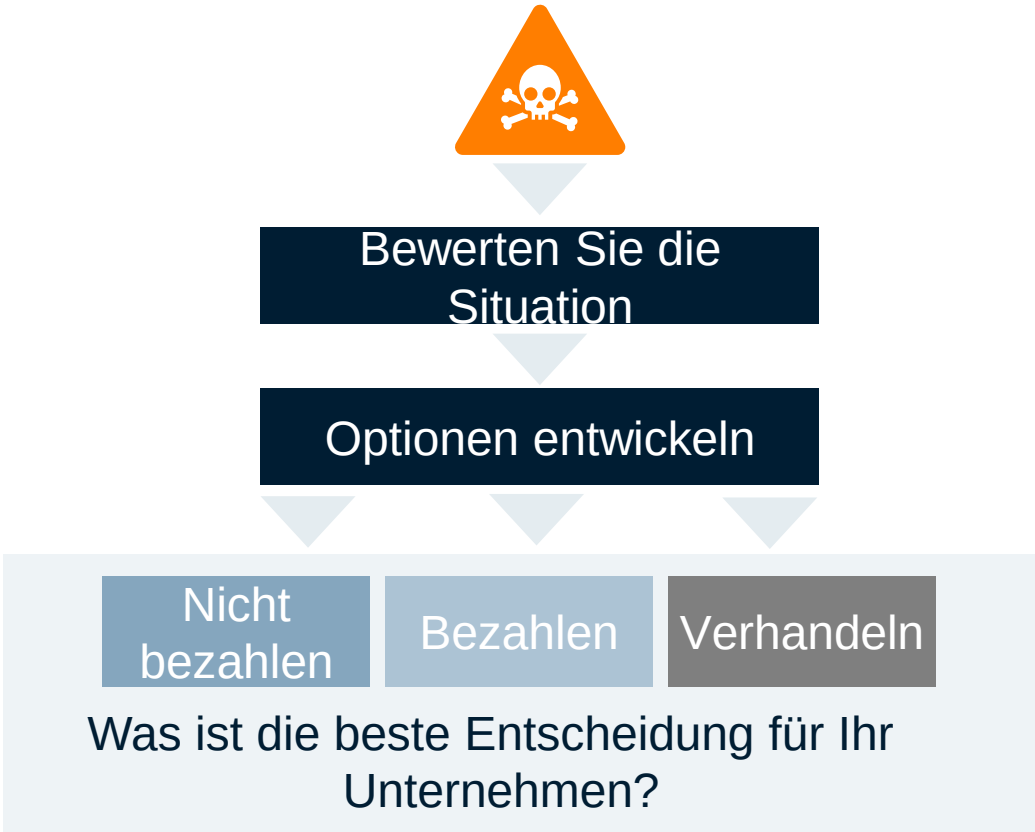
- ALARMMELDUNG

Prozess des Krisenmanagements



“In any moment of decision, the best thing you can do is the right thing, the next best thing is the wrong thing, and the worst thing you can do is nothing.”

- Theodore Roosevelt, 26. Präsident der Vereinigten Staaten



1st CMT-Treffen

Situation: Möglicher Ransomware-Angriff (doppelte Erpressung)

