CYBER-SICHERHEIT NOTFALLPLAN

HANDLUNGSFÄHIG BLEIBEN IM ANGRIFFSFALL

Mag. Angelika Höber

FH CAMPUS 02
Department IT & Wirtschaftsinformatik

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

CYBERANGRIFF NOTFALLPLAN

für Ihr Unternehmen

Technik & Wirtschaft

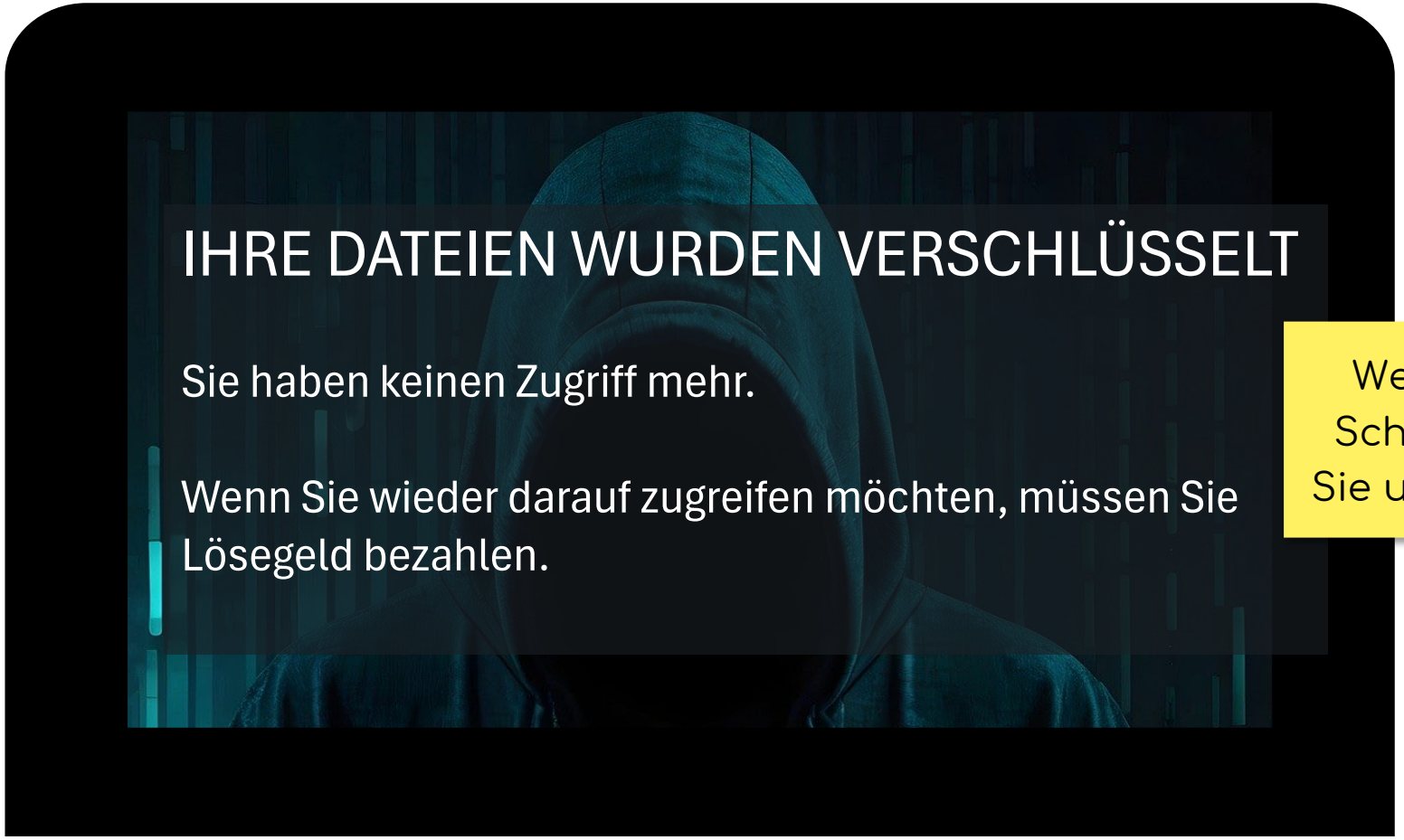
Studieren

Forschen

Department IT & Wirtschafts-informatik

Fortbilden

Ein ganz normaler Tag ….



