

Emergency Response nach einem Cyber Angriff



/ Referent



Maximilian Zahn

Cyber Security Consultant DFIR

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

Mobil: +49 151 12684657
Email: maximilian.zahn@sva.de
www.sva.de

/ Agenda

1. Motivation

2. Top Cyberbedrohung Ransomware

3. Ransomware-Vorfall: Ein Szenario

4. Prevention and Readiness

5. Fazit

/ 1. Motivation – Top Bedrohungen je Zielgruppe

Wirtschaft

- Ransomware
- Abhängigkeit innerhalb der IT-Supply-Chain
- Schwachstellen
- Offene oder falsch konfigurierte Onlineserver

Staat und Verwaltung

- Ransomware
- APT
- Schwachstellen
- Offene oder falsch konfigurierte Onlineserver



Ransomware

SVA

/ Eigenschaften & Auswirkungen

- Professionelle externe Angreifer
- Diebstahl von Daten
- Verschlüsselung von Daten
- Lösegelderpressung

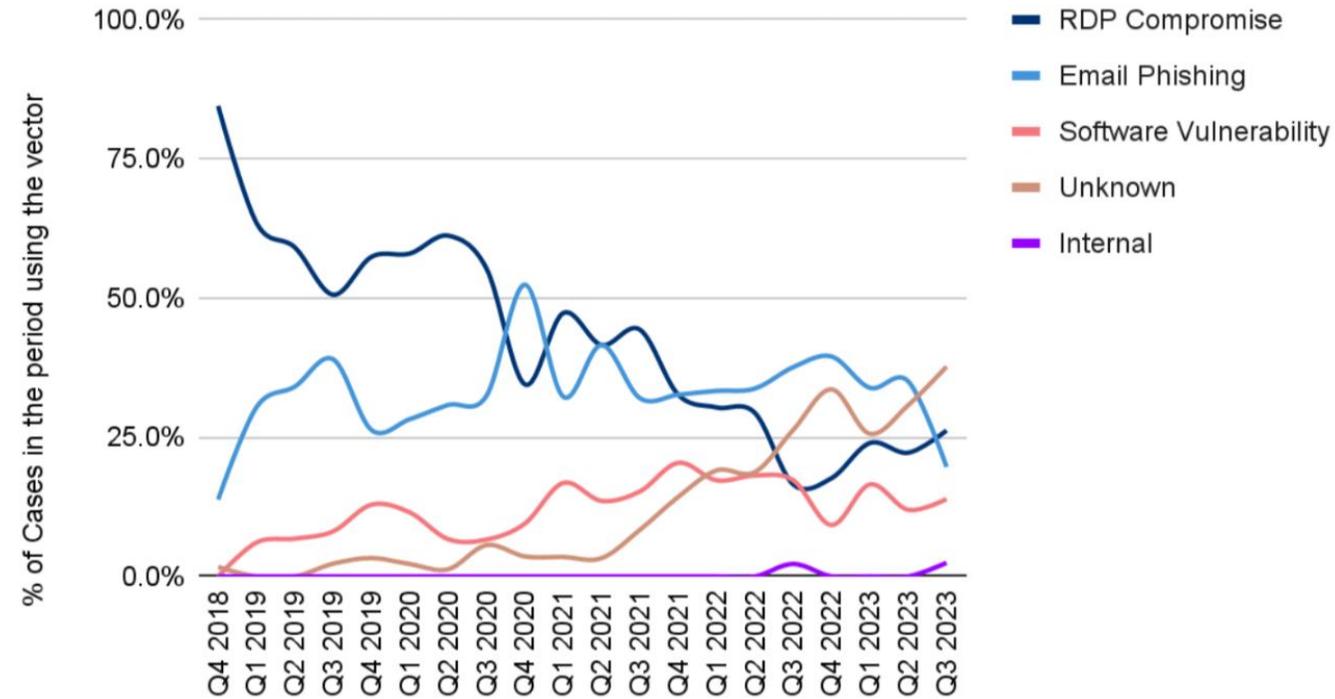
Unterbrechung von Kommunikation, Produktion, Handel, gesamter Wertschöpfungskette



