IKARUS security software

CYBER SECURITY AUSTRIA

Security ist mehr als Ransomware

aber es lohnt sich jedenfalls JETZT über letzteres nachzudenken

CyberSecurity

– res publica – 

ES geht uns alle an!

DIE WICHTIGSTEN GLOBALEN GESCHÄFTSRISIKEN 2020

Der Trend gibt die Änderung der Platzierung im Vergleich zum Vorjahr an.

Rang		Prozent	2019 rang	Trend
1	**Cyber-Vorfälle (z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen).**	**39%**	2 (37%)	▲
2	Betriebsunterbrechung (inkl. Lieferkettenunterbrechung)	**37%**	1 (37%)	▼
3	Rechtliche Veränderungen (z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)	**27%**	4 (27%)	▲
4	Naturkatastrophen (z.B. Sturm, Überschwemmung, Erdbeben)[1]	**21%**	3 (28%)	▼
5	Marktentwicklungen (z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)	**21%**	5 (23%)	=
6	Feuer, Explosion	**20%**	6 (19%)	=
7	Klimawandel/steigende Volatilität des Wetters	**17%**	8 (13%)	▲
8	Reputationsverlust oder Beeinträchtigung des Markenwerts	**15%**	9 (13%)	▲
9	Neue Technologien (z.B. Auswirkung der Vernetzung von Maschinen, Nanotechnologie, künstliche Intelligenz, 3D-Druck, autonome Fahrzeuge, Blockchain)	**13%**	7 (19%)	▼
10	Makroökonomische Entwicklungen (z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)	**11%**	13 (8%)	▲
11	Politische Risiken (z.B. Krieg, Terrorismus, Aufruhr)	**9%**	11 (9%)	=
12	Fachkräftemangel	**9%**	10 (9%)	▼
13	Stromausfälle bei kritischen Infrastrukturen (z.B. Unterbrechung der Stromleistungen)[2]	**8%**	17 (2%)	▲
14	Produktrückruf, Qualitätsmängel, Serienfehler	**8%**	12 (9%)	▼
15	Diebstahl, Betrug, Korruption[3]	**7%**	15 (7%)	=
16	Umweltrisiken (z.B. Verschmutzung)	**7%**	14 (7%)	▼
17	Gesundheitsthemen (z.. B. Pandemien)	**3%**	16 (3%)	▼
	Andere	**3%**	-	-

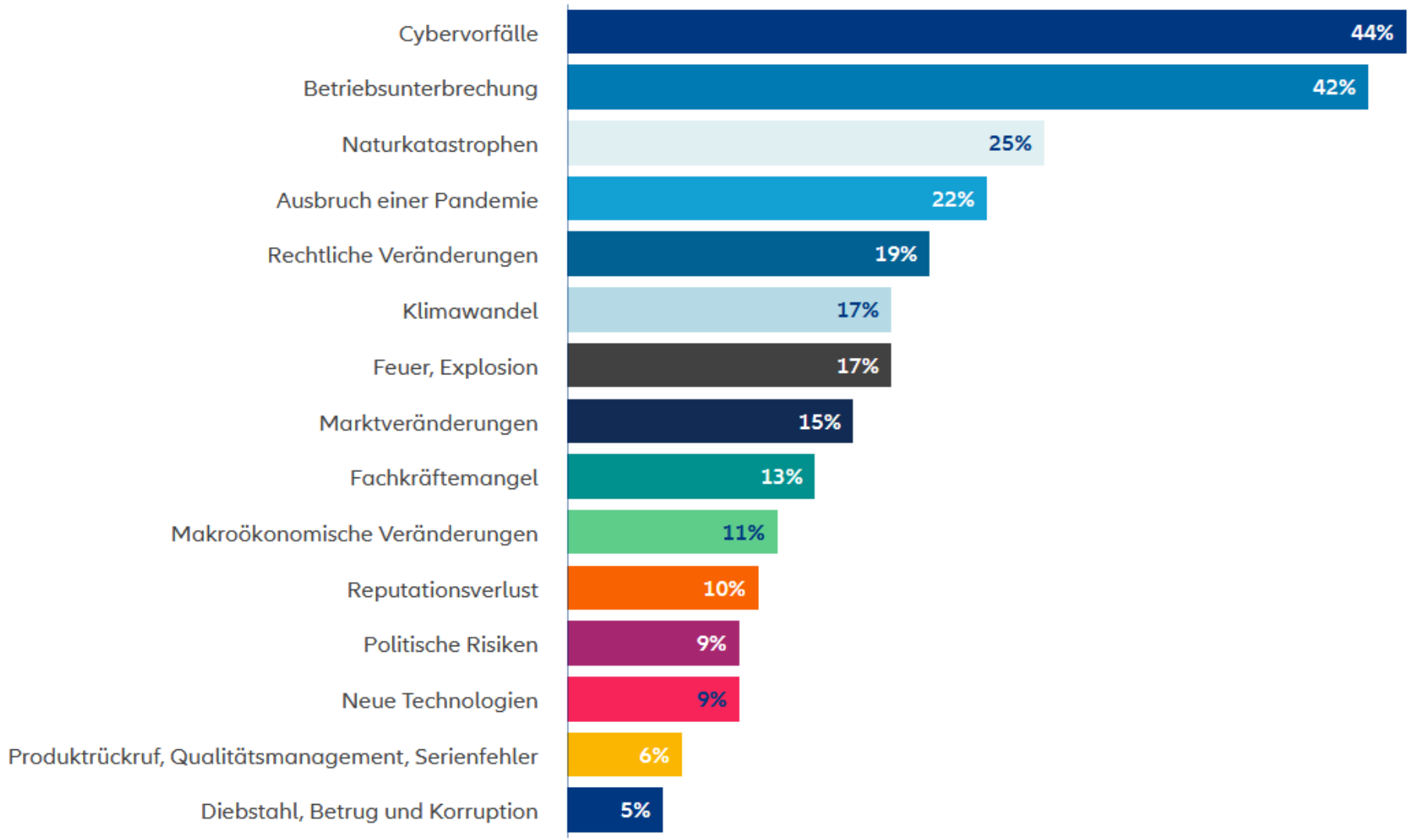
1 Naturkatastrophen rangieren aufgrund der höheren Anzahl der Antworten höher als Marktentwicklungen (Prozentsatz ist gerundet).

