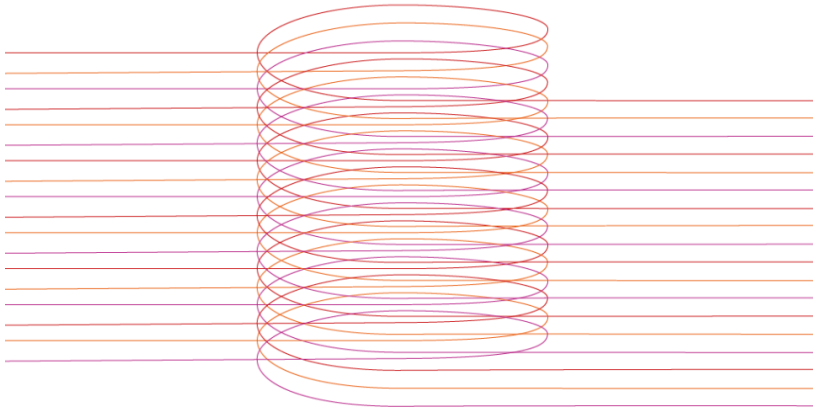
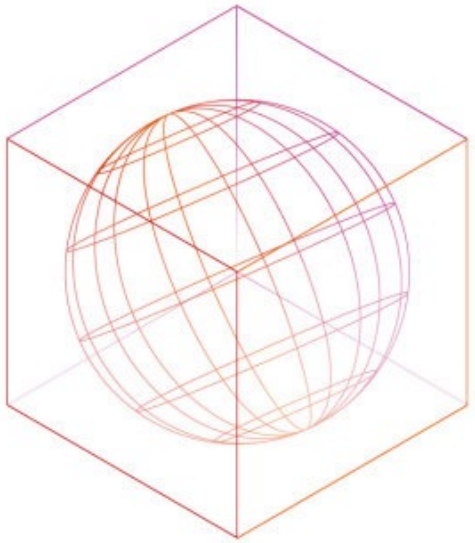




Digitale Sprechstunde

Ransomware - eine Bedrohung für digitalisierte Unternehmen

Silvana Rößler – Leiterin Bereich Security Incident Response, networker, solutions GmbH

Aus den Medien 2021 - 2022

Fuldaer Zeitung

FULDA KINZIGTAL HÜNFELDER LAND VOGELSBERG PANORAMA SPORT HESSEN MEHR

Veröffentlicht am: 15.05.2021 - 21:02

LEERE REGALE, LANGE SCHLANGEN

Alle Filialen nach Hacker-Attacke betroffen: Die Folgen beim Lebensmittelhändler Tegut in Fulda sind extrem

von Volker Nies

Cyber-Kriminalität

Hackerangriff auf Versicherungskonzern AXA in Asien

18. Mai 2021

Cyber-Erpresser: Hacker legten einen Fleischgiganten lahm

Der größte Fleischverarbeiter der Welt, die brasilianische Firma JBS, ist Opfer eines Cyberangriffs geworden. Dieser hat zum Stillstand von Produktionsanlagen in den USA, Kanada und Australien, geführt.

23. Juni 2021

Frankfurter Allgemeine | 15.05.2021 - Aktualisiert: 15.05.2021, 17:41 Uhr
https://www.faz.net/-ikh-abq1h

Ransomware-Attacke

Irland zahlt Hackern kein Lösegeld

Die irische Regierung wird nicht auf Forderungen von Hackern eingehen, die am Freitag den nationalen Gesundheitsdienst angegriffen hatten. Noch sind die Systeme nicht wieder vollständig hochgefahren.

Von PHILIP PLICKERT, LONDON

HACKER GREIFEN ENERGY HAMBURG AN

11.05.2021

OBERSCHÖNEGG

Cyberangriff: Hacker wollten Molkerei Ehrmann erpressen

Bericht zu Cyberangriff

Pipeline-Betreiber soll Hackern fünf Millionen Dollar Lösegeld gezahlt haben

Nach einem Hackerangriff wird die größte Kraftstoff-Pipeline der USA wieder hochgefahren. Die Betreiberfirma hat den Tätern zuvor offenbar Millionen gezahlt haben. Laut Behörden führt die Spur nach Russland.