ENISA Threat Landscape for Ransomware Attacks

/ Angriffsvektor

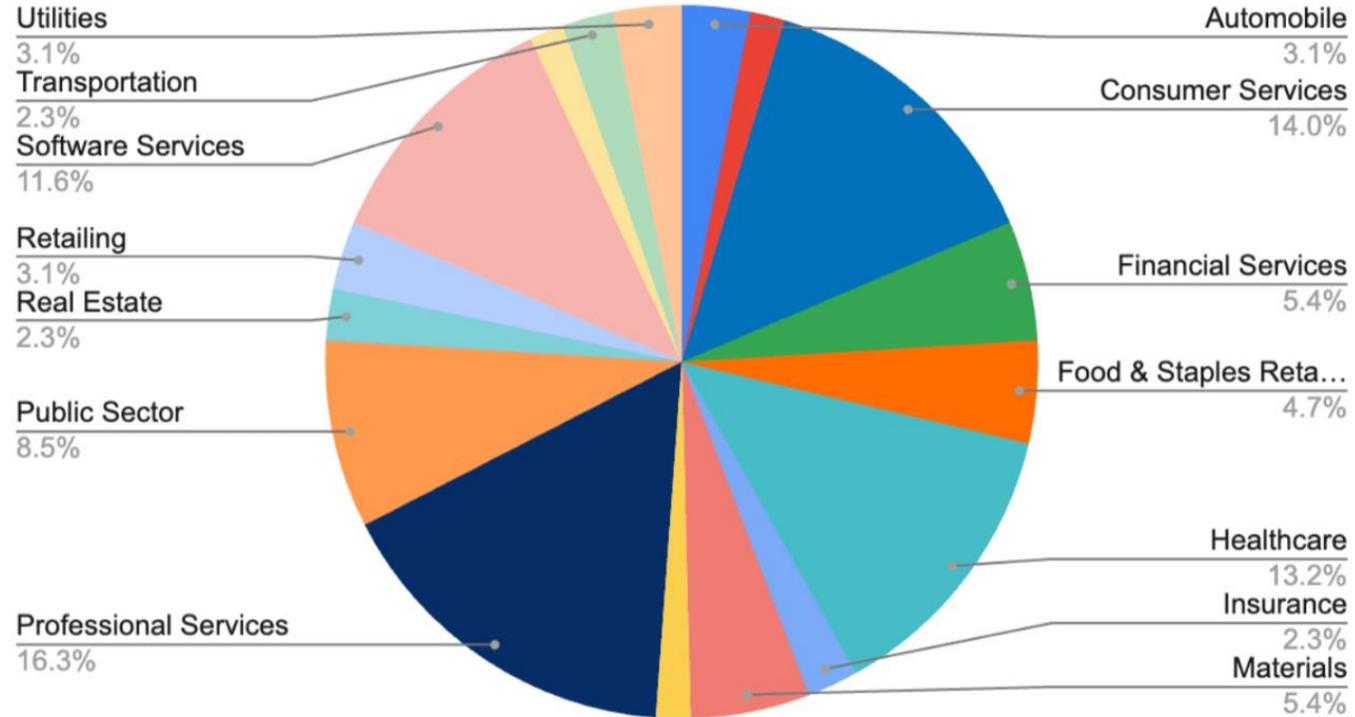
Ransomware Attack Vectors



<https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals>

/ Branchen

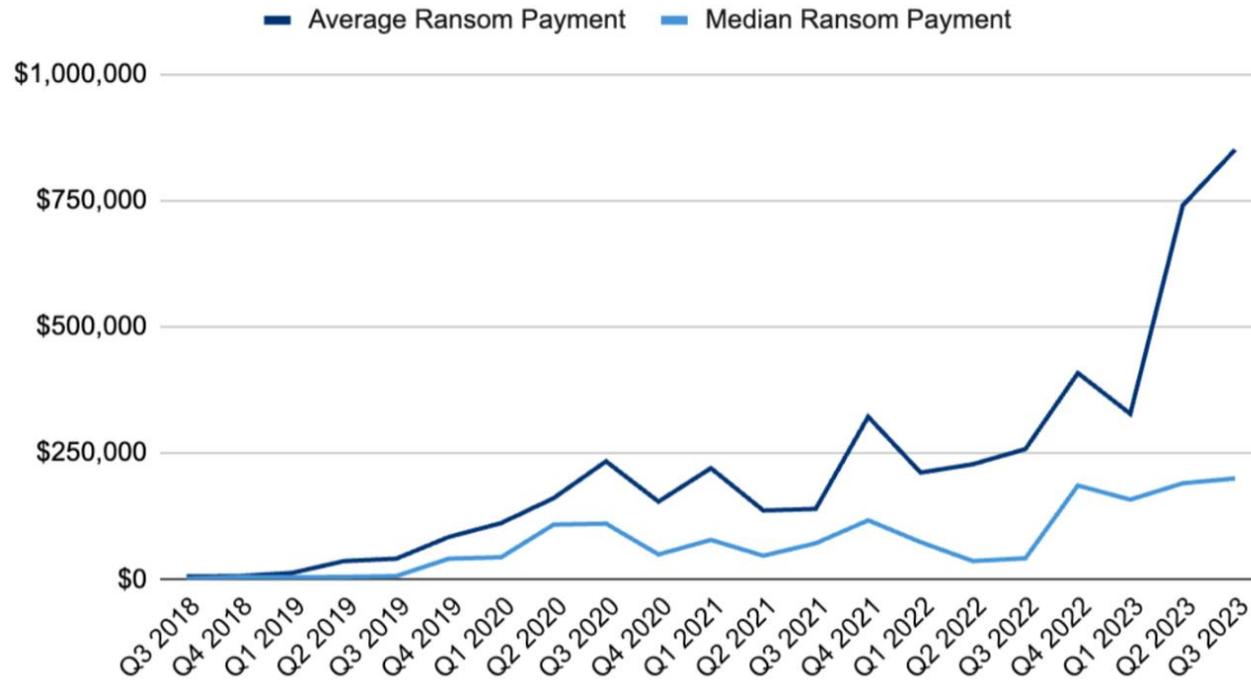
Industries Impacted by Ransomware Q3 2023