2 Stromausfälle bei kritischer Infrastruktur rangieren aufgrund der höheren Anzahl der Antworten höher als Produktrückrufe (Prozentsatz ist gerundet).

3 Diebstahl, Betrug und Korruption rangieren aufgrund der höheren Anzahl der Antworten höher als Umweltrisiken (Prozentsatz ist gerundet).

https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

Top 10 Geschäftsrisiken weltweit in 2022

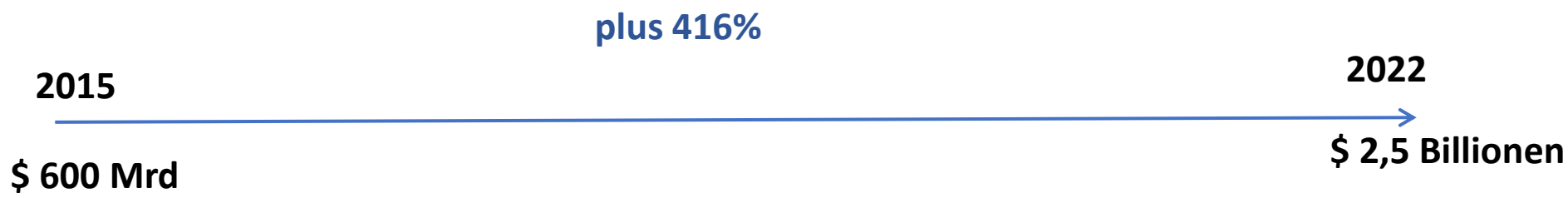


https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html

Successtory CyberCrime