13.05.2021, 18.15 Uhr

HACKER-LEAK

16.05.2022

Stadt informiert Hunderte Bürger über Daten im Darknet

Cyberangriff auf Accenture: Hacker veröffentlichen Daten von IT-Berater und kündigen weitere Leaks an

0 Veröffentlicht am: 14.05.2021 - 07:01

News > Software & Infrastruktur > Microsoft Exchange: Sicherheitslücke noch bei jedem 2. Server nicht gepatcht

News

Microsoft Exchange: Sicherheitslücke noch bei jedem 2. Server nicht gepatcht

21.04.2022, 11:16 Uhr

Donau-Stadtwerke nach Hacker-Angriff vor wochenlanger Aufgabe

LÖSEGELD GEFORDERT

Möbelhaus Sommerlad in Gießen wird erpresst

Stand: 10.05.2022 09:53 Uhr

Das Oldenburger Bauunternehmen Ludwig Freytag ist Opfer eines Cyber-Angriffs geworden, mittlerweile laufen die Bauarbeiten wieder. Noch ist unklar, wer hinter der Attacke steckt.

Traktorenhersteller im Allgäu

Hacker legt Produktion bei Fendt lahm

9. Mai 2022, 14:07 Uhr

Ausgespäht

Computer-Zugriff: Hacker buchen 9999 Euro ab

Redaktion 14.05.2022 - 11:24 Uhr

WIRTSCHAFT

Hacker attackieren Europa-Geschäft von Toshiba

Nach dem schweren Hacker-Angriff auf die Colonial Pipeline in den USA wurde jetzt der japanische Technologiekonzern Toshiba ebenfalls Ziel einer Attacke.

Behörden-Seiten nicht erreichbar

Bundesregierung bestätigt Hacker-Angriffe

Stand: 09.05.2022 15:44 Uhr

Die Bundesregierung hat eine Serie von Cyberangriffen auf deutsche Behörden und Ministerien bestätigt. Es sollen aber keine Schäden entstanden oder Daten abgeflossen sein. Eine russische Gruppe hatte sich zu den Taten bekannt.

23.06.2021, 22:00

Regale bleiben leer – Hacker-Angriff legt Molkerei lahm

Digitale Sprechstunde der Akademie für wissenschaftliche Weiterbildung
Ransomware - eine Bedrohung für digitalisierte Unternehmen

Silvana Rößler – Leiterin Bereich Security Incident Response, networker, solutions GmbH

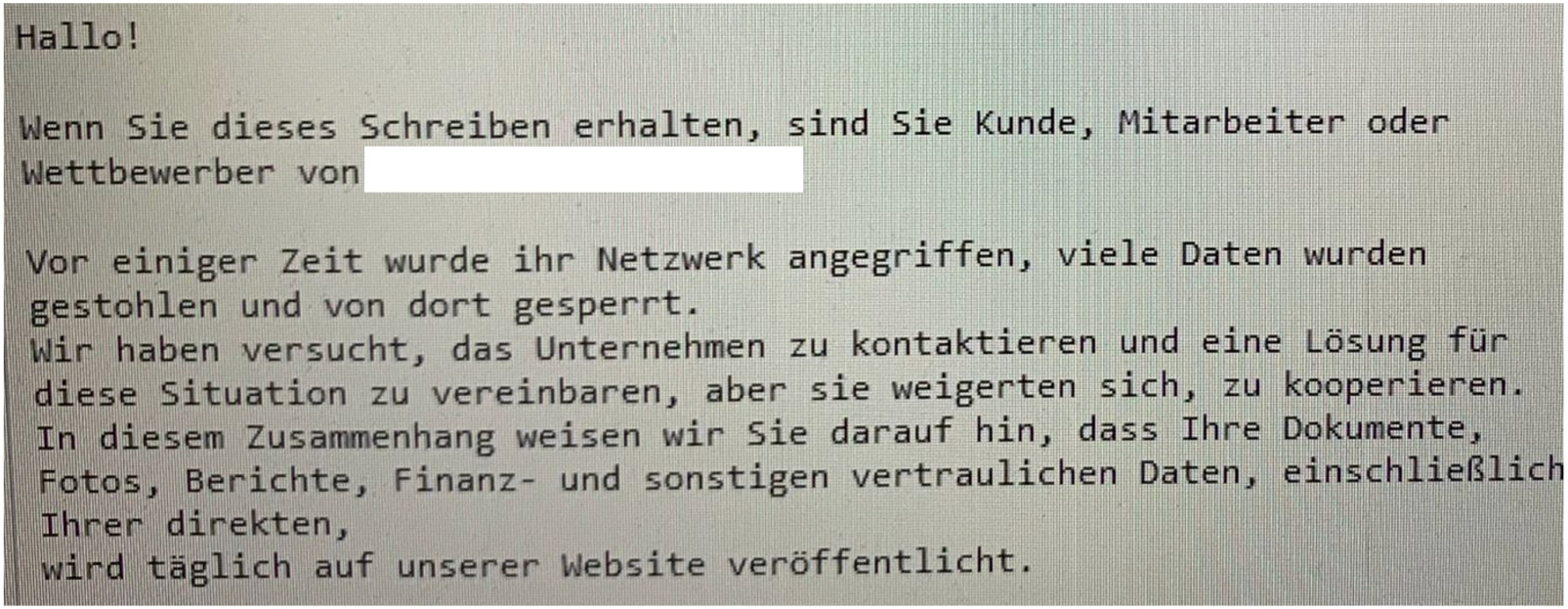
Technology
Arts Sciences
TH Köln

```
==============================

     __,---.
    /__|o\  )
     `-\ / /   MACAW
       ,) (,   LOCKER
      //   \\
     {(     )}

=======""===""===============

Data in your network has been stolen and encrypted.


To get your data back visit:

https://macawfmv54zp5nuugykaxvgqf5wjqg2bousmodtzjvms2w32shbp5qad.onion/xxxxxxxxxxx

Decryption ID: xxxxxxx
```