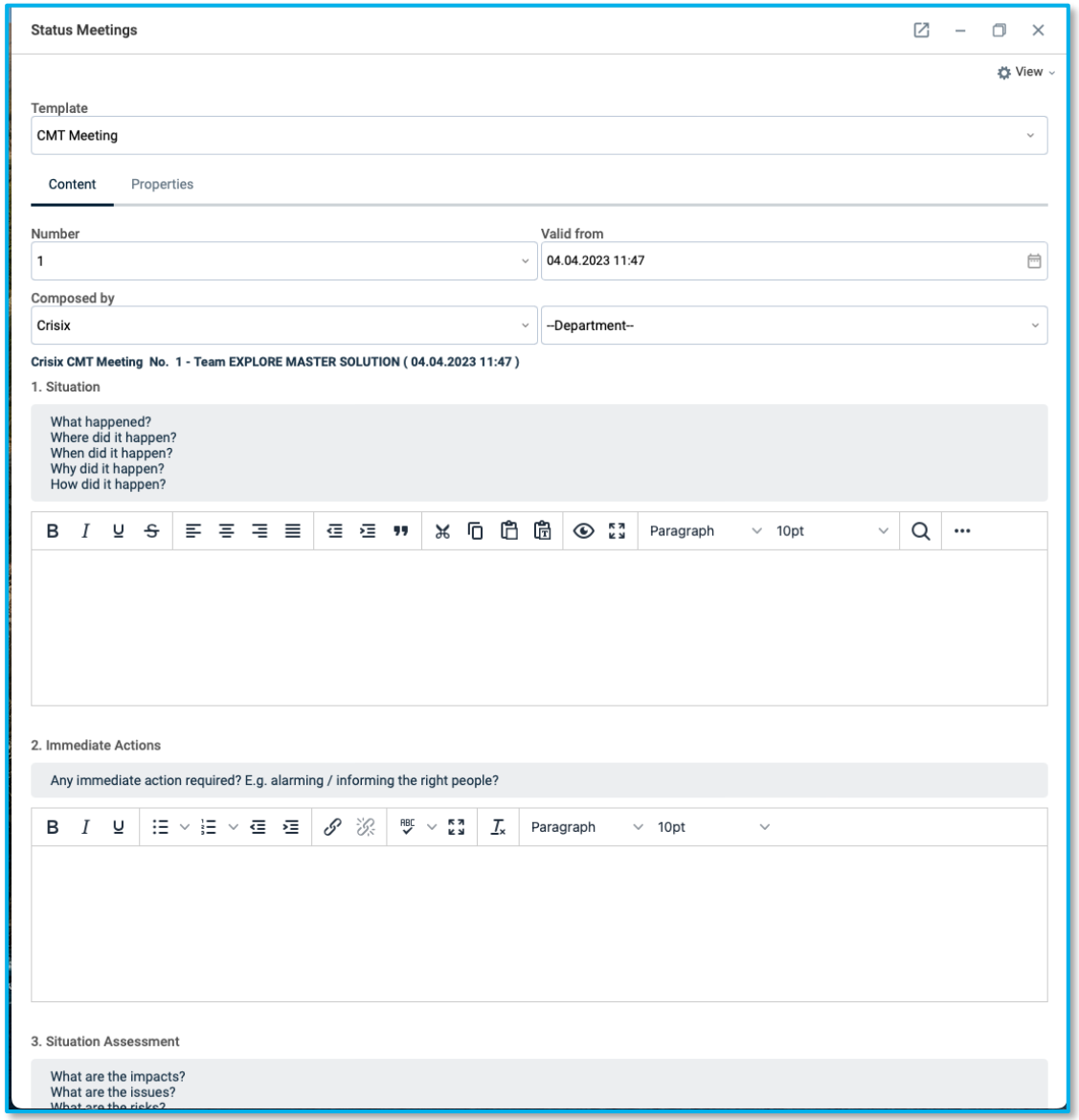
Sofortige Maßnahmen: CIO in das CMT

Beurteilung der Lage: Wiederherstellung von Daten, Reputationssicherung, Management von Interessengruppen,

Optionen: Bezahlen | Verhandeln und Bezahlen | Verhandeln und Wiederherstellen

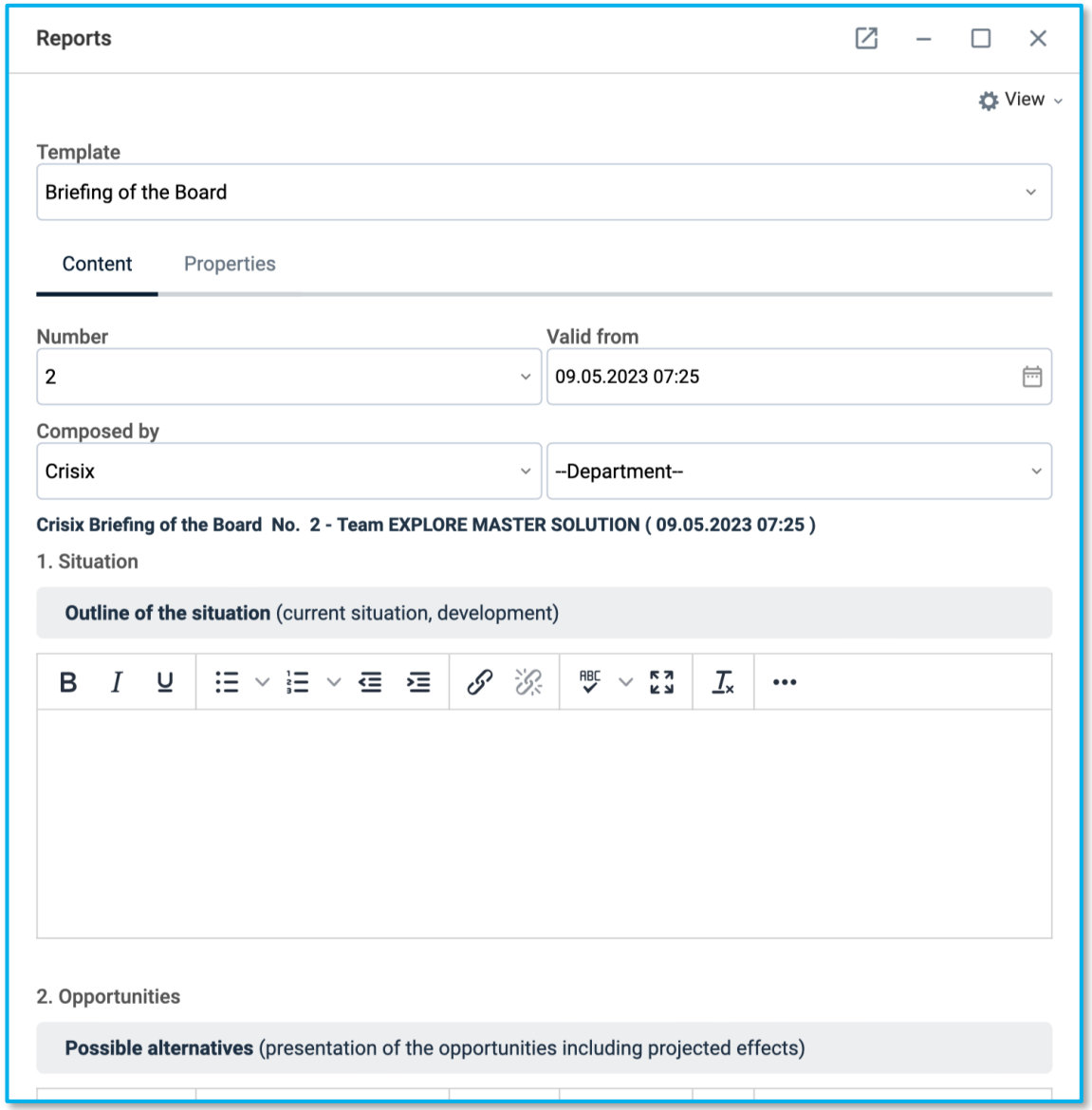
Beschlüsse: Verhandeln und später entscheiden, ob wir zahlen oder zurückgeben

