Cyberangriff auf Gemeinden – was tun?

Erfahrungen aus der Stadtgemeinde Korneuburg

26.08.2024

Stadtamtsdirektor
Mag. Christian Wieser, MBA

Was ist passiert? (1)

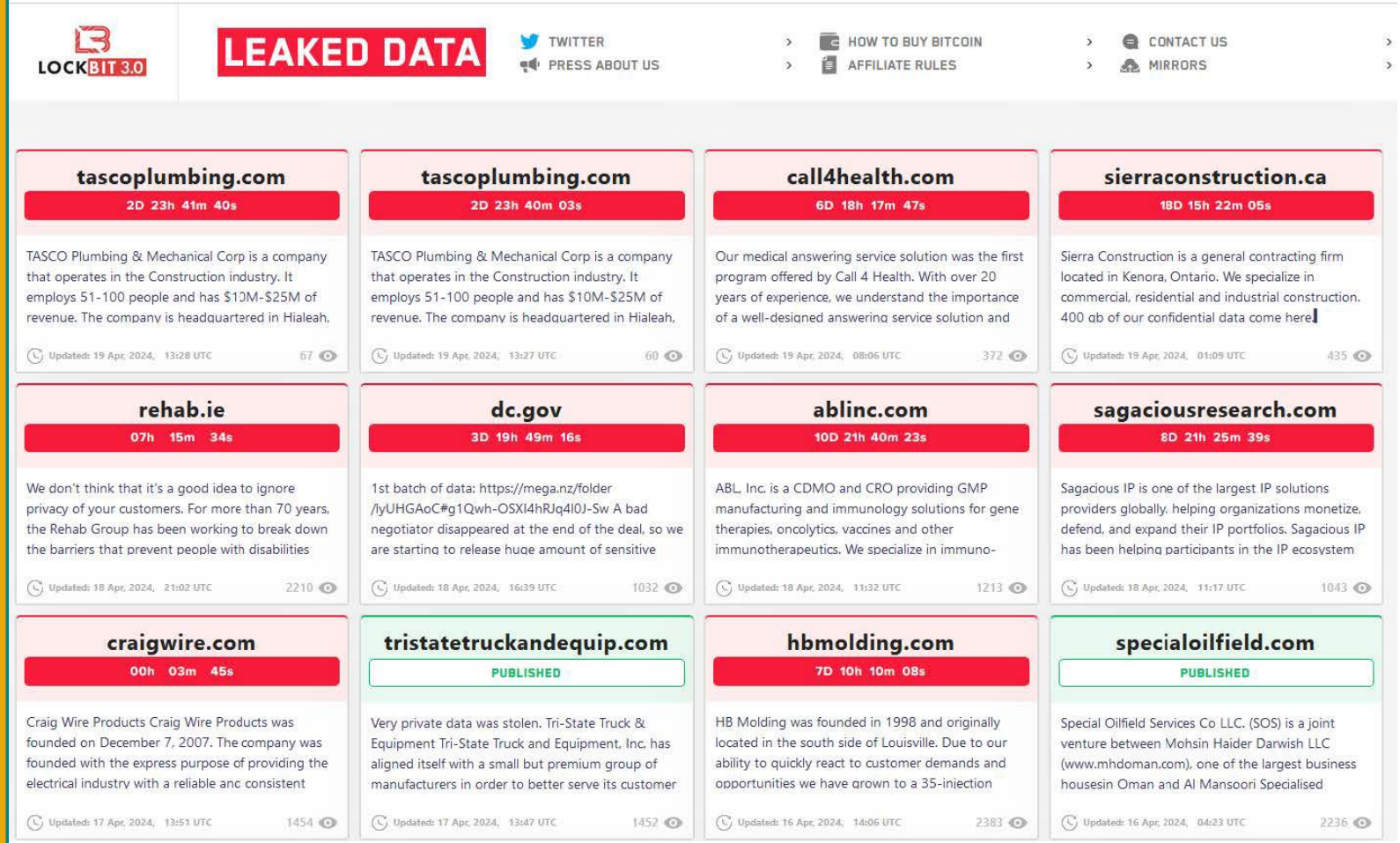
- Hackergruppe drang in unser System ein und „schaute“ sich ab Freitag (02.02.) Nachmittag im EDV-System der Stadt um

- Entschlüsselung des Passworts „print“ binnen 6 Stunden und durch weitere brute-force-Angriffe Zugang zu weiteren Konten erlangt.