Doppelte Erpressung

- 1. Stufe
  Erpressung durch Datenverschlüsselung
- 2.Stufe
  Androhung und spätere Veröffentlichung von (sensiblen) Unternehmensinformationen

Dreifache Erpressung


Hallo!

Wenn Sie dieses Schreiben erhalten, sind Sie Kunde, Mitarbeiter oder Wettbewerber von

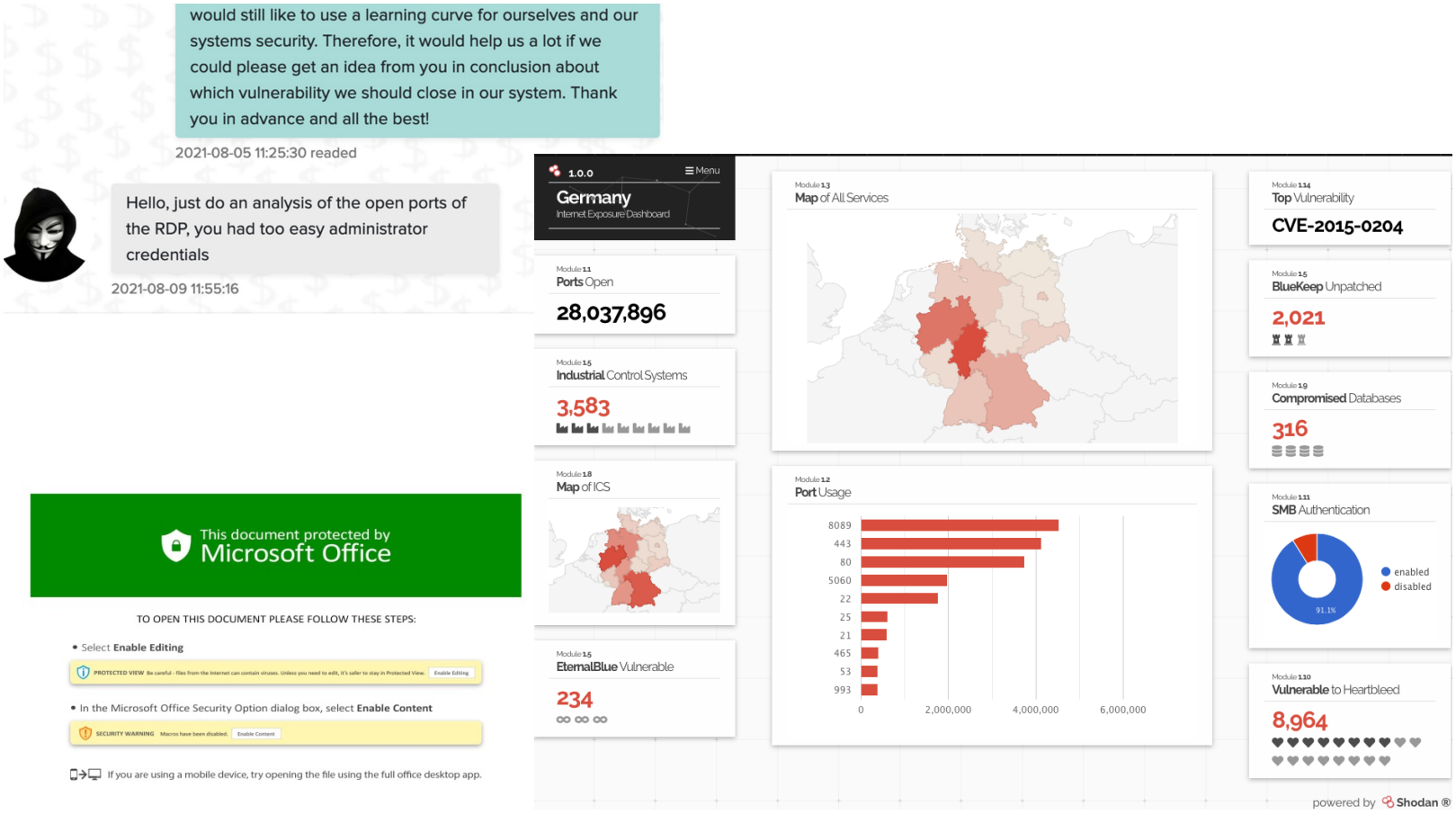
Vor einiger Zeit wurde ihr Netzwerk angegriffen, viele Daten wurden gestohlen und von dort gesperrt.
Wir haben versucht, das Unternehmen zu kontaktieren und eine Lösung für diese Situation zu vereinbaren, aber sie weigerten sich, zu kooperieren.
In diesem Zusammenhang weisen wir Sie darauf hin, dass Ihre Dokumente, Fotos, Berichte, Finanz- und sonstigen vertraulichen Daten, einschließlich Ihrer direkten,
wird täglich auf unserer Website veröffentlicht.