<https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals>

/ Ransomware-Zahlungen

Ransom Payments By Quarter



Average Ransom Payment
\$850,700
+15% from Q2 2023

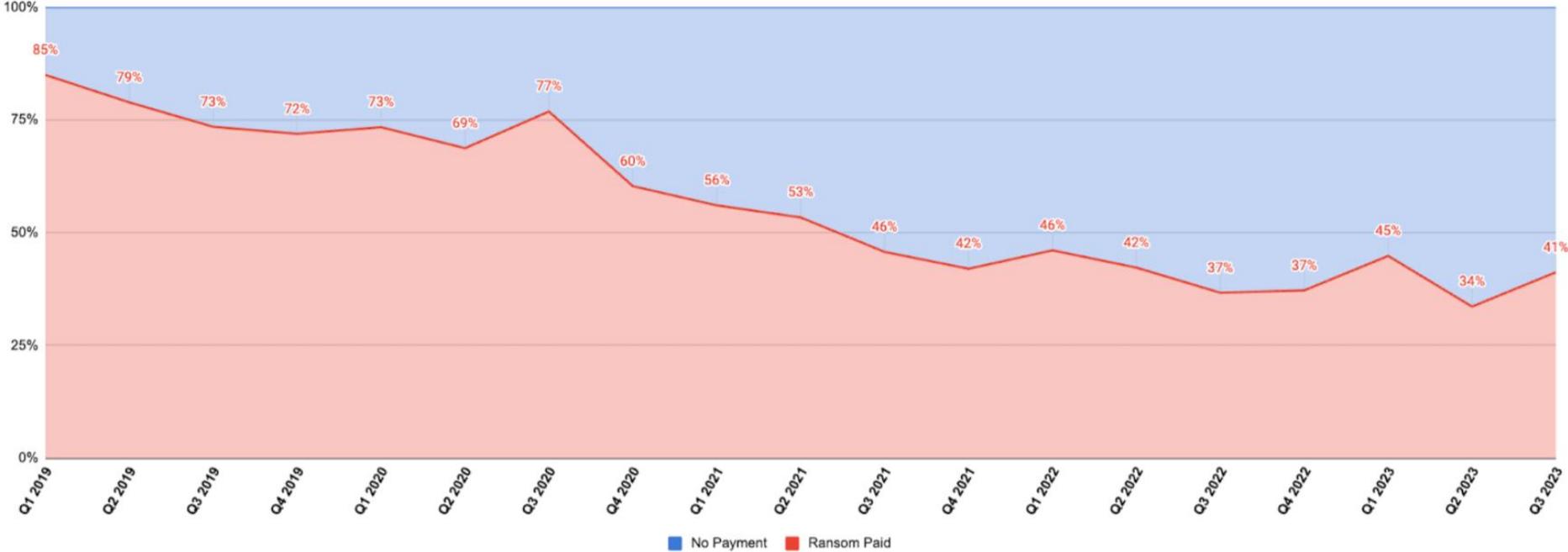
Median Ransom Payment
\$200,000
+5% from Q2 2023



<https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals>

/ Lösegeldzahlungen

All Ransomware Payment Resolution Rates



<https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals>

/ Ransomware Groups

Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem



Source: Halcyon (Q3 2023)