2,5 Billionen Dollar schwer wird der Markt für CyberCrime eingeschätzt

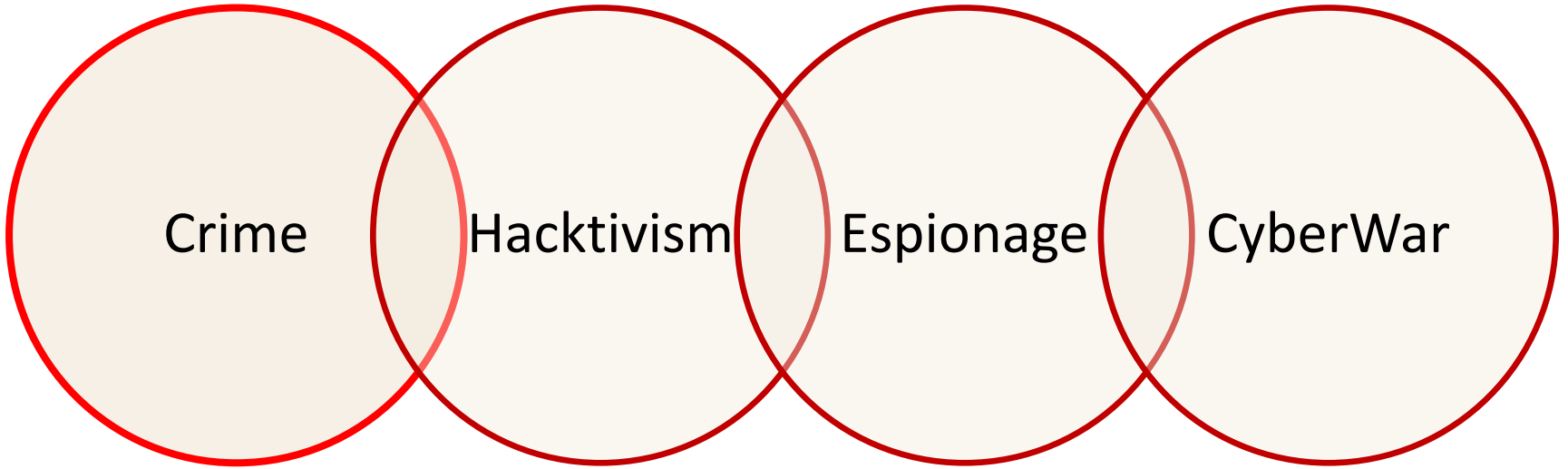
Das würde immerhin schon 0,8% des globalen GDP´s ausmachen. Im Vergleich dazu beträgt das BIP in Österreich „magere“ 369 Mrd. Euro.



2,5E + 12 =

5 Mio Einfamilien Häuser a 500k
oder
Bildungsbudget Österreich 8,8 Mrd Euro wäre ~ 284 mal enthalten

https://bit.ly/2NkEbbP



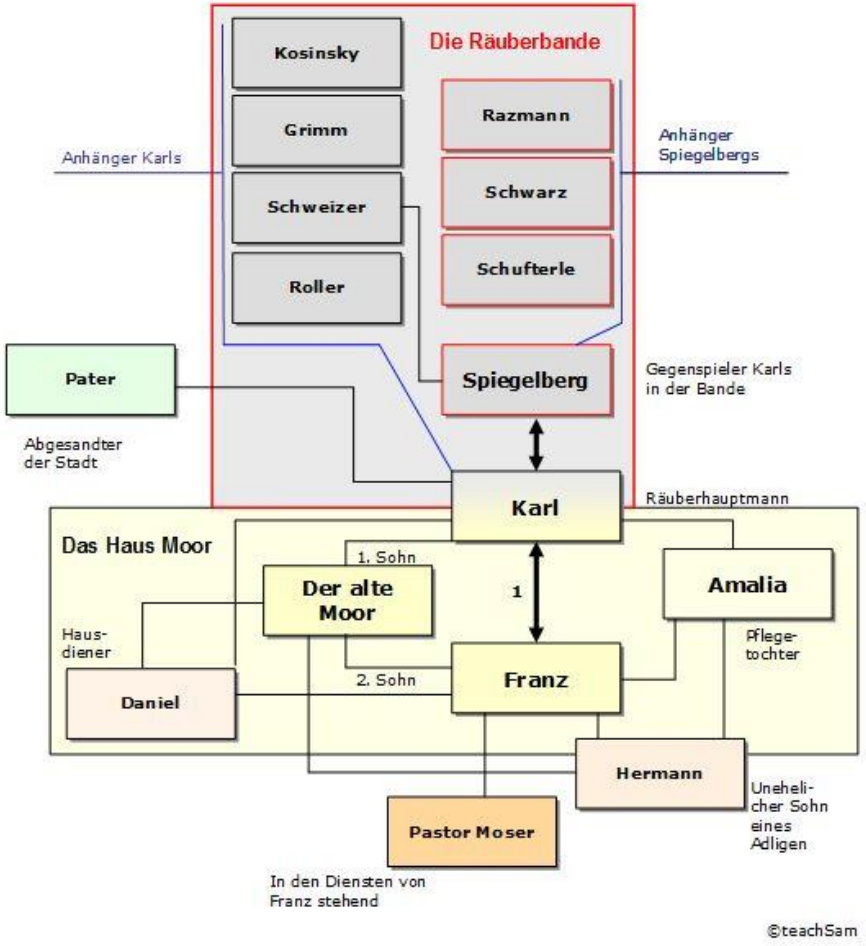
- **Logische Evolution im Angriffsvektor**
  - Vom Einzeltäter zu organisierten hoch-spezialisierten Gruppen