Angriffe

Schwachstellen, Phishing und Co.

Silvana Rößler – Leiterin Bereich Security Incident Response, networker, solutions GmbH

Wie kommen Angreifer in Netzwerke?



Fortinet - Datenleak

```
P@ssw0rd12
123456
Castellon2019
Hallo123
Bonsai123456789
ar!2018
november2020+
Bine1408@
Start1604
Welcome34
Hello123
Thu1030
Lorenzo!
Start891
123Friet
Hello123
Start123
Dezember2020
Mathias03
:Start123
:Start123
:Start1234
:Start.123
:Hamburg2026
:Vergessen9
```

- 2020 wurden über eine Schwachstelle Fortinet-VPN Anmeldename und Passwort abgegriffen
- Schwachstelle wurde inzwischen gepatcht
- Wurden die Passwörter geändert?
- Wie ist die Reaktion der Betroffenen?

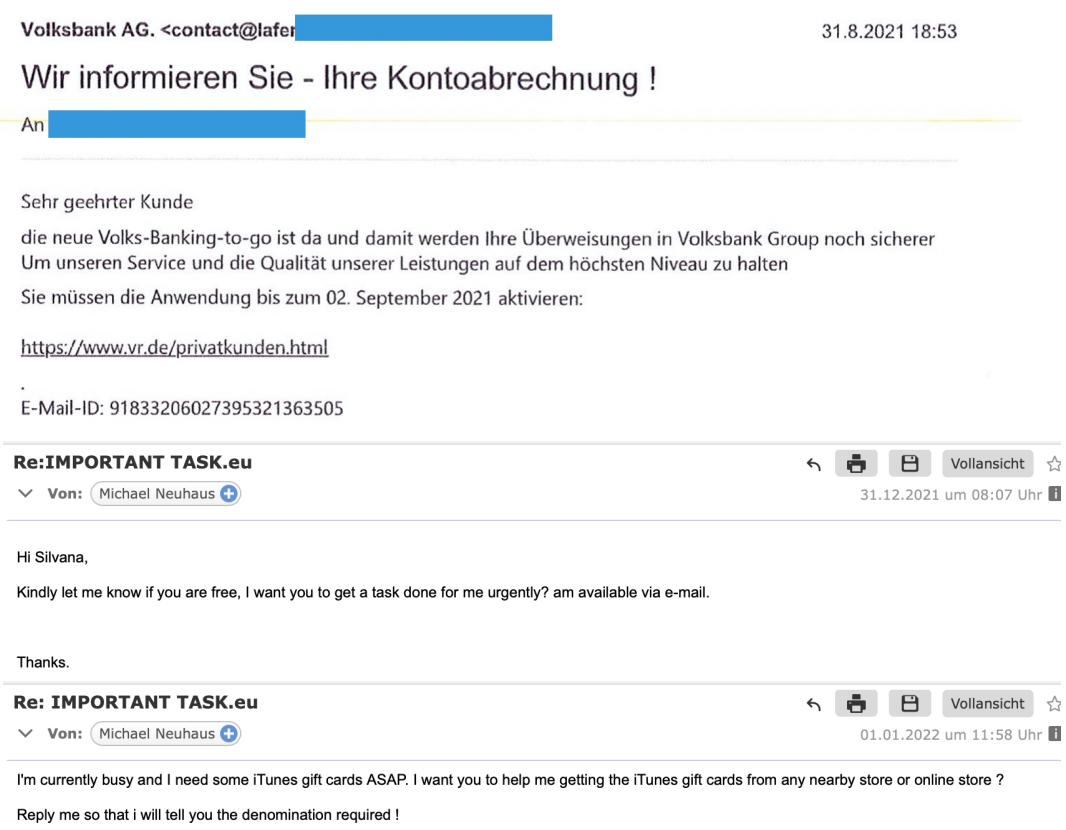
```
homeoffice05:siegburg+2020!
homeoffice15:siegburg+2020!
homeoffice09:siegburg+2020!
homeoffice03:siegburg+2020!
lager:start
kiel:kiel
test:test123
```