- IT-Health check (Dezember zuvor) hatte uns ein gutes Zeugnis ausgestellt
  TROTZDEM:
  Verschlüsselung der Daten auf allen Servern und allen online gewesenen Geräten (Laptops, Drucker) in der Nacht von Montag auf Dienstag (05.-06.02.)

Was ist passiert? (2)

(Symbolbild)

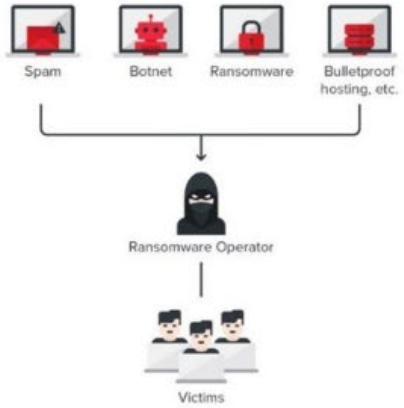

LOCKBIT 3.0
LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
tascoplumbing.com
2D 23h 41m 40s
TASCO Plumbing & Mechanical Corp is a company that operates in the Construction industry. It employs 51-100 people and has $10M-$25M of revenue. The company is headquartered in Hialeah,
Updated: 19 Apr, 2024, 13:28 UTC
67
tascoplumbing.com
2D 23h 40m 03s
TASCO Plumbing & Mechanical Corp is a company that operates in the Construction industry. It employs 51-100 people and has $10M-$25M of revenue. The company is headquartered in Hialeah,
Updated: 19 Apr, 2024, 13:27 UTC
60
call4health.com
6D 18h 17m 47s
Our medical answering service solution was the first program offered by Call 4 Health. With over 20 years of experience, we understand the importance of a well-designed answering service solution and
Updated: 19 Apr, 2024, 08:06 UTC
372
sierraconstruction.ca
18D 15h 22m 05s
Sierra Construction is a general contracting firm located in Kenora, Ontario. We specialize in commercial, residential and industrial construction. 400 gb of our confidential data come here
Updated: 19 Apr, 2024, 01:09 UTC
435
rehab.ie
07h 15m 34s
We don't think that it's a good idea to ignore privacy of your customers. For more than 70 years, the Rehab Group has been working to break down the barriers that prevent people with disabilities
Updated: 18 Apr, 2024, 21:02 UTC
2210
dc.gov
3D 19h 49m 16s
1st batch of data: https://mega.nz/folder /lyUHGAoC#g1Qwh-OSXl4hRJq4l0J-Sw A bad negotiator disappeared at the end of the deal, so we are starting to release huge amount of sensitive
Updated: 18 Apr, 2024, 16:39 UTC
1032
ablinc.com
10D 21h 40m 23s
ABL, Inc. is a CDMO and CRO providing GMP manufacturing and immunology solutions for gene therapies, oncolytics, vaccines and other immunotherapeutics. We specialize in immuno-
Updated: 18 Apr, 2024, 11:32 UTC
1213
sagaciousresearch.com
8D 21h 25m 39s
Sagacious IP is one of the largest IP solutions providers globally, helping organizations monetize, defend, and expand their IP portfolios. Sagacious IP has been helping participants in the IP ecosystem
Updated: 18 Apr, 2024, 11:17 UTC
1043
craigwire.com
00h 03m 45s
Craig Wire Products Craig Wire Products was founded on December 7, 2007. The company was founded with the express purpose of providing the electrical industry with a reliable anc consistent
Updated: 17 Apr, 2024, 13:51 UTC
1454
tristatetruckandequip.com
PUBLISHED
Very private data was stolen. Tri-State Truck & Equipment Tri-State Truck and Equipment, Inc. has aligned itself with a small but premium group of manufacturers in order to better serve its customer
Updated: 17 Apr, 2024, 13:47 UTC
1452
hbmolding.com
7D 10h 10m 08s
HB Molding was founded in 1998 and originally located in the south side of Louisville. Due to our ability to quickly react to customer demands and opportunities we have grown to a 35-injection
Updated: 16 Apr, 2024, 14:06 UTC
2383
specialoilfield.com
PUBLISHED
Special Oilfield Services Co LLC. (SOS) is a joint venture between Mohsin Haider Darwish LLC (www.mhdoman.com), one of the largest business housesin Oman and Al Mansoori Specialised
Updated: 16 Apr, 2024, 04:23 UTC
2236