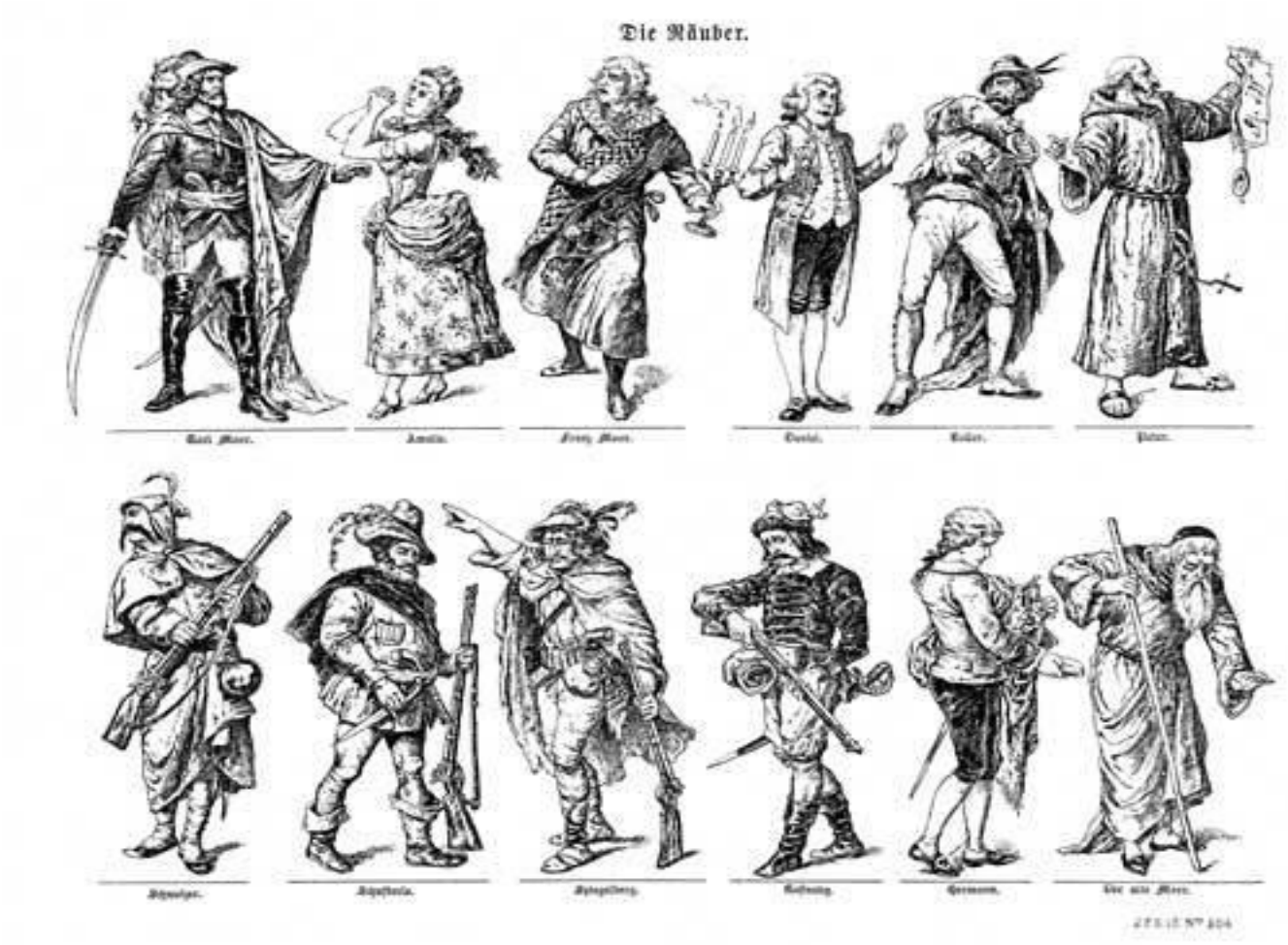
- **Hochkomplexe Nachfrage/Angebot Situation**
  - Fast jeder Bedarf kann “befriedigt” werden

- **Hochspezialisiertes KnowHow**
  - Global agierende Angreifer verfügen über ausreichen KnowHow

Hochentwickelte Angriffsinfrastrukturen sind für jederman zugänglich !