Aufgaben & Maßnahmen: Nachweis der Daten, Überprüfung der Schadenshöhe, Überprüfung der Kosten für die Wiederherstellung



Bericht

Situation:	**Möglicher Ransomware-Angriff (doppelte Erpressung)**
Möglichkeiten:	**Bezahlung | Verhandeln und bezahlen | Verhandeln und wiederherstellen**
Entscheidung:	**Verhandeln und später entscheiden, ob wir zahlen oder zurückgeben**
Gründe für die :	**Schaden vs. Wiederherstellungskosten Entscheidung**
Fazit:	**Zeit kaufen und dann die insgesamt bessere Option wählen.**



Wie gehen Sie mit den Angreifern um?

A:
Wir kontaktieren die Angreifer

B:
Wir überlassen die Verhandlungen der Polizei

C:
Wir verhandeln nicht mit Kriminellen

D:
Solange wir den genauen Schaden nicht kennen, hat es keinen Sinn, zu verhandeln.

Ich überlasse die Verhandlungen der Polizei

Keine schlechte Idee, ABER sie werden nicht für Sie verhandeln!

Die Polizei ist für die Untersuchung der Straftat zuständig. Die Polizei kann weder den Schaden für ihr Unternehmen noch die Bedeutung der verschlüsselten Daten einschätzen.

Was wäre also eine bessere Entscheidung?

ZURÜCK

Wir verhandeln nicht mit Kriminellen

Das zeigt Haltung! Aber man muss sich diese Haltung auch leisten können.

Die Ausfallzeiten für Unternehmen, die von Ransomware betroffen sind, betragen durchschnittlich 21 Tage. Manchmal können sie auch Monate dauern.

Was sagen Ihr Vorstand, der Aufsichtsrat und Ihre Investoren zu dieser höchstwahrscheinlich sehr kostspieligen Entscheidung?

ZURÜCK

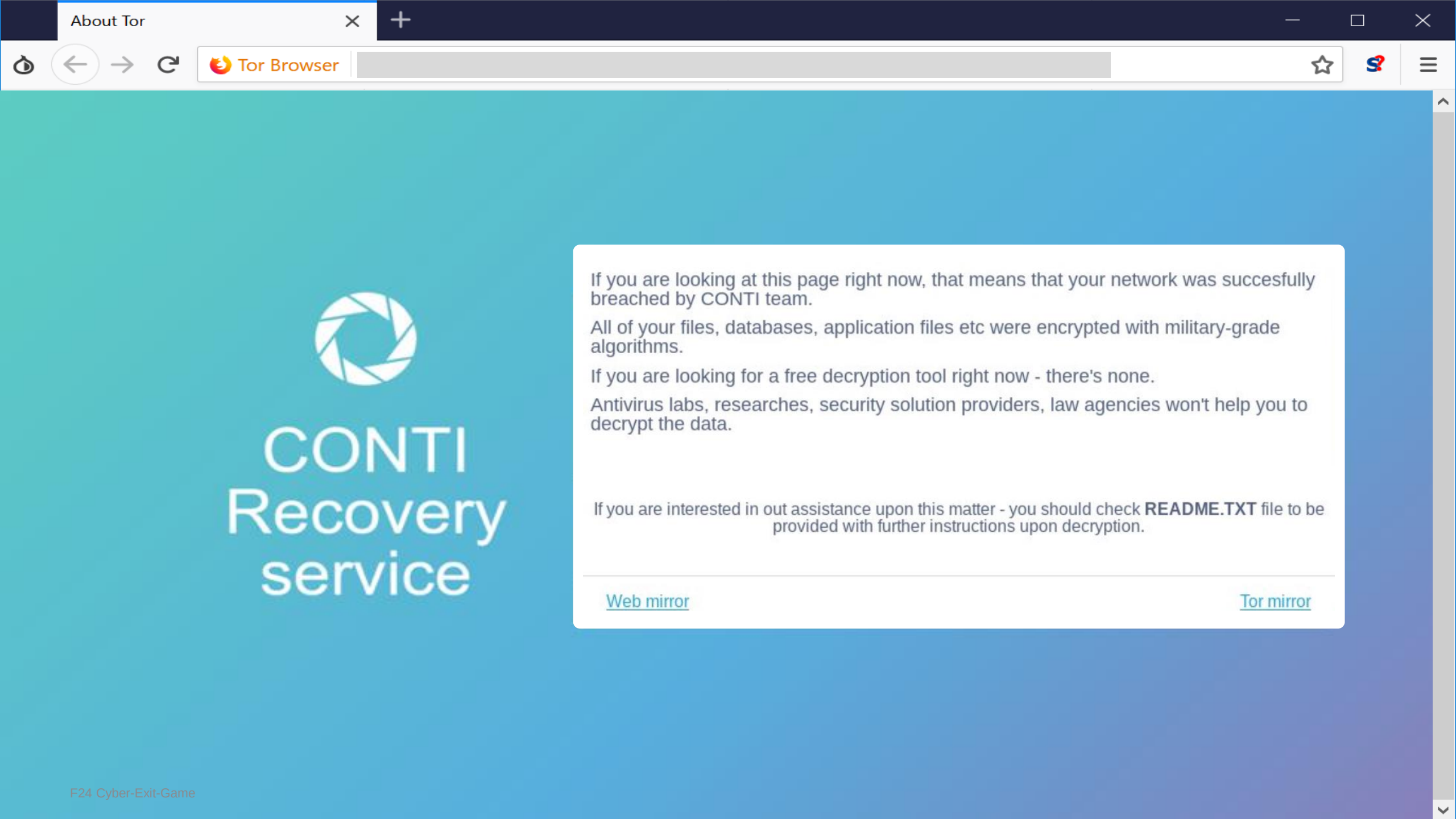
Solange ich den genauen Schaden nicht kenne, hat es keinen Sinn, zu verhandeln.