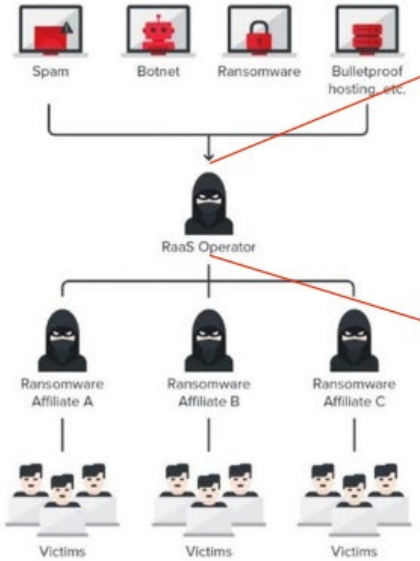
KORNEUBURG

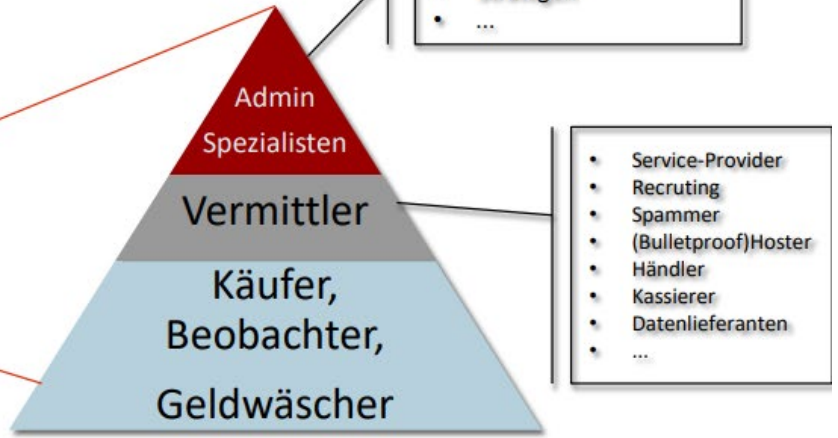
Bundesministerium
Inneres
Bundeskriminalamt