Hochgradig - Arbeitsteilig Organisiert





Crime as a Service - CaaS

Produkt/Service

Bereitstellung von Bots/Botnetzen
Dos / DDoS-Attacken
Malware-Herstellung on Demand und Verteilung
Daten/Identitätsdiebstahl
Verkauf/Angebot sensibler Daten, z. B. Zugangs- oder Zahlungsdaten,
Logistik (Finanz- oder Warenagenten)
Simulatoren/Trainingsplattformen,
Anonymisierungs- und Hostingdienste
Safe Dropzones
etc

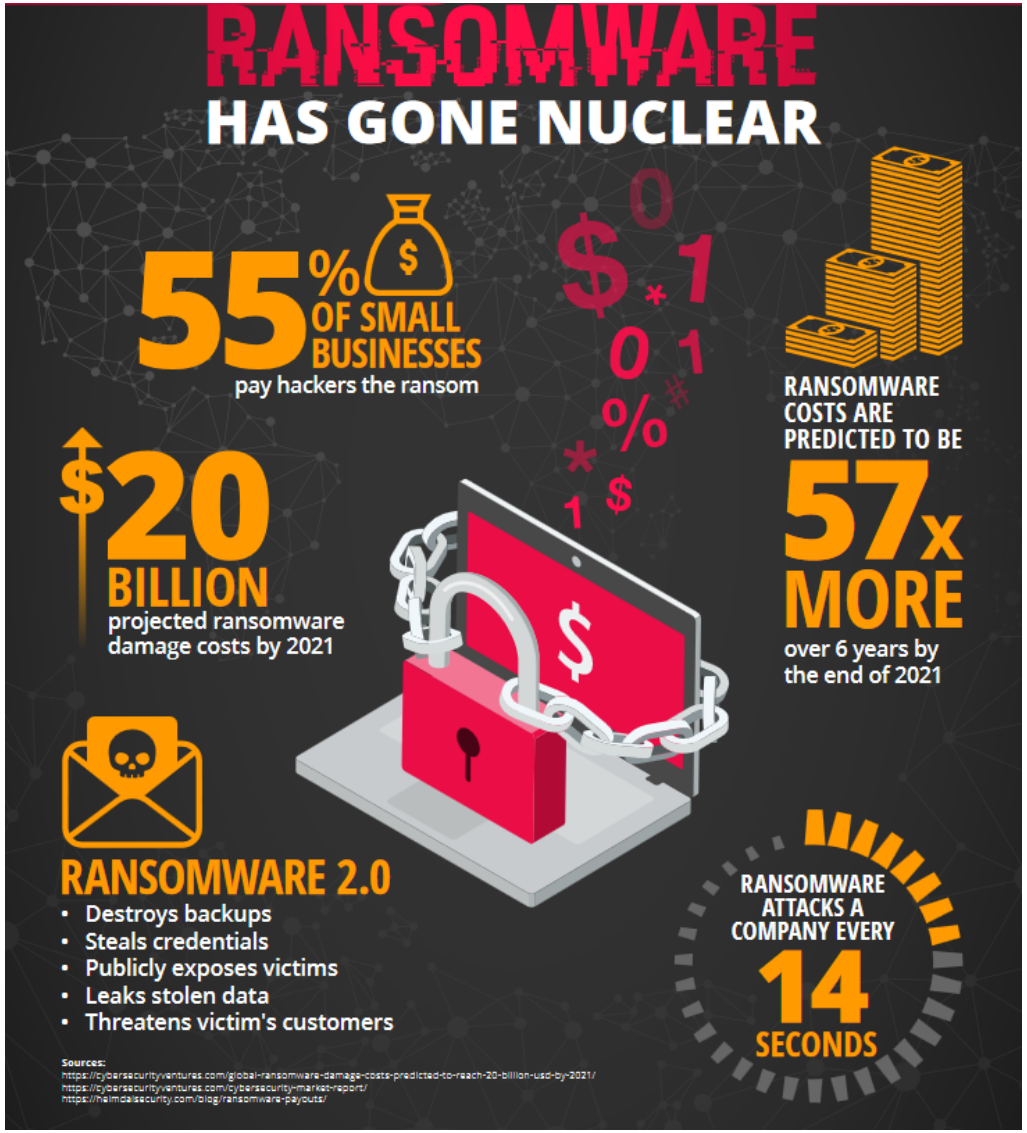
SLA /Wartungsvertrag

Updates von Schadsoftware,
Beratungsdienste
Anti-Erkennungsmechanismen,
Hilfestellung bei technischen Problemen
Ausgelagerter „Kunden“Support
„Infection on Demand“
Trainings
Identitäten
etc