Eine der wichtigsten Aufgaben im Umgang mit Erpressern ist es, auf Zeit zu spielen, aber dazu muss man kommunizieren.

Wenn Sie nicht mit ihnen sprechen, werden Sie Ihre vertraulichsten Dokumente sehr schnell im Internet finden.

Na los! Du kannst es besser!

ZURÜCK


About Tor
Tor Browser
CONTI
Recovery
service
If you are looking at this page right now, that means that your network was succesfully breached by CONTI team.
All of your files, databases, application files etc were encrypted with military-grade algorithms.
If you are looking for a free decryption tool right now - there's none.
Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.
If you are interested in out assistance upon this matter - you should check README.TXT file to be provided with further instructions upon decryption.
Web mirror
Tor mirror
F24 Cyber-Exit-Game

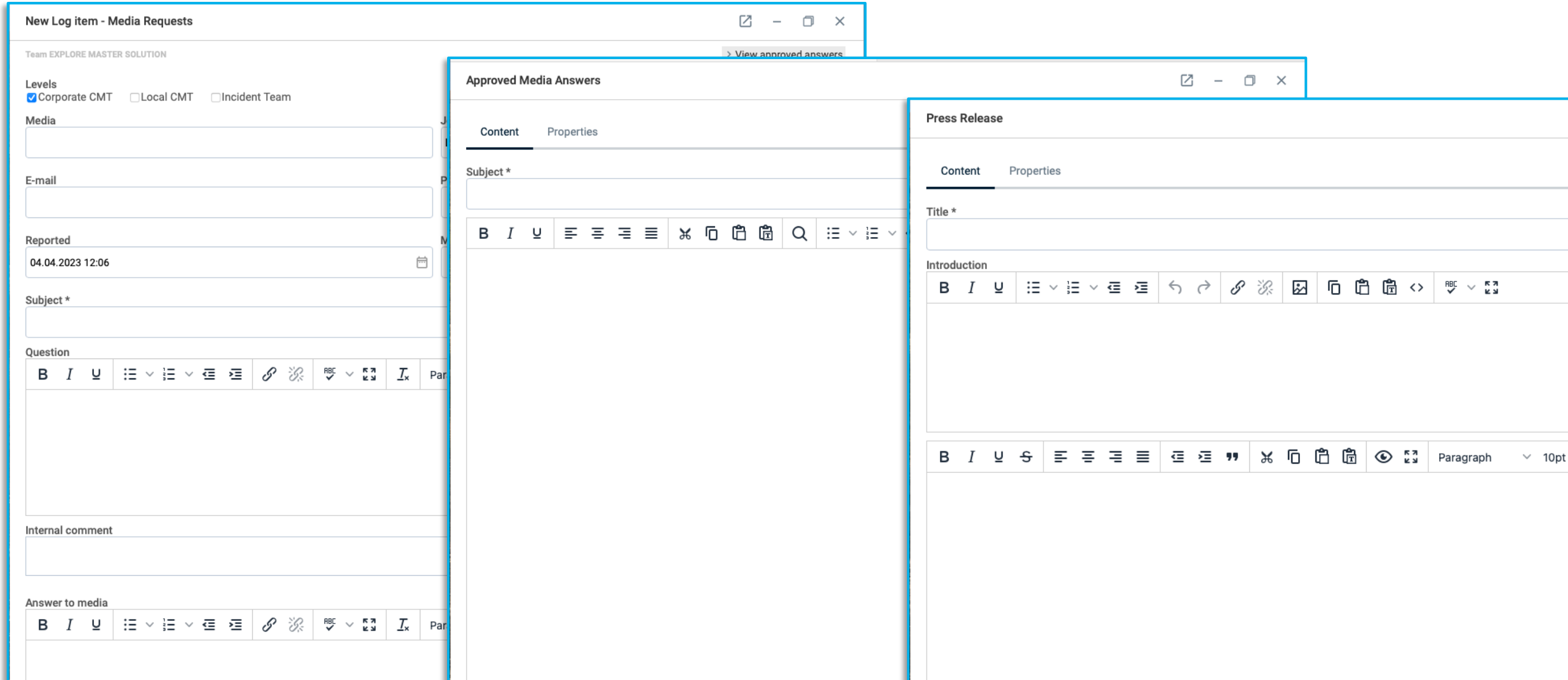
CONTI Bergungsdienst

Hallo zusammen! Hier ist das Conti-Team.
Wie Sie bereits wissen, **sind wir in Ihre Netzwerke eingedrungen**, haben sie erforscht und kritische Schwachstellen gefunden, die es uns ermöglichten, auf Ihre interne Dokumentation zuzugreifen und diese zu exfiltrieren sowie **Ihre Dateiserver, SQL-Server, Subdomänen und lokalen Netzwerke zu verschlüsseln.**
Aufgrund der mangelhaften Sicherheit Ihrer Netzwerke **haben wir Ihre kritischen Informationen mit einem Gesamtvolumen von mehr als 450 GB heruntergeladen.** Zu diesen Informationen gehören persönliche Daten Ihrer Kunden, Mitarbeiter und Lieferanten sowie Ihre Rechts-, Finanz-, Personal-, IT-, Audit- und Compliance-Verzeichnisse (neben anderen Dateien). **Wir haben persönliche Dokumente, Telefonnummern, Kontaktinformationen, konsolidierte Jahresabschlüsse, Gehaltsabrechnungen und Bankauszüge erhalten**.
Zum Glück ist Conti da, um weitere Schäden zu verhindern!
Zunächst können wir Sie mit IT-Unterstützung versorgen, indem wir ein Entschlüsselungs-Tool sowie einen Sicherheitsbericht anbieten, der sich mit den anfänglichen Problemen mit Ihrer Netzwerksicherheit befasst, die zu dieser Situation geführt haben.