Welche ersten Schritte würden Sie unternehmen?

GLOBAL THREAT INDEX MAP

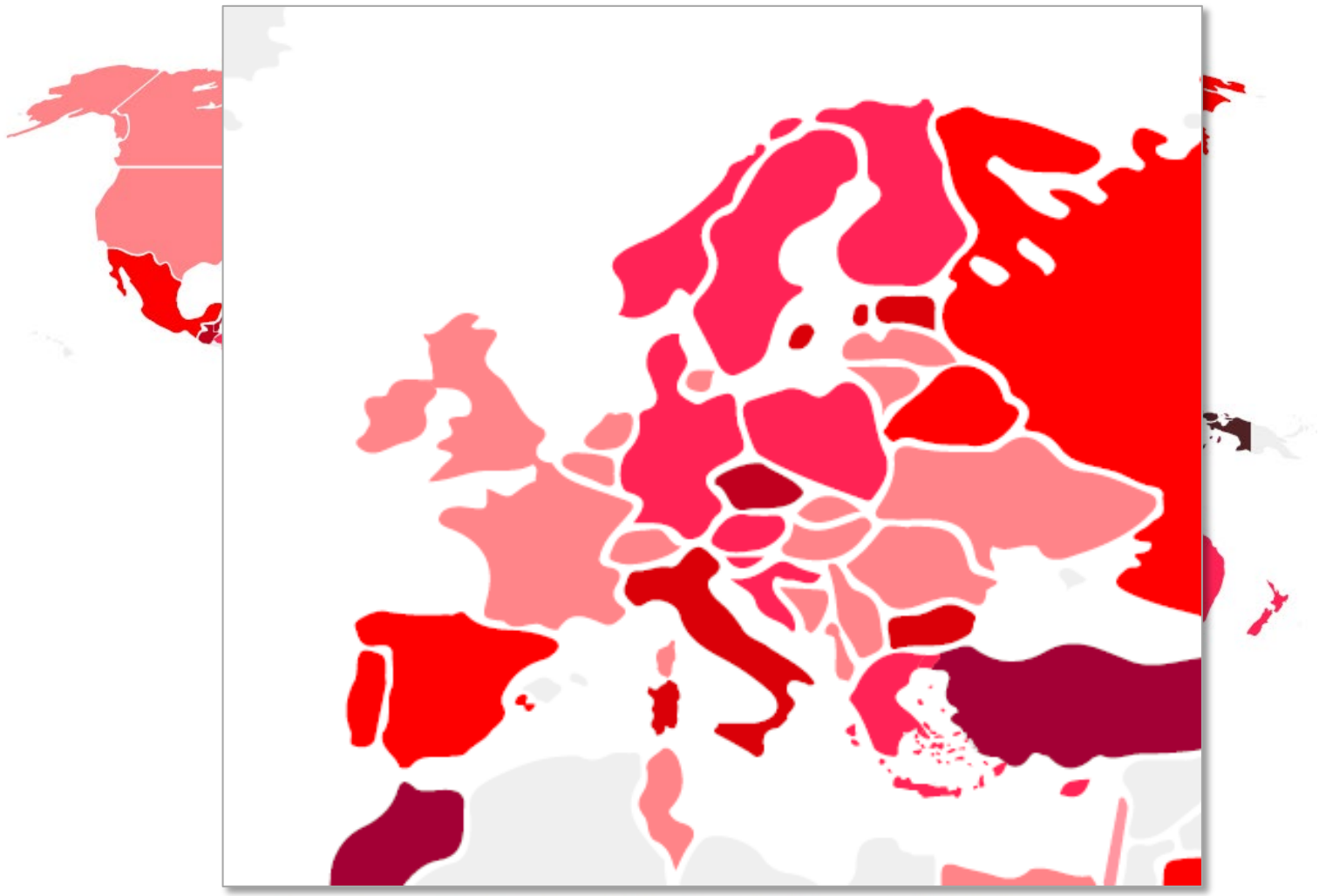


Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.