Ransomware

Ransom zahlt sich aus…

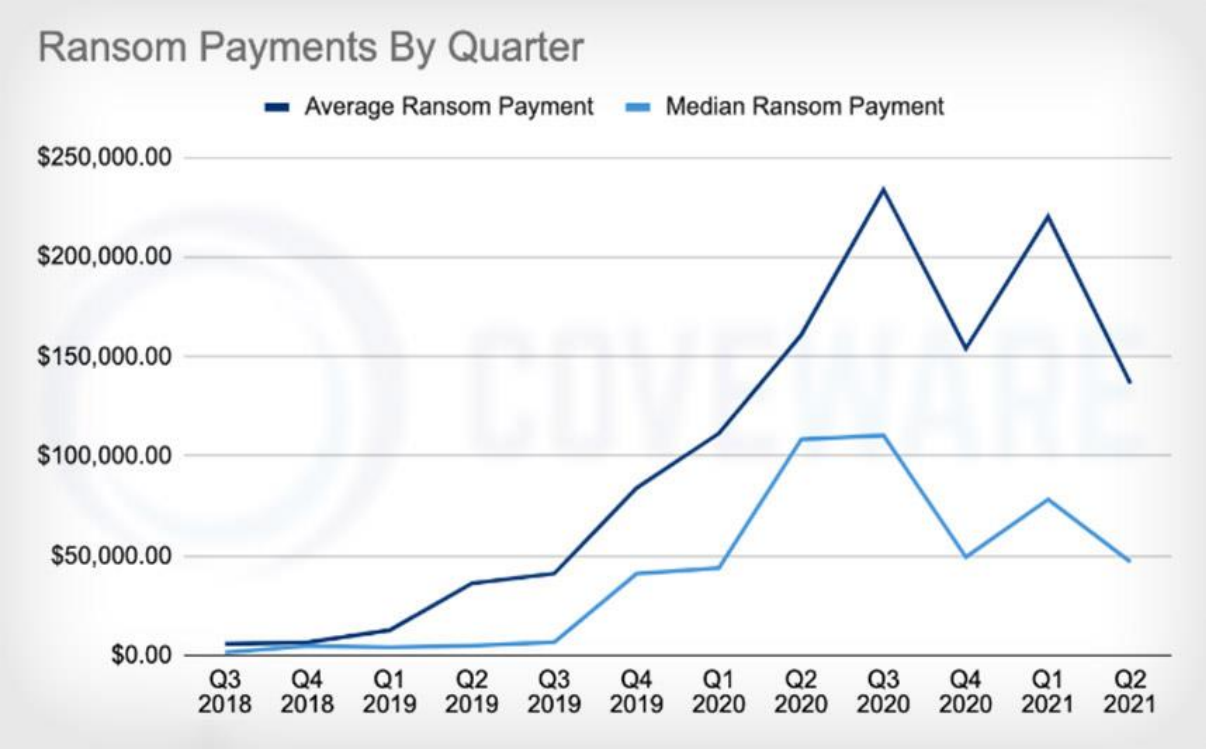
Durschnittlich bezahlten Lösegeld stark gestiegen da immer mehr grosse Unternehmen erfolgreich angegriffen werden