Zweitens bieten wir Ihnen Dienstleistungen zur Schadensverhütung an. Zu diesem Zeitpunkt werden alle Ihre Dateien in unserem Blog veröffentlicht und sind für jedermann zugänglich, auch für Kriminelle im Darknet, die Ihre Informationen für ihre eigenen bösen Zwecke missbrauchen wollen, z. B. für Social-Engineering-Angriffe gegen Ihre Kunden und Lieferanten, Spamming und andere böse Aktionen.
Ihre Kunden, Lieferanten, Mitarbeiter und Investoren (Listen sind in Ihren internen Unterlagen verfügbar) werden ebenfalls von uns über die Sicherheitsverletzung informiert. Auf diese Weise können sie wissen, was zu tun ist, da ihre privaten Daten öffentlich werden.
Es versteht sich von selbst, dass diese Verletzung des Datenschutzes zu langfristigen rechtlichen, regulatorischen, finanziellen und rufschädigenden Schäden führen wird, einschließlich verlorener Verträge und Sammelklagen von Personen, deren Daten offengelegt wurden. Als Teil unserer Vereinbarung bieten wir jedoch eine Lösung an, um dies zu verhindern!
Wir werden Ihnen zunächst einen Dateibaum zur Verfügung stellen, um zu zeigen, welche Dateien wir aus Ihrem Netzwerk heruntergeladen haben. Dann können Sie bestimmte Dateinamen aus dieser Liste auswählen, und wir stellen Ihnen diese Dateien zur Verfügung, um zu beweisen, dass wir sie haben. Dann übertragen wir alle Dateien, die wir haben, an Sie zurück und löschen sie von all unseren Servern, um sicherzustellen, dass nur Sie Zugang zu ihnen haben. Auf diese Weise werden alle oben genannten Risiken vermieden!
Der Preis für alle unsere Dienstleistungen beträgt 2.000.000 USD.
Da wir diese Frage schon einmal erhalten haben, möchten wir sie vorsorglich klären:
Nein, es gibt keine Möglichkeit, dass wir unsere Versprechen nicht erfüllen, nachdem Sie bezahlt haben. Um es einfach auszudrücken: Die Wahrscheinlichkeit, dass die Hölle gefriert, ist größer, als dass wir unsere Kunden in die Irre führen. Wir sind die elitärste Gruppe in diesem Markt, und unser Ruf ist die absolute Grundlage unseres Geschäfts, und wir werden niemals unsere vertraglichen Verpflichtungen brechen.
Bitte lassen Sie mich wissen, wenn Sie weitere Fragen haben.

Hallo Conti-Team,
Wir haben Ihre Forderungen erhalten und erörtern derzeit unsere Möglichkeiten. Wir werden Ihnen so schnell wie möglich Bericht erstatten. Wir sind bereit, Sie zu bezahlen.