/ Data Leaks

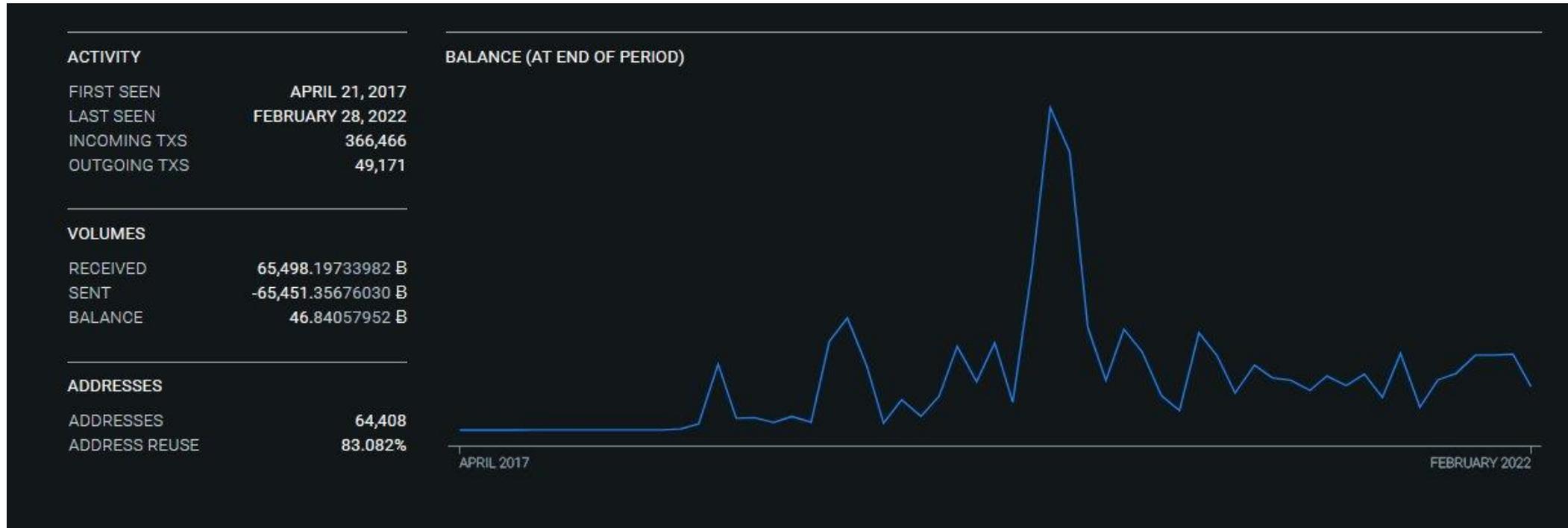
The screenshot shows the LockBit BLOG website with a grid of 16 data leak entries. Each entry includes the domain name, a timestamp, a brief description of the leak, and the date it was updated. The entries are as follows:

Domain	Timestamp	Description	Updated	Views
interfides.de	19D 23h 37m 27s	interfides Steuerberatungsgesellschaft mbH was established in 1978, and specialises in providing advisory services to foreign clients with a business presence in Germany.	09 May, 2023, 12:47 UTC	22
hk-finance.pl	13D 22h 50m 15s	LEADING PROVIDER OF ACCOUNTING, HR & PAYROLL, AND FINANCIAL CONSULTANCY SERVICES	09 May, 2023, 11:58 UTC	58
cbelaw.com	19D 22h 08m 27s	Cohen Buchan Edwards LLP is a full service law firm providing practical, client-oriented service that delivers results. For more than 40 years, an exceptional legal team of lawyers and staff have	09 May, 2023, 11:18 UTC	73
astate.edu	8D 22h 14m 39s	Founded in 1909, A-State meets the challenges of continuing as a destination university for more than 14,000 students through the combination of world-class research with a long tradition of	09 May, 2023, 07:24 UTC	179
stmarys.net	8D 20h 36m 00s	St Mary's Catholic School is part of the mission of the Catholic Church, which places the educational process in this setting. Complete database and file data exfiltrated. Failure to negotiate with us will	08 May, 2023, 09:45 UTC	736
unity.edu	8D 20h 30m 37s	Unity College is a private college based in New Gloucester, Maine with an additional campus in Unity and facilities in Moose River and Thorndike. It offers undergraduate and graduate education	08 May, 2023, 09:40 UTC	714
lssny.org	8D 20h 23m 14s	Today, Lutheran Social Services of New York provides a myriad of social services, including helping seniors live independently, finding loving families for children, providing safe and affordable	08 May, 2023, 09:32 UTC	721
namibmills.com	2D 02h 12m 36s	Namib Mills Ltd, established in 1982, is the largest grain processing company in Namibia. It produces flour, pasta, animal feeds and other products from raw materials including maize, much of which is	07 May, 2023, 15:22 UTC	1210
marshallconstruction.co.uk	17D 19h 25m 34s	MARSHALL CONSTRUCTION Established in 1983 we are one of Scotland's foremost independent building contractors	07 May, 2023, 08:35 UTC	1271
joysonsafety.com	2D 06h 48m 23s	We took 20TB of data from the company and are publishing the name to encourage them to connect and discuss before we post all the data and cause irreparable damage to the company.	04 May, 2023, 17:57 UTC	3033
layherna.com	18h 31m 42s	Layher North America is a company that operates in the Construction industry. It employs 251-500 people and has \$50M-\$100M of revenue. The company is headquartered in Houston, Texas.	04 May, 2023, 11:41 UTC	3078
fullertonindia.com	PUBLISHED	Founded in 1994 and headquartered in Mumbai, India, Fullerton India Credit Company Limited provides financial solutions. The Company offers commercial vehicle, home improvement, personal,	03 May, 2023, 18:34 UTC	7725
triaflex.at	8D 02h 34m 58s	Welcome to TRIAFLEX We design the ergonomic living space work!	03 May, 2023, 15:44 UTC	3331
cydsa.com	PUBLISHED	Cydsa, S.A.B. de C.V., together its subsidiaries, engages in the production and marketing of salt, chlorine, caustic soda, and refrigerant gases in Mexico, the United States, Canada, Central and	03 May, 2023, 01:15 UTC	3831
hasenauer-anlagenbau.at	7D 08h 24m 23s	QUALITY IS THE BEST When it comes to water, heating, cooling, air and climate, we always get to work with fresh wind and full motivation. We offer the highest professional quality at all levels – from	02 May, 2023, 21:33 UTC	3671
multimedica.it	PUBLISHED	The MultiMedica Group First of all there is Ethics. It is not limited to a series of principles to be followed, but constitutes the overall vision of MultiMedica's activities, its mission, its raison	02 May, 2023, 21:33 UTC	10324