Check Point, Cyber Security Report, 2025, S. 33

EMEA

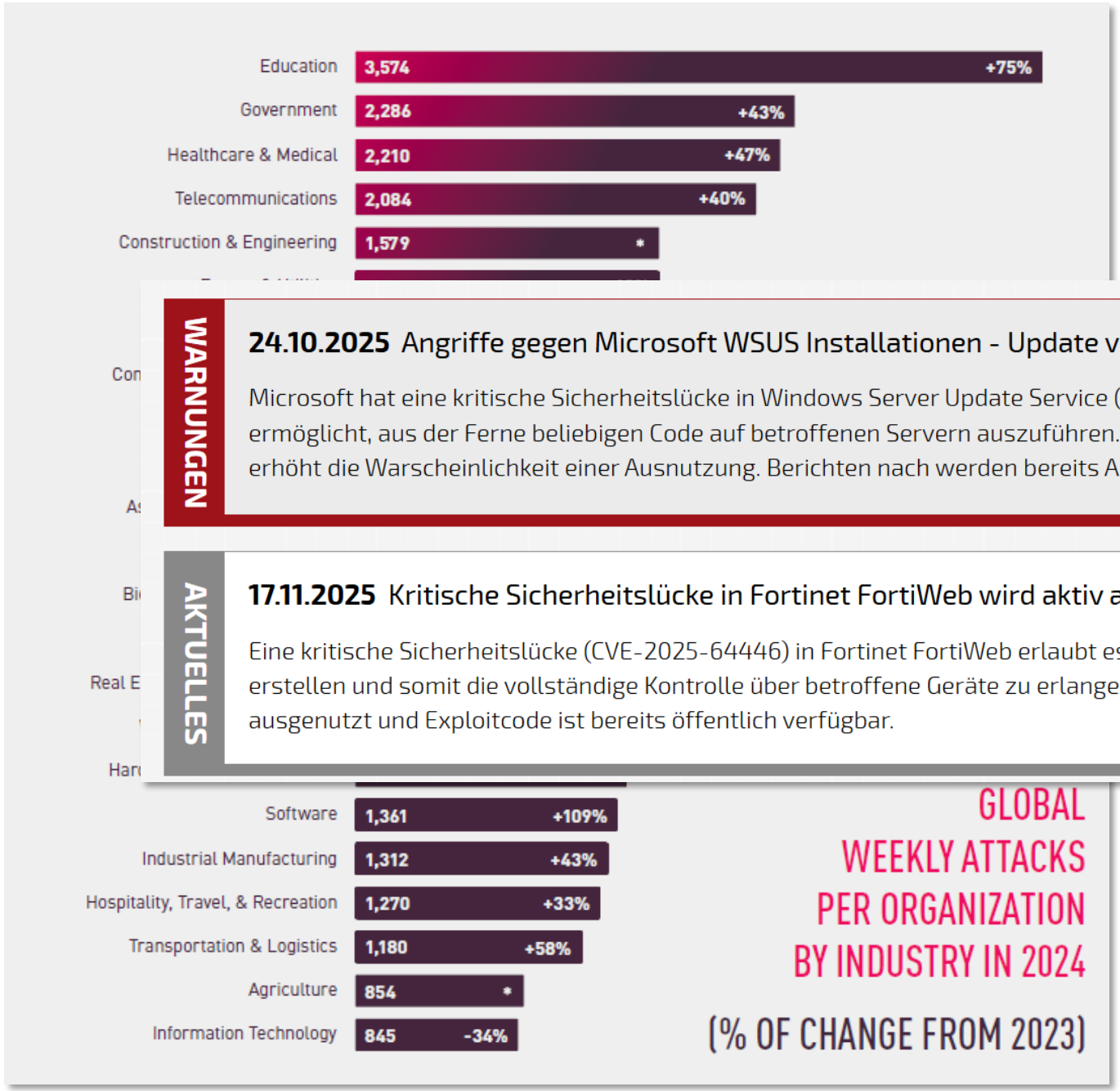
42%	20%	6%	2%
Multipurpose Malware	Infostealer	Mobile	Crypto Miners