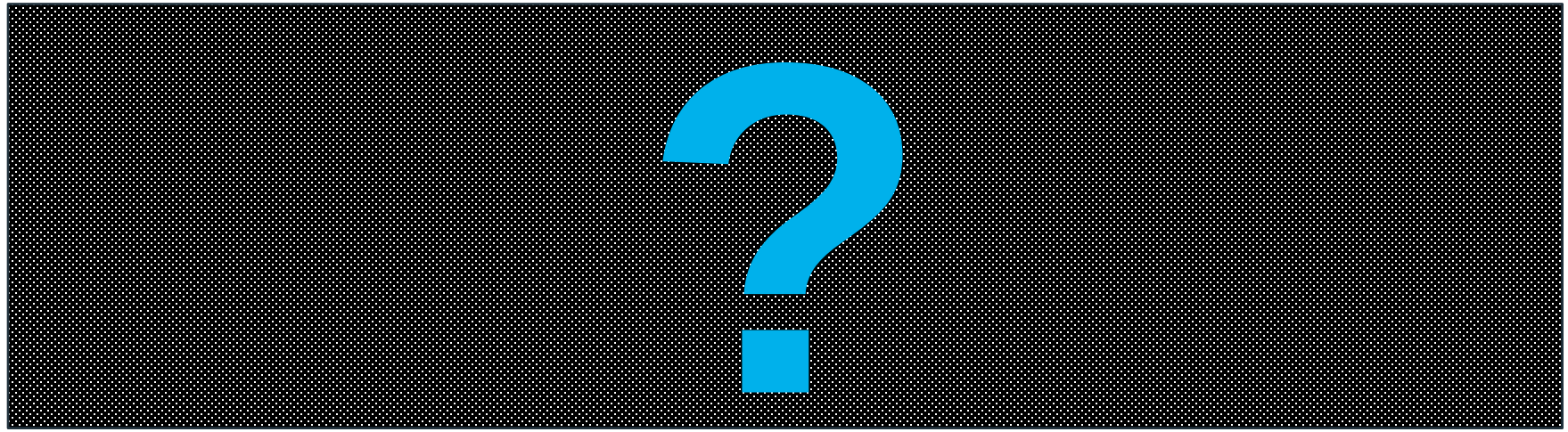
22

Verwalten Sie Ihre Medienanfragen, Medienantworten und Pressemitteilungen in FACT24 CIM



CONTI Bergungsdienst

Hallo Conti-Team,
Wir haben Ihre Forderungen erhalten und erörtern derzeit unsere Möglichkeiten. Wir werden Ihnen so schnell wie möglich Bericht erstatten. Wir sind bereit, Sie zu bezahlen.



CONTI Bergungsdienst

Hallo Conti-Team,
Wir haben Ihre Forderungen erhalten und erörtern derzeit unsere Möglichkeiten. Wir werden Ihnen so schnell wie möglich Bericht erstatten. Wir sind bereit, Sie zu bezahlen.

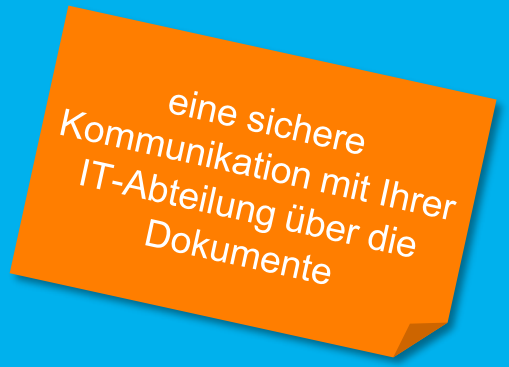
Können Sie mir bitte den Datennachweis übermitteln.

Hier sind einige Beispiele:
Hier herunterladen...
Kennwort: 7Jhgd)nndu§iduhAfs$fevNfjd)m

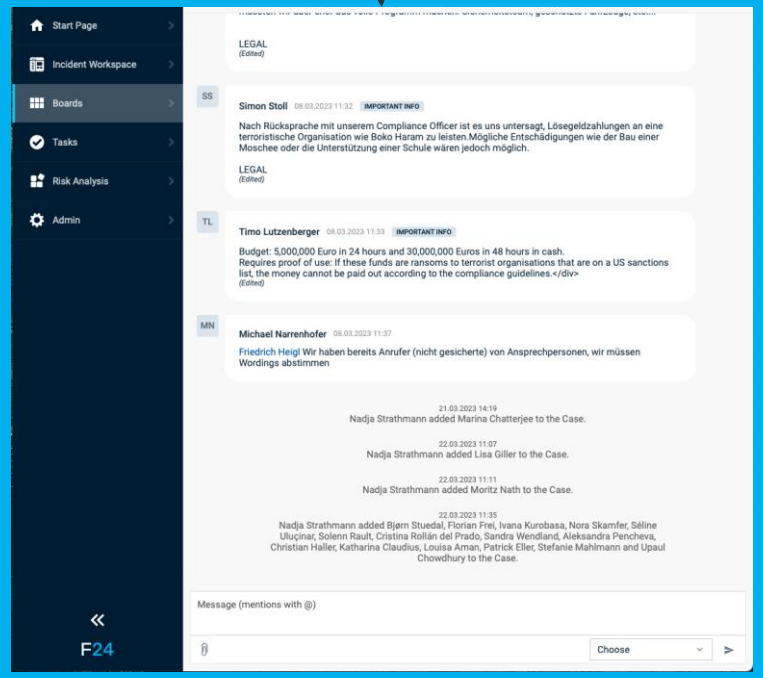
Vielen Dank für den Nachweis. Wir prüfen die Unterlagen und werden uns in Kürze wieder bei Ihnen melden.

Verschwenden Sie nicht Ihre Zeit. Die Zeit läuft.

INFORMATIONS-AUSTAUSCH



Incident Potential:
HIGH



Reports

View

Template

Situation Report

Content | Properties

Number

1

Situation Report No. 1 - Team EXPLORE MASTER SOLUTION

1. Situation summary

Describe the situation and the developments briefly and precisely.