/ Lohnt sich das?

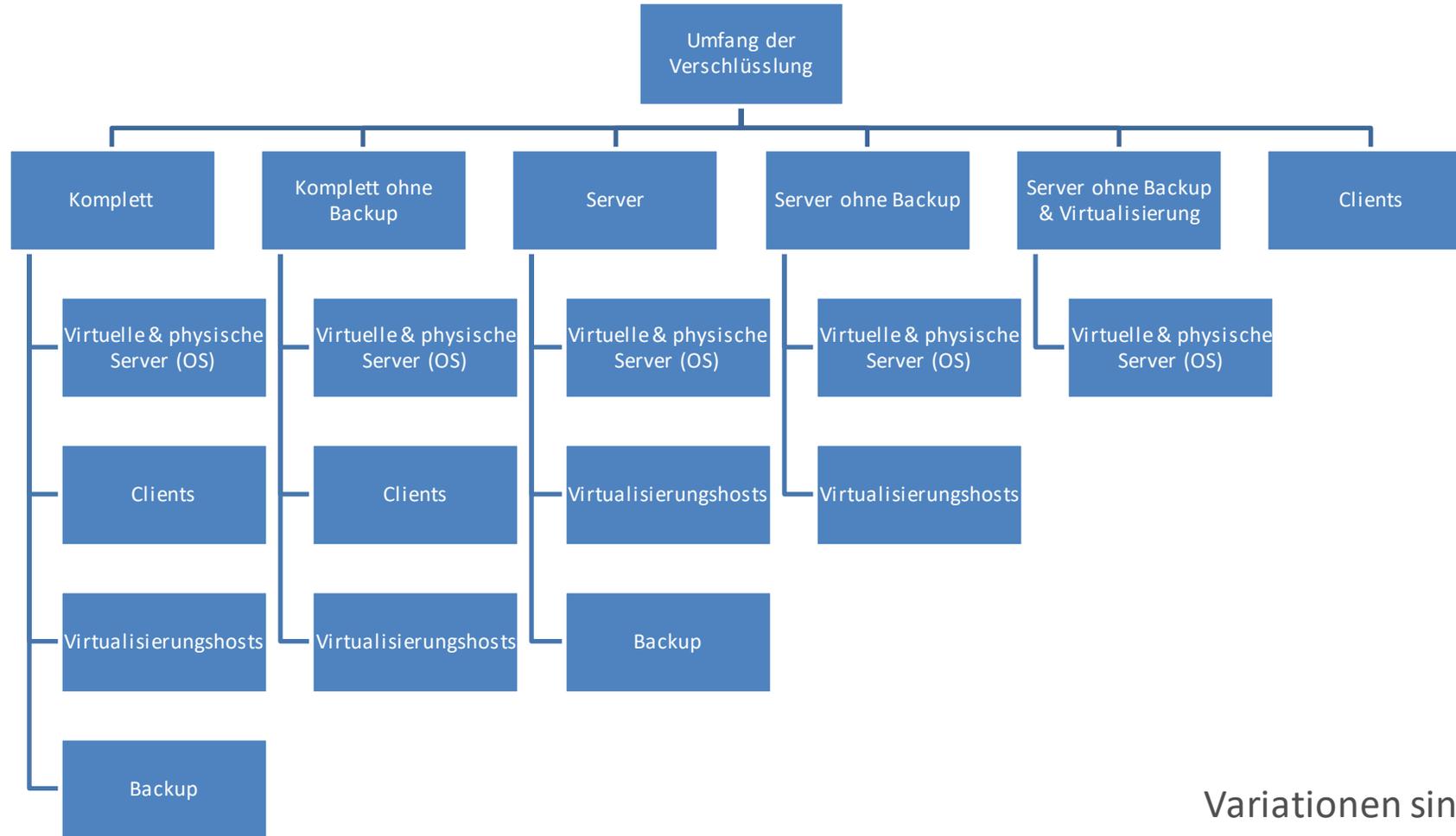
Primäre Bitcoin Adresse von Conti: Von April 2017 bis Februar 2022 **65.498,197 BTC** empfangen