Hafnium // Proxyshell

- März 2021
- Massenhack von Exchange-Servern
- Kombination mehrerer Schwachstellen
- Umgehen der regulären Authentifizierung zu und Anmeldung als Administrator eines Exchange-Servers
- Ablegen von Dateien für eine Remote Code-Ausführung (RCE)

- Stunden nach Veröffentlichung des außerplanmäßigen Updates am 03.03.21 und Offenlegung der vier Schwachstellen, startete die massenhafte Infektion aller per Internet erreichbaren und ungepatchten Exchange-Server

Phishing



Volksbank AG. <contact@lafer[redacted] 31.8.2021 18:53

Wir informieren Sie - Ihre Kontoabrechnung !

An [redacted]

Sehr geehrter Kunde

die neue Volks-Banking-to-go ist da und damit werden Ihre Überweisungen in Volksbank Group noch sicherer
Um unseren Service und die Qualität unserer Leistungen auf dem höchsten Niveau zu halten

Sie müssen die Anwendung bis zum 02. September 2021 aktivieren:

https://www.vr.de/privatkunden.html

.
E-Mail-ID: 91833206027395321363505

Re:IMPORTANT TASK.eu Vollansicht

Von: Michael Neuhaus 31.12.2021 um 08:07 Uhr

Hi Silvana,

Kindly let me know if you are free, I want you to get a task done for me urgently? am available via e-mail.

Thanks.

Re: IMPORTANT TASK.eu Vollansicht

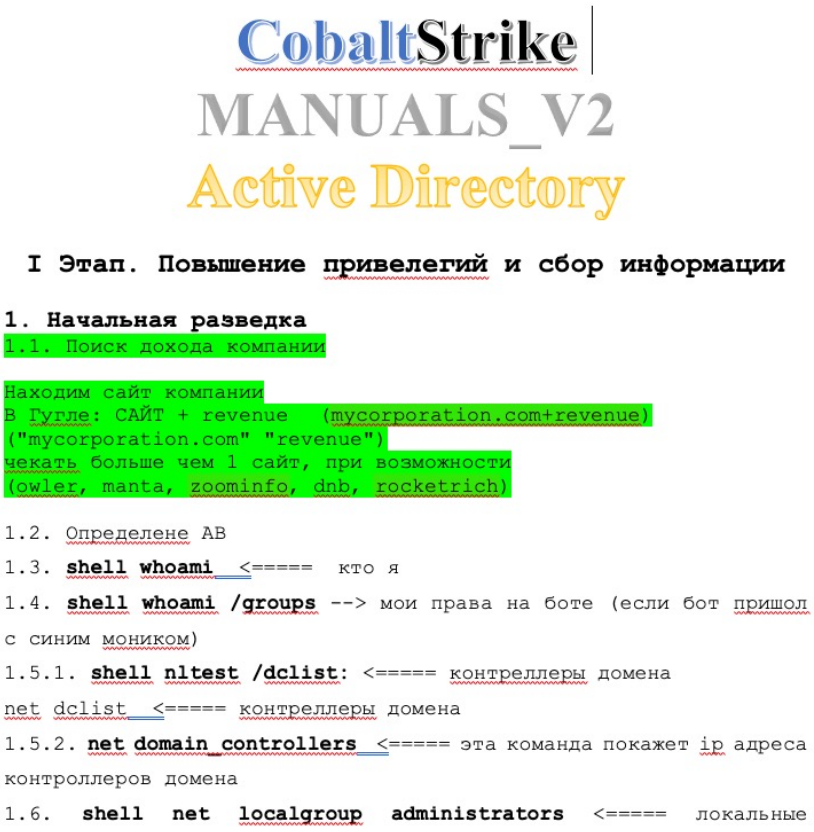
Von: Michael Neuhaus 01.01.2022 um 11:58 Uhr

I'm currently busy and I need some iTunes gift cards ASAP. I want you to help me getting the iTunes gift cards from any nearby store or online store ?

Reply me so that i will tell you the denomination required !

Zunahme professionell geplanter Angriffe

- In den Handbüchern für Partner beschreiben CONTI ausführlich für absolute Laien, wie man ein Netz auskundschaftet und sich in diesem bewegt, nach welchen Daten man sucht und wie man sie schließlich verschlüsselt.
- …inklusive Skripte
- Als Erstes sollen die Partner Informationen zum Umsatz des zukünftigen Opfers sammeln:
  Google: "mycorporation.com" "revenue"



Nach einem Angriffs

We've seen your message to your employees and customers. We know that you and your customers don't have backups. In addition, even if you recovered some part of the data, the price will not change. And we stole your data, and the data of one of the law firms you serve. If you don't pay, we'll publish their details along with yours!