2. Risks and Impact

What are the main risks and there impact

CONTI Bergungsdienst

Hallo Conti-Team,
Wir haben Ihre Forderungen erhalten und erörtern derzeit unsere Möglichkeiten. Wir werden Ihnen so schnell wie möglich Bericht erstatten. Wir sind bereit, Sie zu bezahlen.

Können Sie mir bitte den Datennachweis übermitteln.

Hier sind einige Beispiele:
Hier herunterladen...
Kennwort: 7Jhgd)nndu§iduhAfs$fevNfjd)m

Vielen Dank für den Nachweis. Wir prüfen die Unterlagen und werden uns in Kürze wieder bei Ihnen melden.

Verschwenden Sie nicht Ihre Zeit. Die Zeit läuft.

Unsere Einnahmen sind zwar hoch, aber leider können wir Ihre Nachfrage nicht befriedigen, denn wir brauchen das Geld für die Patienten und die Bezahlung unserer Mitarbeiter. Wir müssen herausfinden, wie wir das Geld aufbringen können. Können wir bitte mehr Zeit haben?

Nach Rücksprache mit meinem Chef kann ich Ihnen zwei zusätzliche Tage geben. Aber das ist eine endgültige Verlängerung, mehr können wir nicht tun.

Wir werden in Kürze auf Sie zurückkommen.

Wir haben keinen rechtzeitigen Zugang zu so viel Geld. Unsere Finanzen sind nicht so strukturiert. Wir versuchen unser Bestes, aber dieser Betrag ist definitiv nicht möglich.

Wir werden den Preis auf 1,5 Mio. senken, aber das ist endgültig. Die Registerkarte "Häufig gestellte Fragen" ist ein Beispiel für das Wissen, das wir über Sie haben. Dies sollte Ihnen helfen, das Geld zu finden. Seien Sie kein Narr!

Wie lautet Ihre nächste Antwort?

CONTI Bergungsdienst

Wir sind bereit, Ihnen 954.500 Dollar zu zahlen. Aber mehr ist im Moment nicht möglich.

Wir sind bereit, Ihnen 800.000 Dollar zu zahlen. Aber mehr ist im Moment nicht möglich.

Nachdem wir unsere Gewinne für das nächste Jahr überprüft haben, können wir Ihnen 1.000.000 $ anbieten.

WIE MAN MIT EINEM HACKER VERHANDELT

F24

CONTI Bergungsdienst

Hallo Conti-Team,
Wir haben Ihre Forderungen erhalten und erörtern derzeit unsere Möglichkeiten. Wir werden Ihnen so schnell wie möglich Bericht erstatten. Wir sind bereit, Sie zu bezahlen.

Können Sie mir bitte den Datennachweis übermitteln.

Hier sind einige Beispiele:
Hier herunterladen...
Kennwort: 7Jhgd)nndu§iduhAfs$fevNfjd)m

Vielen Dank für den Nachweis. Wir prüfen die Unterlagen und werden uns in Kürze wieder bei Ihnen melden.

Verschwenden Sie nicht Ihre Zeit. Die Zeit läuft.

Unsere Einnahmen sind zwar hoch, aber leider können wir Ihre Nachfrage nicht befriedigen, denn wir brauchen das Geld für die Patienten und die Bezahlung unserer Mitarbeiter. Wir müssen herausfinden, wie wir das Geld aufbringen können. Können wir bitte mehr Zeit haben?

Nach Rücksprache mit meinem Chef kann ich Ihnen zwei zusätzliche Tage geben. Aber das ist eine endgültige Verlängerung, mehr können wir nicht tun.

Wir werden in Kürze auf Sie zurückkommen

Wir haben keinen rechtzeitigen Zugang zu so viel Geld. Unsere Finanzen sind nicht so strukturiert. Wir versuchen unser Bestes, aber dieser Betrag ist definitiv nicht möglich.

Wir werden den Preis auf 1,5 Mio. senken, aber das ist endgültig. Die Registerkarte "Häufig gestellte Fragen" ist ein Beispiel für das Wissen, das wir über Sie haben. Dies sollte Ihnen helfen, das Geld zu finden. Seien Sie kein Narr!

Wir sind bereit, Ihnen 954.500 Dollar zu zahlen. Aber mehr ist im Moment nicht möglich.

CONTI Bergungsdienst

Wir werden in Kürze auf Sie

Wir haben keinen rechtzeitigen Zugang zu so viel Geld. Unsere Finanzen sind nicht so strukturiert. Wir versuchen unser Bestes, aber dieser Betrag ist

Wir werden den Preis auf 1,5 Mio. senken, aber das ist endgültig. Die Registerkarte "Häufig gestellte Fragen" ist ein Beispiel für das Wissen, das wir über Sie haben. Dies sollte Ihnen helfen, das Geld zu finden. Seien Sie kein Narr!

Wir sind bereit, Ihnen 954.500 Dollar zu zahlen. Aber mehr ist im Moment nicht möglich

Ich habe mich bei meinen Chefs erkundigt, und unser letzter Preis beträgt 1,1 Mio. Euro. Bezahlen Sie jetzt oder wir beginnen undicht.

Wir werden jetzt zahlen

Ist dies das Ende?