bundeskriminalamt.at

Ransomware - Aufbau



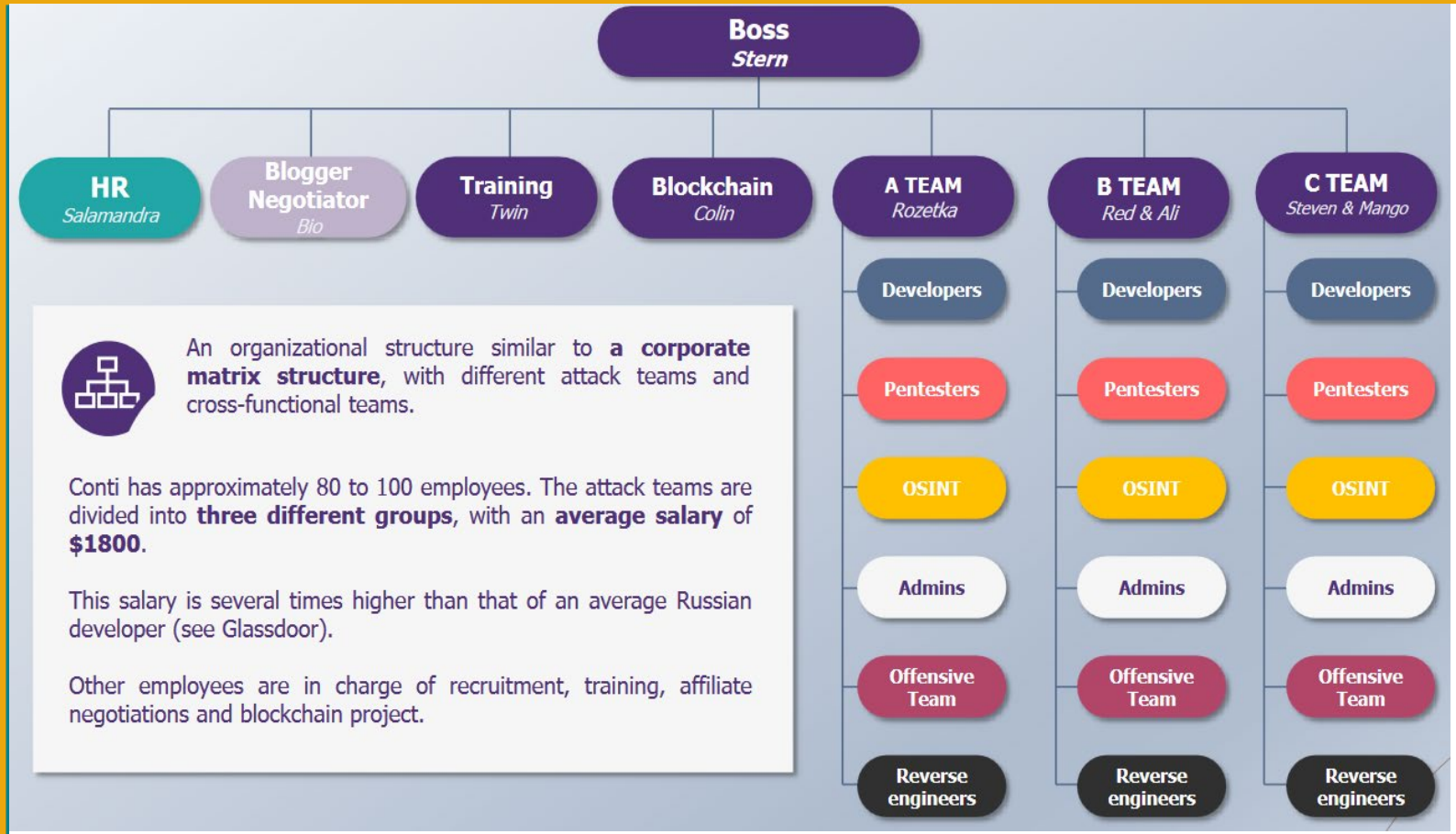




- Forscher/Entwickler
- Malware-Schreiber
- Programmierer
- Technik-Experten
- Strategen
- ...

- Service-Provider
- Recruting
- Spammer
- (Bulletproof)Hoster
- Händler
- Kassierer
- Datenlieferanten
- ...

Quelle: Bundeskriminalamt



Quelle: https://www.riskinsight-wavestone.com/wp-content/uploads/2022/06/Note-de-synthese-groupes-de-ransomware-ANG.pdf

CODERS

In charge of **writing malicious code** by integrating various new technologies.

CRYPTERS

In charge of **making syntactic changes** to payloads, binaries and scripts to **make them more difficult to detect**.

OFFENSIVE TEAM

In charge of obtaining **initial access** to the victims' network, battling against corporate security teams to **steal data**, and **plant ransomware**.

OSINT

In charge of **conducting research** on the **targeted company**.

REVERSE ENGINEERS

In charge of **disassembling** the victims' computer code to study it and **identify vulnerabilities**.

HUMAN RESSOURCES (HR)

In charge of **recruitment** (online interview, profile search, etc.)

SYSADMINS

Responsible **for setting up the attack infrastructure** and provide assistance if needed.

TESTERS

Check various malware against known security solutions to **make sure that they avoid detection**

NEGOTIATION STAFF

In charge of **negotiating ransom** payments and securing a deal with victims.