A part of our customers don't have complete backups. We want to protect them and support them.

I know. Let's find a solution. x Mio $ would kill the company immediately.

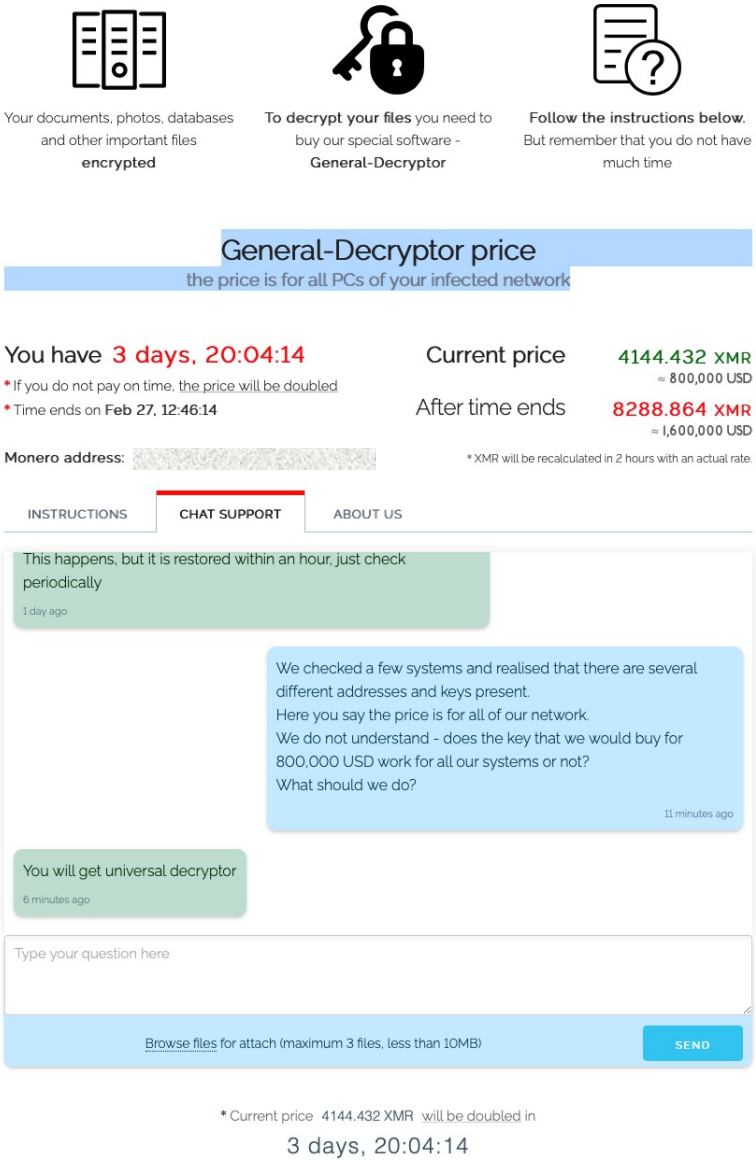
If we won't pay: We are out of business. If we would pay $ x Mio we are out of business.

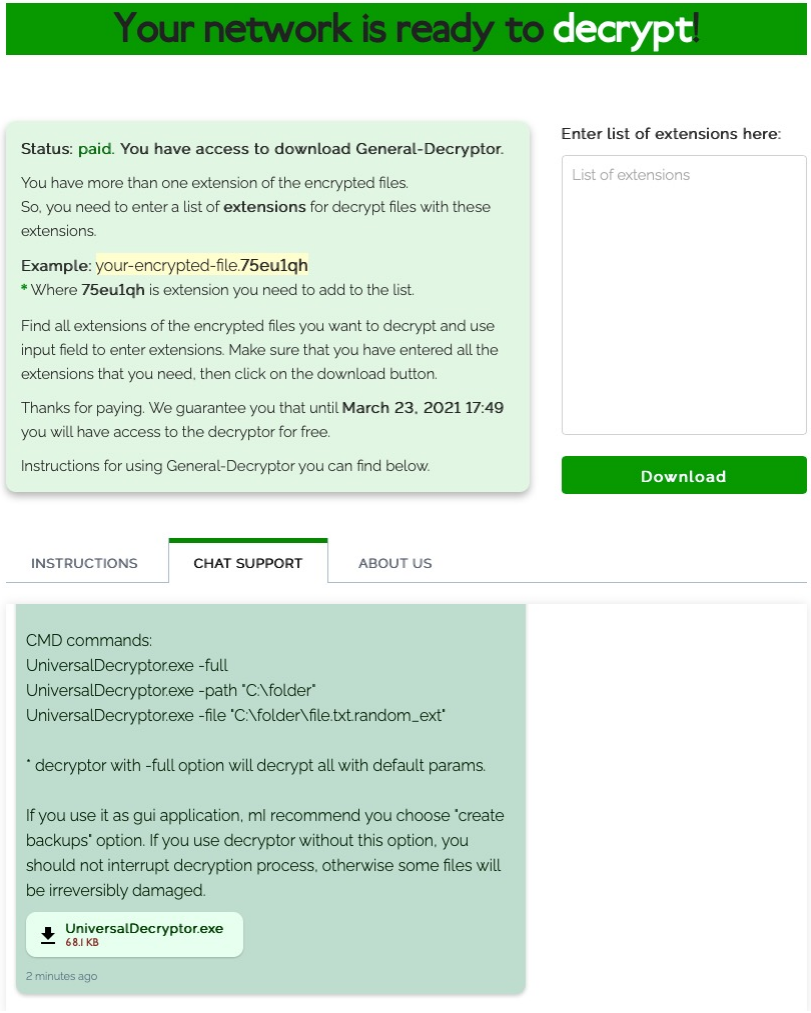
How much do you want to pay?