Ca. 2.512.605.814 €



<https://twitter.com/vxunderground/status/1498394338027610124>

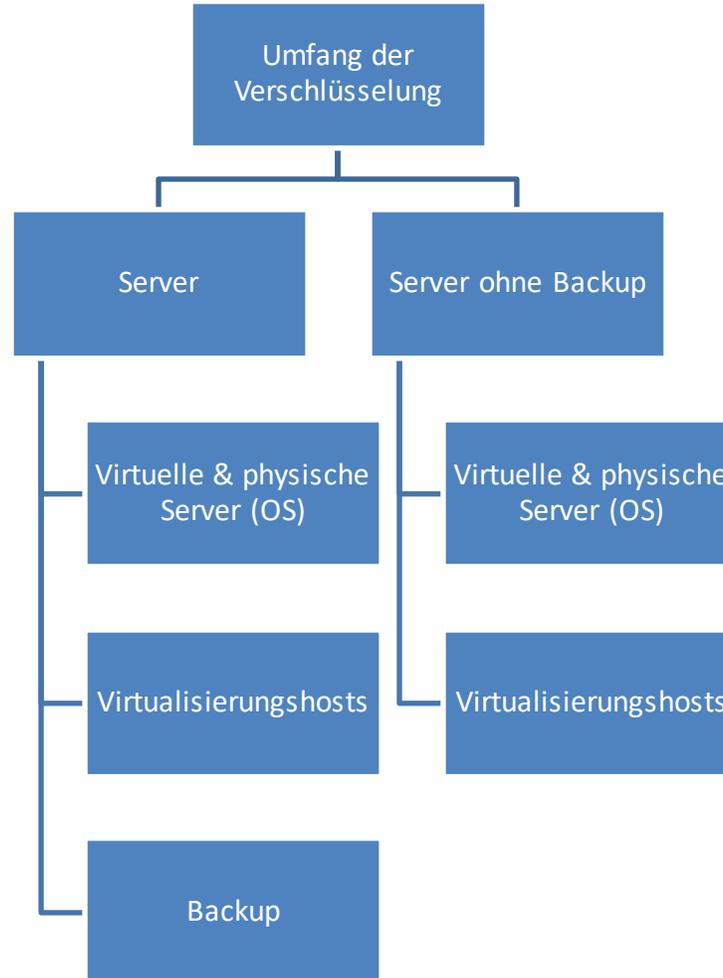
/ Was wird verschlüsselt?



Variationen sind möglich

/ Beobachtung von SVA

1. Backup Jobs entfernen & Snapshots löschen
2. Backup verschlüsseln
3. Server auf Betriebssystemebene
4. VMDKs/VMX auf Virtualisierungshosts verschlüsseln



So viel wie möglich
in kurzer Zeit.



Montagmorgen in ihrem Unternehmen

SVA

/ Erste Meldung vom Mitarbeiter/in

- Alice betritt das Büro an einem ganz normalen Morgen
- Als Alice den Computer hochfährt, bemerkt sie, dass ihre Dateien und Ordner seltsam benannt sind und sie keinen Zugriff auf wichtige Dokumente hat
- Auf dem Bildschirm ist eine seltsame Nachricht zu lesen, in der von einer Bitcoin Forderung die Rede ist
- Sie erkennt, dass etwas nicht stimmt und meldet sich bei Bob in der IT

/ Troubleshooting durch IT-Admins

- Bob probiert sich am Client System remote anzumelden
- Nachdem das nicht funktioniert kommt Bob bei Alice vorbei und begutachtet den Computer
- Ein Erpresserschreiben ist zu erkennen
- Seltsame Dateinamen
- Von "LockBit" ist die Rede