Quelle: https://www.riskinsight-wavestone.com/wp-content/uploads/2022/06/Note-de-synthese-groupes-de-ransomware-ANG.pdf

KORNEUBURG

Was ist passiert? (3)

- 2 von 3 Sicherungssystemen der Stadt wurden infiziert
  (Magnetbandsicherung (wöchentlich) „rettete“ die Stadt (Datenverlust von 1 Woche) (Jahresabschlusstätigkeiten, STR und GR Vorlagen weg)

- gegen Zahlung von 5,5 Mio € (100 BTC) werden Daten freigegeben

- es dauerte ca. 1 Tag, bis wir realisierten, was passiert war –
  fact-finding gemeinsam mit externer EDV-Firma (Schadensumfang? Was funktioniert noch? Was sind die nächsten Schritte?)

- Meldung an die Datenschutzbehörde ! (Art 33 und 34 DSGVO)

Was haben wir gemacht?

- Meldung an die Datenschutzbehörde ! (Art 33 und 34 DSGVO)
  und an die örtliche Polizeidienststelle – diese löste eine vorgegebene Meldekette aus (govCERT.gv.at., BMI.BK, BMI.LSE, BMLV)

- rasche interne Info an Bedienstete und Gemeinderäte

- behelfsmäßige Nutzung von Notfall-Laptops und privaten Geräten,
  sowie einer mechanischen Schreibmaschine

- Einrichten einer internen Krisenstelle und regelmäßige Info an die Medien - Kompetenzkonflikt (MedienSTR und VBM)

KOR NEU BURG

Medienarbeit

- GANZ WICHTIG: Jedes Wort mit Bedacht wählen!

- erste Presseaussendung – Erwähnung, dass aktuell keine Beurkundungen von Sterbefällen ausgestellt werden können

- Ergebnis in den Medien:
  „Es mussten sogar Begräbnisse verschoben werden!“

  Diese Information war nicht richtig, aber hielt sich über Monate und wurde von anderen Medien aufgenommen und wiedergegeben.

CYBERANGRIFF

Erpresser legen Korneuburger Rathaus lahm

ERSTELLT AM 07. FEBRUAR 2024 | 16:30 NÖN

Cyberangriff in NÖ: Spuren führen nach Moskau

Tätergruppe "Lockbit" mutmaßliche Urheber

Salzburg24.at (21.02.2024)

Cyberangriffe auf Korneuburg und Therme Laa

Das gesamte Bürgerservice von Korneuburg ist durch einen Hackerangriff lahmgelegt worden: Sämtliche Anfragen müssen derzeit handschriftlich bearbeitet werden. Auch die Therme Laa in Laa a. d. Thaya (Bezirk Mistelbach) ist von einem Cyberangriff betroffen.

8. Februar 2024, 17.44 Uhr ORF.at

Schlag gegen die gefährlichsten Hacker der Welt: Mehrere „Lockbit“-Mitglieder festgenommen

Tiroler Tageszeitung 21.02.2024

„Es wird dauern“: Korneuburg arbeitet an Wiederherstellung der Daten

ERSTELLT AM 13. FEBRUAR 2024 | 09:00 NÖN

Als Korneuburg auf eine Schreibmaschine angewiesen war

PROFIL 16.03.2024

KOR NEU BURG

Auswirkungen (1)

- 97 Clients (PC und Laptops) und 52 Server waren betroffen und mussten neu aufgesetzt werden

- Datenverlust – letzte 5 Tage vor dem Angriff (Datenrückspielung seit letztem Magnetband-backup vom 27.01.)

- Unmittelbarer finanzieller Schaden „nur“ rd. 100.000 € (ca. 600 Stunden durch externe IT-Firma) - größtenteils konnte eigene IT-Geschäftsstelle Wiederherstellungsarbeiten erledigen.

- Normalbetrieb ab 23.02. wieder möglich

Auswirkungen (2)

- Neuanschaffung zusätzlicher hardware (zusätzl. rd. 68.000 €)

- Erweiterte Dienstleistungen (zusätzliche ca. 15.000 € (Servicepaket, Lizenzkosten)

- neues Sicherheitskonzept: (Passwortkomplexität, 2-Wege-Anmeldung, Geoblocking, Monitoring-software, Schulungen, Sicherheitsüberprüfung usw.)