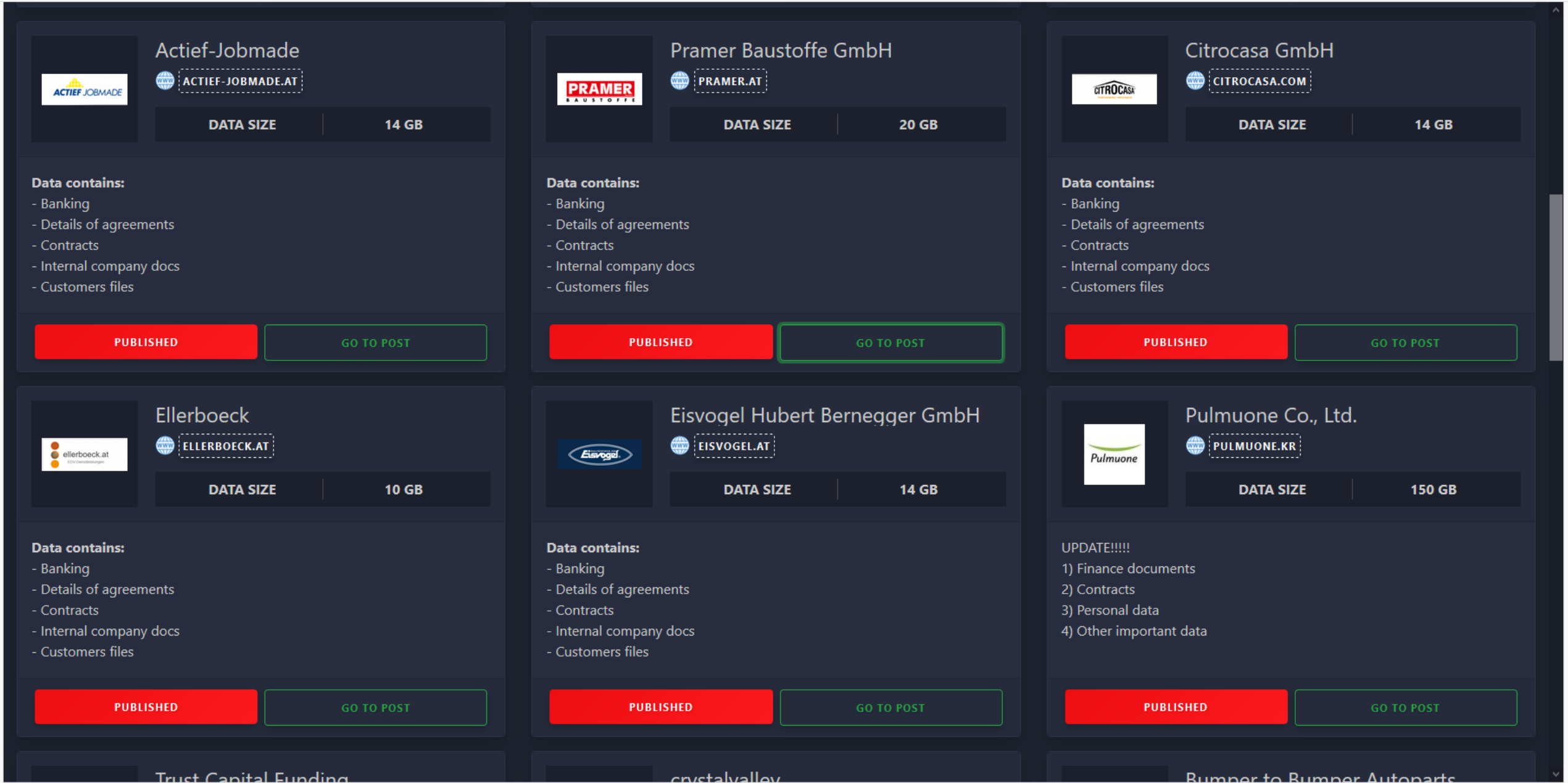
Durchschnittliche Zahlungen

$ 233,817

+31% gegenüber Q2 2020



Österreich natürlich mit dabei..



Salzburg Milch_

URL

https://www.milch.com/en/

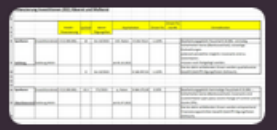
Details_

The company appointed by the negotiator was not interested in resolving the situation and was stalling the time. Our support still online but there's no response from company.

SalzburgMilch GmbH is located in Salzburg, Salzburg, Austria and is part of the Dairy Products Manufacturing Industry. SalzburgMilch GmbH has 359 employees at this location and generates $253.26 million in sales (USD). There are 4 companies in the SalzburgMilch GmbH corporate family.

Images:_






Example files:_

Banken.zip (34758Kb)
Clientsicherung.zip (34013Kb)
Intrastat.zip (53825Kb)
Misc.zip (111809Kb)
Steiner Josef.zip (285593Kb)

6/23/2021, 1:09:45 PM

Hello

We have received your claim. It is posssible for us to make a payment in the amount demanded. It exceeds our financial possibilities. We are a small producing company for dairy products. With our 370 employees we provide only a small part of the basic supply for the population in Salzburg. Furthermore we need a proof that you can decode the data again.

6/23/2021, 2:07:55 PM

Make a ZIP containing few pairs of files you want to decrypt. For exapmple: PATCHES.txt.payOrgrief + PATCHES.txt.iwant2survive.html and Geometry.pdf.payOrgrief + Geometry.pdf.iwant2survive.html and attach this ZIP here. Size is limited to 5Mb. Files should be anything we able to check it's content (photo, office documents, etc).