$ 250k
Because this is covered by the insurance.

No, that's not enough. You offer 4 times less! If you pay quickly, we will give you a discount.

Large payments have to be declared in Germany. XX is known as a group from Russia. Neither the banks nor my Bitcoin exchange and insurance are willing to violate the embargo regulations (war is always bad for business). This means: we are currently looking for very creative ways to exchange the money into Bitcoin. In addition, the customer has to cope with the loss of funds from the insurance company. WE NEED TIME.


Your documents, photos, databases and other important files **encrypted**
To decrypt your files you need to buy our special software - **General-Decryptor**
Follow the instructions below. But remember that you do not have much time
General-Decryptor price
the price is for all PCs of your infected network
You have 3 days, 20:04:14
* If you do not pay on time, the price will be doubled
* Time ends on Feb 27, 12:46:14
Current price
4144.432 XMR
≈ 800,000 USD
After time ends
8288.864 XMR
≈ 1,600,000 USD
Monero address:
* XMR will be recalculated in 2 hours with an actual rate.
INSTRUCTIONS
CHAT SUPPORT
ABOUT US
This happens, but it is restored within an hour, just check periodically
1 day ago
We checked a few systems and realised that there are several different addresses and keys present.
Here you say the price is for all of our network.
We do not understand - does the key that we would buy for 800,000 USD work for all our systems or not?
What should we do?
11 minutes ago
You will get universal decryptor
6 minutes ago
Type your question here
Browse files for attach (maximum 3 files, less than 10MB)
SEND
* Current price 4144.432 XMR will be doubled in
3 days, 20:04:14


Your network is ready to decrypt!
Status: paid. You have access to download General-Decryptor.
You have more than one extension of the encrypted files.
So, you need to enter a list of **extensions** for decrypt files with these extensions.
Example: your-encrypted-file.**75eu1qh**
* Where **75eu1qh** is extension you need to add to the list.
Find all extensions of the encrypted files you want to decrypt and use input field to enter extensions. Make sure that you have entered all the extensions that you need, then click on the download button.
Thanks for paying. We guarantee you that until **March 23, 2021 17:49** you will have access to the decryptor for free.
Instructions for using General-Decryptor you can find below.
Enter list of extensions here:
List of extensions
Download
INSTRUCTIONS
CHAT SUPPORT
ABOUT US
CMD commands:
UniversalDecryptor.exe -full
UniversalDecryptor.exe -path "C:\folder"
UniversalDecryptor.exe -file "C:\folder\file.txt.random_ext"
* decryptor with -full option will decrypt all with default params.
If you use it as gui application, ml recommend you choose "create backups" option. If you use decryptor without this option, you should not interrupt decryption process, otherwise some files will be irreversibly damaged.
UniversalDecryptor.exe
68.1 KB
2 minutes ago

CYBERVERSICHERUNGEN

Silvana Rößler – Leiterin Bereich Security Incident Response, networker, solutions GmbH

Welche Kosten können im Schadenfall entstehen

- Betriebsausfall und –unterbrechung
- Eigenschaden
- Fremdschaden
- Datenwiederherstellung
- IT-Expertenleistungen
- Rechtsberatung
- Datenschutz
- Krisenmanagement
- PR

Die Kosten eines Cyberschadens können so hoch sein, dass diese die Existenz der Betroffenen bedrohen können.

Herausforderungen im Schadenfall

- Wo fängt man an?
- Wie geht man vor?
- Wo findet man Spezialisten?
- Wer koordiniert die vielen einzelnen Parteien?