- keine Datenexfiltration! Aufgrund eines europaweit angelegten Schlages gelang es Mitte Februar Lockbit zu zerschlagen und einige Hintermänner zu verhaften (Hinweis auf „affiliates“)

Quelle: Bundeskriminalamt

Dauer für Brute-Force-Attacken

		Nur Zahlen	Kleinbuchstaben	Gross- und Kleinbuchstaben	Gross-, Kleinbuchstaben und Zahlen	Alle Symbole auf der Tastatur
Beispiele		1234	ameisen	QrtM	F3P9mN	z&M@P#3
Mögliche Zeichen		10	26	52	62	95
Zeichenzahl	4	0,3 Millisekunden	15 Millisekunden	24 Millisekunden	490 Millisekunden	2,7 Sekunden
Länge des Kennworts	5	3 Millisekunden	400 Millisekunden	13 Sekunden	31 Sekunden	4,3 Minuten
	6	33 Millisekunden	10 Sekunden	11 Minuten	32 Minuten	6,8 Stunden
	7	330 Millisekunden	4,5 Minuten	9,5 Stunden	33 Stunden	27 Tage
	8	3,3 Sekunden	1,9 Stunden	21 Tage	84 Tage	7 Jahre
	9	33 Sekunden	2,1 Tage	2,9 Jahre	14 Jahre	670 Jahre
	10	5,6 Minuten	54 Tage	150 Jahre	890 Jahre	$6{,}3 \times 10^4$ Jahre
	11	56 Minuten	3,9 Jahre	$7{,}9 \times 10^3$ Jahre	$5{,}5 \times 10^4$ Jahre	6×10^6 Jahre
	12	9,3 Stunden	100 Jahre	$4{,}1 \times 10^5$ Jahre	$3{,}4 \times 10^6$ Jahre	$5{,}7 \times 10^8$ Jahre
	13	3,9 Tage	$2{,}6 \times 10^3$ Jahre	$2{,}1 \times 10^7$ Jahre	$2{,}1 \times 10^8$ Jahre	$5{,}4 \times 10^{10}$ Jahre
	14	39 Tage	$6{,}8 \times 10^4$ Jahre	$1{,}1 \times 10^9$ Jahre	$1{,}3 \times 10^{10}$ Jahre	$5{,}1 \times 10^{12}$ Jahre
	15	1,1 Jahre	$1{,}8 \times 10^6$ Jahre	$5{,}8 \times 10^{10}$ Jahre	$8{,}1 \times 10^{11}$ Jahre	$4{,}9 \times 10^{14}$ Jahre
	16	11 Jahre	$4{,}6 \times 10^7$ Jahre	3×10^{12} Jahre	5×10^{13} Jahre	$4{,}7 \times 10^{16}$ Jahre

Quelle: Bundeskriminalamt

Lessons learned - Empfehlungen für die Praxis (1)

- Keine Organisation und kein IT-System ist vor Angriffen gefeit
- Angriffe erfolgen selten gezielt, sondern oftmals „zufällig“ (affiliates)
- Im Falle des Falles - Ruhe bewahren (professionell vorgehen – sowohl seitens Verwaltung als auch Politik)
- Meldung an DSB und Polizei (Meldekette auslösen) und mit Behörden kooperieren (Negativbeispiel Land Kärnten)

Lessons learned - Empfehlungen für die Praxis (2)

- möglichst rasch professionelle IT-Hilfe anfordern (eher nicht auf 1-2 Bedienstete-Unternehmen setzen)

- Medienarbeit nicht unterschätzen (insbes. soziale Medien) – daher aktiv betreuen (nicht zu viel – nicht zu wenig)

- Anmeldedaten und Zugriffsrechte ändern, Webseite auf Wartungsmodus stellen, Logfiles der Webseite überprüfen, Bedienstete jährlich schulen, fake phishing mails versenden um Bedienstete zu sensibilisieren, usw.

- Links zur Erkennung von Schadsoftware finden sich im Internet.

Dankeschön!

Für Fragen stehe ich Ihnen gerne zur Verfügung.
christian.wieser@korneuburg.gv.at