Nein!

CONTI Bergungsdienst

Hallo CONTI-Team,
Wie es zwischen Geschäftsleuten üblich ist, sollten wir schließlich einen Vertrag aufsetzen, auf den sich beide Parteien geeinigt haben.
Vertrag
Zwischen CRISIX AG und Conti Team (im Folgenden Conti)
Bedingungen und Konditionen
Conti und Montafy einigten sich am 16.11.2022 auf die folgenden Bedingungen:

1) Conti wird Montafy einen detaillierten schriftlichen IT-Sicherheitsbericht zukommen lassen, aus dem hervorgeht, wann und wie es möglich war, in das IT-Sicherheitssystem von Montafy einzudringen, wie die Server infiltriert wurden und welche Daten genau heruntergeladen wurden. Der Bericht wird von Conti direkt nach Zahlungseingang weitergeleitet.
2) Conti bestätigt hiermit, dass die kompletten Daten von Montafy nicht kopiert worden sind. Die heruntergeladenen Dateien werden an Montafy ausgehändigt. Der Link zur Cloud wird von Conti direkt nach Zahlungseingang weitergeleitet.
3) Conti bestätigt hiermit, dass die Dateien weder in der Vergangenheit noch in der Gegenwart oder in der Zukunft an ein anderes Unternehmen oder einen Kunden von Conti verkauft wurden.
4) Conti bestätigt hiermit, dass die Dateien weder in der Vergangenheit noch in der Gegenwart veröffentlicht wurden oder in Zukunft veröffentlicht werden.
5) Conti oder jede Partei, die Zugang zu diesen Daten hat, garantiert für die oben genannten Dienstleistungen und Garantien eine Zahlung von 1.100.000 USD. Die Zahlung wird in Bitcoin übertragen werden.

CMT CRISIX, München
Im Namen des Conti-Teams.

Operator Kay, der im Namen des Conti-Teams spricht, bestätigt alle oben genannten Punkte der Vereinbarung zwischen dem CMT von CRISIX und dem Conti-Team. Auch wollen wir den Zeitrahmen für die Zahlung. 1.100.000 USD in Bitcoin müssen an die Adresse bc1qcrqqt3gv4wwpvnrptgzw8en2ej3k3927nmw9zt innerhalb von 48 Stunden nach dieser Erklärung überwiesen werden.

CONTI Bergungsdienst

Hier sind Ihre Daten:
Mega.nz
wgzmepox@pokemail.net
hylpnlius65@45fGha!

Der Dekriptor wird jetzt vorbereitet.

03aovna0r9ßnkenöf09JHIP`98jölan_j7ejdndkeinJGTV%DniunZVV_decryptor.exe (108kB)

Entschlüssler:

1) Starten Sie das Entschlüsselungsprogramm mit Administratorrechten
2) Warten Sie, bis das Entschlüsselungsfenster geschlossen ist.
3) Wenn eine der Dateien die Endung nicht wieder in die ursprüngliche Endung geändert hat, wiederholen Sie 1 und 2.

Wir sind über eine E-Mail-Kompromittierung in Ihr Netzwerk eingedrungen. Geben Sie also zunächst allen Ihren Mitarbeitern strenge Anweisungen zu den Sicherheitsmaßnahmen.
Grundlegende Empfehlungen zum Netzwerk:

1. bessere Maßnahmen zur Filterung von E-Mails einführen
2. bessere Passwortrichtlinien einzuführen.
3. einige besondere Angriffe wie Pass-the-Hash und Pass-the-Ticket zu blockieren.
4. Aktualisieren Sie alle Ihre internen Systeme auf die neuesten Versionen.
5. Überprüfen Sie die Netzwerksegmentierung und achten Sie auf die Anschaffung von Hardware-Firewalls mit Filterungsrichtlinien.
6. Blockieren Sie Kerberoasting-Angriffe.
7. Durchführung vollständiger Penetrationstests, sowohl extern als auch intern.
8. Einführung besserer AV/EDR-Systeme.
9. Überprüfen Sie die Gruppenrichtlinien, entfernen Sie Domänen- und lokale Administratorrechte für einige Benutzer.
10. Implementierung besserer DLP-Software-Systeme.

BOARD UPDATE

SIE HABEN DIE VERHANDLUNG ABGESCHLOSSEN UND DIE DATEN SIND ENTSCHLÜSSELT. DAS GREMIUM MÖCHTE EINE AUSFÜHRLICHE ANALYSE DER EREIGNISSE UND WIE SIE DIESE SITUATION IN ZUKUNFT VERMEIDEN WERDEN.

SIE HABEN DEN ANGREIFERN 1,1 MIO. EURO BEZAHLT

SIE HABEN WAHRSCHEINLICH 50 % WENIGER BEZAHLT ALS VERGLEICHBARE UNTERNEHMEN.

Herzlichen Glückwunsch

SIE HABEN DIE KRISE GELÖST UND DIE DATEN WIEDER ENTSCHLÜSSELT.

IHRE MITARBEITER UND DIE ÖFFENTLICHKEIT HABEN VERTRAUEN IN IHRE REIBUNGSLOSE KOMMUNIKATION.

IHRE VORSTANDSMITGLIEDER SIND ZUFRIEDEN DAMIT, WIE SIE DIE SITUATION GEHANDHABT HABEN.

F24