Papierkorb



Microsoft Edge



HLJkNskOq.READ...



kunden.csv



partner.xlsx



m8akrbl



xRH9Bwy

LockBit Black

**All your important files are stolen and encrypted!
You must find **HLJkNskOq.README.txt** file
and follow the instruction!**



Suchen



19°C Meist sonnig



14:45
09.05.2023



LockBit 3.0 the world's fastest and most stable ransomware from 2019

>>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate

Tor Browser Links:

<http://lockbitapt2d73kr1bewgv27tquljgxr33xbwvsp6rkyieto7u4ncead.onion>
<http://lockbitapt2yfbt71chxejug47kmqvqqxvvpqkmbev413azl3gy6pyd.onion>
<http://lockbitapt34kvr1p6xojy1ohhxrswvpzdfffgs5z4pbbsywnzsbduqd.onion>
<http://lockbitapt5x4zkjbcqzm6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion>
<http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion>
<http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion>
<http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqppid.onion>
<http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion>
<http://lockbitaptc2iq4atewz2ise62q63wfkyr14qtuwk5qax262kgtzjqd.onion>

Links for normal browser:

<http://lockbitapt2d73kr1bewgv27tquljgxr33xbwvsp6rkyieto7u4ncead.onion.ly>
<http://lockbitapt2yfbt71chxejug47kmqvqqxvvpqkmbev413azl3gy6pyd.onion.ly>
<http://lockbitapt34kvr1p6xojy1ohhxrswvpzdfffgs5z4pbbsywnzsbduqd.onion.ly>
<http://lockbitapt5x4zkjbcqzm6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly>
<http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion.ly>
<http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly>
<http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqppid.onion.ly>
<http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly>
<http://lockbitaptc2iq4atewz2ise62q63wfkyr14qtuwk5qax262kgtzjqd.onion.ly>

>>>> What guarantee is there that we won't cheat you?

We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide

>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser <https://www.torproject.org/>

Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret c

Tor Browser Links for chat:

<http://lockbitsupa7e3b4pkn4mgkgojr15iqgx24clbzc4xm7i6jeetsia3qd.onion>
<http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion>
<http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hznzmtxdvjoqlp7yd.onion>
<http://lockbitsupo7vv5vc13jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion>
<http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkkt5xfw3draxk6gwwd.onion>
<http://lockbitsupqfyacidr6upt6nhhyipujsvaablubuevxj6xy3frthvr3yd.onion>
<http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoymb1niabj4uwvzapqd.onion>
<http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kfcg6u33zfvq3oyd.onion>
<http://lockhitsunxncintihhmat4rrh7ktowins2azvvh67er5r3xafhivihad.onion>

SO I JUST HAVE TO PAY YOU HALF A



BITCOIN TO UNLOCK MY COMPUTER?

/ Und jetzt?