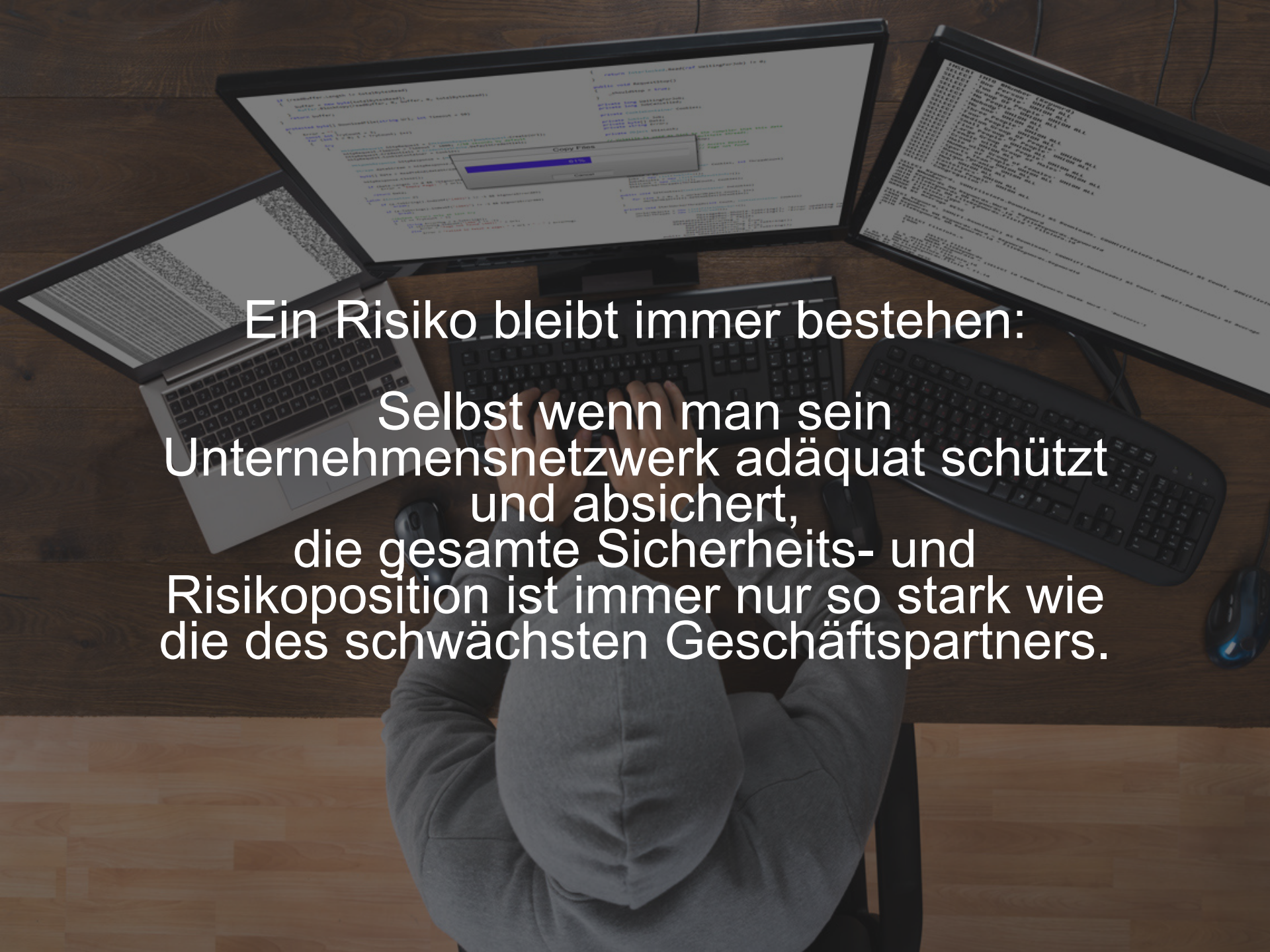
- Muss man Lösegeld bezahlen? Muss man mit Angreifern kommunizieren?
- Wie funktioniert dies?

Wer ist an einem Wochenende / Feiertag für mich da?

Vor Abschluss

Fragen beispielsweise zu

- Vorschäden
- Aufbau der IT
- Sicherheitsupdates
- Back-Ups !!!!!!
- Zwei-Faktor-Authentisierung
- Firewall // Antivirenlösung
- Verpflichtendes 4-Augen-Prinzip bei größeren Überweisungen


Ein Risiko bleibt immer bestehen:
Selbst wenn man sein Unternehmensnetzwerk adäquat schützt und absichert,
die gesamte Sicherheits- und Risikoposition ist immer nur so stark wie die des schwächsten Geschäftspartners.