Here two file for decytion

6/29/2021, 3:01:59 PM

Ok, how much time do you need to make the first payment?

6/30/2021, 3:33:56 PM

Very strange that this simple question become so hard. Looks like you not interested in cooperation with us? So we have to publish your data in next couple of hours?

7/1/2021, 2:41:53 PM

Because you keep silence your data is published. Say thanks to your negotiators.
http://griefcameifmv4hfr3auozmovz5yi6m3h3dwbuqw7baomfxoxz4qteid.onion/details/authentic-a68bcf1a46aecaccd03645ba4daa02cc

6/24/2021, 8:37:42 AM

Are you ignoring the instructions? Read again. Make a ZIP containing few PAIRS of files you want to decrypt. For example: PATCHES.txt.payOrgrief + PATCHES.txt.iwant2survive.html and Geometry.pdf.payOrgrief + Geometry.pdf.iwant2survive.html and attach this ZIP here. Size is limited to 5Mb. Files should be anything we able to check it's content (photo, office documents, etc).

6/24/2021, 3:26:16 PM

This data is for example. Tomorrow we will publish the first portions of the data on our website for public access.

Wie entscheiden Ransomware-Hacker, wie viel Lösegeld verlangt wird ?

- „open intelligence“ – Finanzielle Lage / Zugang zu internen Finanzdaten
- Kritikalität des Geschäftsfortganges
- die Sensibilität der verschlüsselten / gestohlenen Daten
- Welche Systeme und Daten / in welchem Umfang / in welcher Branche betroffen
- Reife- und Technologiegrad auf Seiten der Erpresser
- Bekanntheitsgrad und Medieninteresse
- Manchmal völlig willkürlich oder weil selbst unter Zeitdruck

Was bedeutet das für MICH?

Wenn sie erst darüber nachdenken wenn es passiert ist…..
sind sie zwar in guter Gesellschaft – aber das kostet !

Sie können eine Ransomattacke NICHT verhindern

Aber sie können verhindern, dass sie Erfolgreich ist
oder zumindest den Schaden minimieren!!

Vertrauen sie NICHT auf ihr Verhandlungstalent !!

Aus der Praxis

Wie schützen Sie ihr Unternehmen gegen Ransomware?

Infizierte Backups sind nutzlos

1. Verhindern Sie, dass User Malware (Ramsomware) auf Clients (inkl. Mobiles) herunterladen.

   Spam, Phising und URL Filter, Anti Malware udn Endpoint Protection, Awareness Trainings.

2. Setzen Sie Maßnahmen gegen das Verbreiten von Malware im lokalen Netzwerk und ihren Cloudspeichern (inkl. Hochladen und Syncen).

   Anti Mailware und Endpoint Protection, Intrusion Prevention Systeme mit Cyber Threat Intelligence, Segmentierung

3. Etablieren Sie eine 3-2-1 Backup Strategie.

   Original File - Kopie Onsite auf Backup Medium verschlüsselt - Offsite Kopie verschlüsselt

4. Prüfen Sie laufend ihre Backups auf Malware.

   Anti Mailware

5. Testen Sie laufend ihre Recovery Prozesse.

6. Seien Sie auf den Ransomware Notfall vorbereitet inkl. Meldung bei möglichen Datenverlusten bei der Datenschutzbehörde.

7. Klassifizieren Sie ihre Daten nach Geheimhaltung-, Integritäts- und Verfügbarkeitsanforderungen.

8. Binden Sie ihre IT Dienstleister und Versicherungen in ihre Anti Ransomware Strategie ein.

9. Schliessen Sie mit ihren bevorzugten Managed Security Service Provider eine Servicevereinbarung zu Incident Response mit kurzen Reaktionszeiten ab.

Was tun wenn´s doch passiert ?

Bewahren Sie Ruhe

Suchen sie SOFORT professionelle Hilfe wenn Sie NICHT

über eigene Ressourcen verfügen
die das Problem erfassen
und die richtigen Maßnahmen einleiten können.

IKARUS security software

CYBER SECURITY AUSTRIA

CyberSecurity

– res publica –

ES geht uns alle an!

www.cybersecurityaustria.at

Vielen DANK

und Kopf hoch

Joe Pichlmayr, CEO Ikarus, Vorstand CybersecurityAustria, joe@ikarus.at