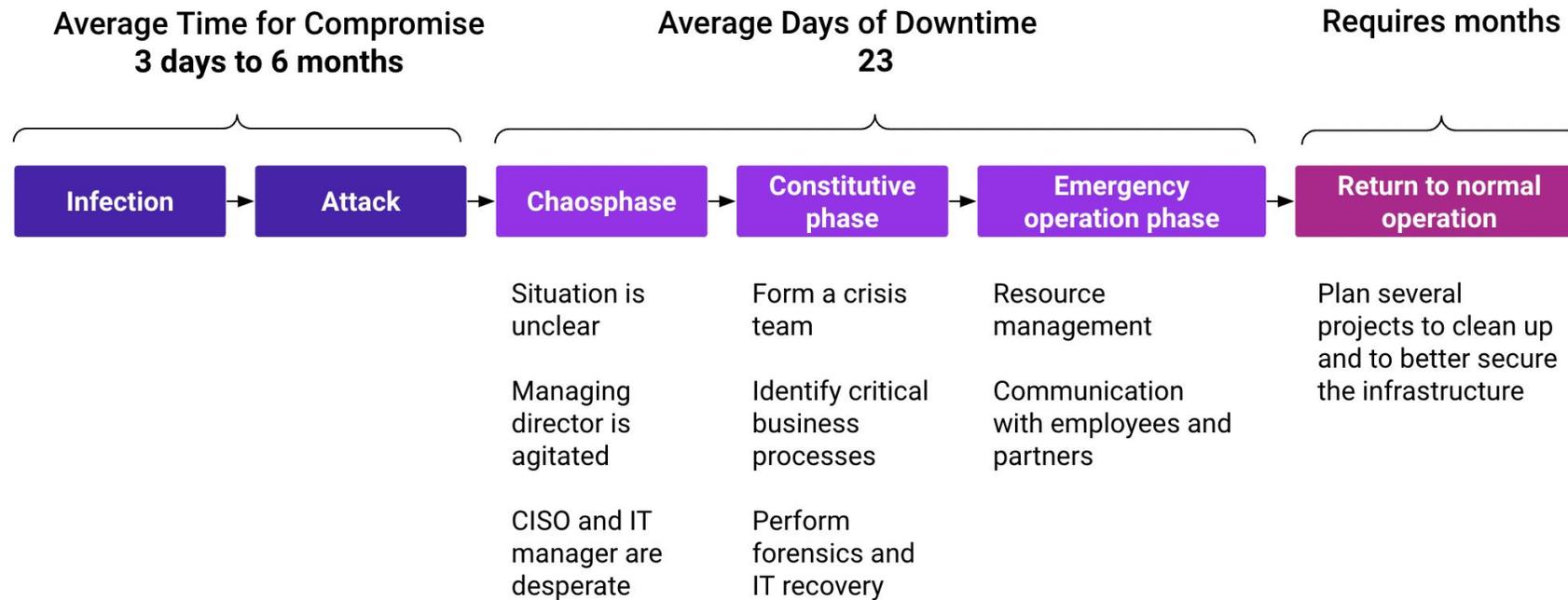
- Was muss wer jetzt machen?
- Wer hat den Hut auf?
- Wer trifft Entscheidungen?
- Funktionierte mein Backup?
- Wie und wann leite ich ein Restore ein?
- Wie wird kommuniziert?
- Gibt es einen Krisenstab?
- Wo tagt der Krisenstab?
- Wie erreiche ich die Mitglieder des Krisenstabs?
- Lesen die Angreifer bei Teams mit?
- Wurden Daten gestohlen und wenn ja welche?
- Datenschutzvorfall melden?
- Externer Support zum Incident Handling?
- ...



/ Wie organisieren Sie sich?

Konkret wissen, wie zu handeln ist, gibt Sicherheit und ist der Schlüssel für ein geregeltes Incident Handling.

Phases After a Ransomware Attack



<https://blog.mondoo.com/how-to-handle-a-ransomware-incident-part3>

/ Optionen

Restore aus dem Backup

Neuaufbau

Lösegeldzahlung



Restore

SVA

/ Restore, die beste Option

- Wo ist das Backup?
- Wie viele und welche Systeme sollen wiederhergestellt werden?
- In welcher Reihenfolge?
- Welche Voraussetzungen bestehen für das Backup?
 - Storage
 - Neue Virtualisierungshosts?
 - Datensicherung der kompromittierten Systeme?
- Wie lange dauert die Wiederherstellung?
- Sind die Systeme sauber oder kompromittiert im Backup?



Neuaufbau

SVA

/ Neuaufbau, Vor- und Nachteile

- Neuaufbau mit neuer Infrastruktur
- Einhaltung aktueller Sicherheitsempfehlungen
- Saubere Systeme und Infrastruktur

- Zeitlicher Aufwand
- Technisches Know-How
- Hardware / Software / Lizenzen

Lösegeldverhandlung



/ Kryptowährung?



- Wie zahle ich mit Monero oder Bitcoin?
- Was ist eine Kryptobörse?
- Was ist ein Wallet?
- Warum blockiert meine Hausbank die Überweisung?
- Warum sperrt die Kryptobörse meinen Account?



Prevention & Readiness



/ Wie man es vermeidet Lösegeld zu zahlen

- **Technische und organisatorische Maßnahmen**
- Backup & Restore
 - 3-2-1 Regel
 - Backup-System mit lokaler Authentifizierung (nicht in Active Directory)
 - Restore Plan & Listen
 - Restore Übungen
- **Vertrauliche Daten**
 - Identifizieren (personenbezogene Daten, Geschäftsdaten etc.)
 - Zugriff beschränken
 - Zugriff auditieren
 - Datenabfluss detektieren
- **Notfallinfrastruktur**

/ Übliche Stolperfallen

- Fehlender Krisenplan
- Fehlendes Restore-Konzept
- Fehlende Restore-Reihenfolge
- Fehlende Notfallinfrastruktur
 - Telefonie
 - E-Mail
 - Zweiter Internetanschluss (DSL, LTE, 5G)
 - Saubere Notebooks
- Sicherung verschlüsselter Daten (wohin?)
- Speicherplatz für Restore zu gering
- Ungeübte Mitarbeiter

/ Übung macht den Meister

- Table Top Exercises
- Stabsübungen
- Technische Übungen

Fazit

/ Check Out

Fragen?

Offene Themen?

Feedback

DANKE