58% INCREASE OF INFOSTEALER INFECTION ATTEMPTS IN 2024

DEFINING INFOSTEALERS

Infostealers, often called "stealers", are malware engineered to covertly extract sensitive data from compromised systems, primarily targeting browser data. They can also exfiltrate files from the infected machines and take screenshots. Stealers are spread through phishing emails or malicious downloads. Once they infiltrate a computer, they can harvest a wide range of valuable information that can be used for further cyber crime or fraudulent activities. This includes usernames and passwords, financial details, system configurations, browser cookies, and cryptocurrency wallets. Infostealers are marketed on the Dark Web as Malware-as-a-Service (MaaS), where buyers receive customer support, regular updates, and detailed documentation, lowering the barrier to entry for would-be cyber criminals.

Check Point, Cyber Security Report, 2025, S. 32



WARNUNGEN

24.10.2025 Angriffe gegen Microsoft WSUS Installationen - Update verfügbar

Microsoft hat eine kritische Sicherheitslücke in Windows Server Update Service (WSUS) veröffentlicht, die es unauthentifizierten Angreifern ermöglicht, aus der Ferne beliebigen Code auf betroffenen Servern auszuführen. Ein bereits öffentlich verfügbarer Proof-of-Concept (PoC) Exploit erhöht die Warscheinlichkeit einer Ausnutzung. Berichten nach werden bereits Angriffe verzeichnet.

AKTUELLES

17.11.2025 Kritische Sicherheitslücke in Fortinet FortiWeb wird aktiv ausgenutzt

Eine kritische Sicherheitslücke (CVE-2025-64446) in Fortinet FortiWeb erlaubt es unauthentifizierten Angreifer:innen, eigene Admin-Konten zu erstellen und somit die vollständige Kontrolle über betroffene Geräte zu erlangen. Die Schwachstelle wird mindestens seit dem 6. Oktober 2025 aktiv ausgenutzt und Exploitcode ist bereits öffentlich verfügbar.

https://www.cert.at/de/, 24.11.25

Check Point, Cyber Security Report, 2025, S. 34

Was können Sie tun?

PRÄVENTION

REAKTION

z.B. Check Point, Cyber Security Report
Externe Dienstleister

CYBERANGRIFF NOTFALLPLAN

für Ihr Unternehmen

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

HEUTE
gemeinsam für Situation vorbereiten

NACH DEM WORKSHOP
Notfallplan im Betrieb weiterentwickeln

Was bringt das?

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

handlungsfähig bleiben

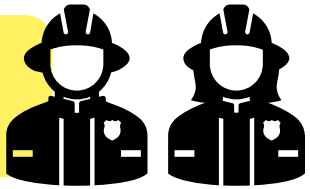
schnell und zielgerichtet reagieren

Auswirkungen eines Angriffs minimieren

Dem Chaos mit organisatorischen Maßnahmen vorbeugen

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- Vorgehensplan



CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse

Was muss täglich laufen?

Der Leitfaden

1. Schritt: **Geschäftsprozesse** absichern

1. Kritische Geschäftsprozesse identifizieren ➡ Liste erstellen und nach Priorität sortieren

Der Leitfaden

1. Schritt: **Geschäftsprozesse** absichern

Arbeitsblatt *Geschäftsprozesse*

Schritt 1 – Zentrale Prozesse benennen

Nr.	*Was sind die zentralen Prozesse in Ihrem Unternehmen?*	*Läuft dies täglich ab?*	*Muss es IMMER laufen können?*
1			
2			
3			
4			

Beispiel:

1	Frischmilchprodukte müssen immer **gekühlt** werden können.	*Ja*	*Ja*

- 6 -

Der Leitfaden

2. Schritt: **Alternative Lösungen** finden

1. Kritische Geschäftsprozesse identifizieren ➡ Liste erstellen und nach Priorität sortieren

2. Alternativen suchen

Der Leitfaden

2. Schritt: **Alternative Lösungen** finden

Schritt 2 – Alternativen finden

Nr.	*Was ist eine mögliche Alternative, wenn der Prozess so nicht laufen kann?*

Beispiel:

1	Partnerunternehmen anfragen, ob diese Kapazitäten haben. Zulieferer anfragen, ob Anlieferung verzögert werden kann.

- 7 -

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

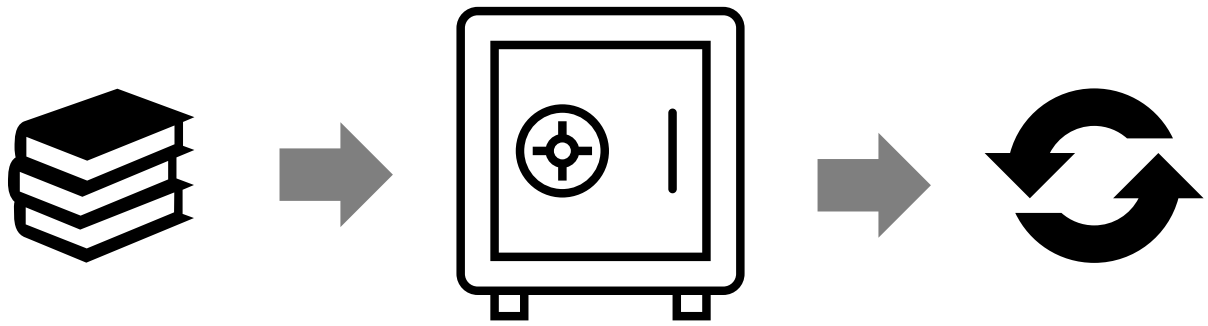
Dokumentation

Auf welche Dokumente muss immer zugegriffen werden können?

Der Leitfaden

Dokumentation offline bereitstellen

- Kontaktdaten, Dokumente, Auftragslisten, Tools, …



Der Leitfaden

1. Schritt: **Wen** müssen wir kontaktieren können?

Arbeitsblatt *Dokumentation* (1/2)

Wen müssen sie immer kontaktieren können (z.B. IT-Firma, Zulieferer, Kund*innen, ...)

Wen	*Wofür*

Beispiel:

Milchlieferanten	Änderung Anlieferungszeiten/-modalitäten

- 9 -

Der Leitfaden

2. Schritt: **Welche Dateien** müssen immer da sein?

Arbeitsblatt *Dokumentation* (2/2)

Welche Informationen müssen immer verfügbar sein (z.B. Wochenplan, Notfallhandbuch, ...)

Dokument	*Wo soll dieses abgelegt werden?*	*Wie oft soll es aktualisiert werden?*	*Wer macht das?*	*Allfällige Anmerkungen*

Beispiel:

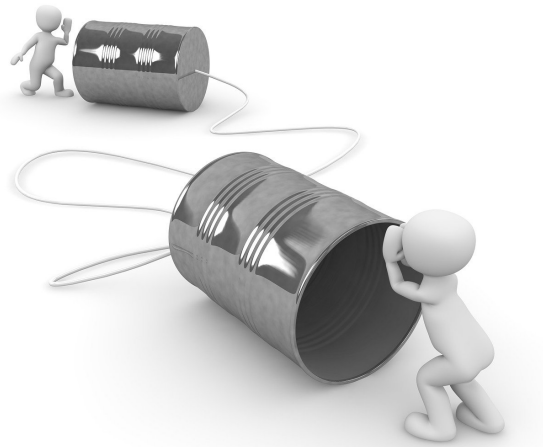
Lieferantenliste mit Namen, Telefonnummern	Büro, Safe	Halbjährlich (1.12., 1.6.)	Frau Huber	Unbedingt auch Handynummern für Erreichbarkeit im Notfall!

- 10 -

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

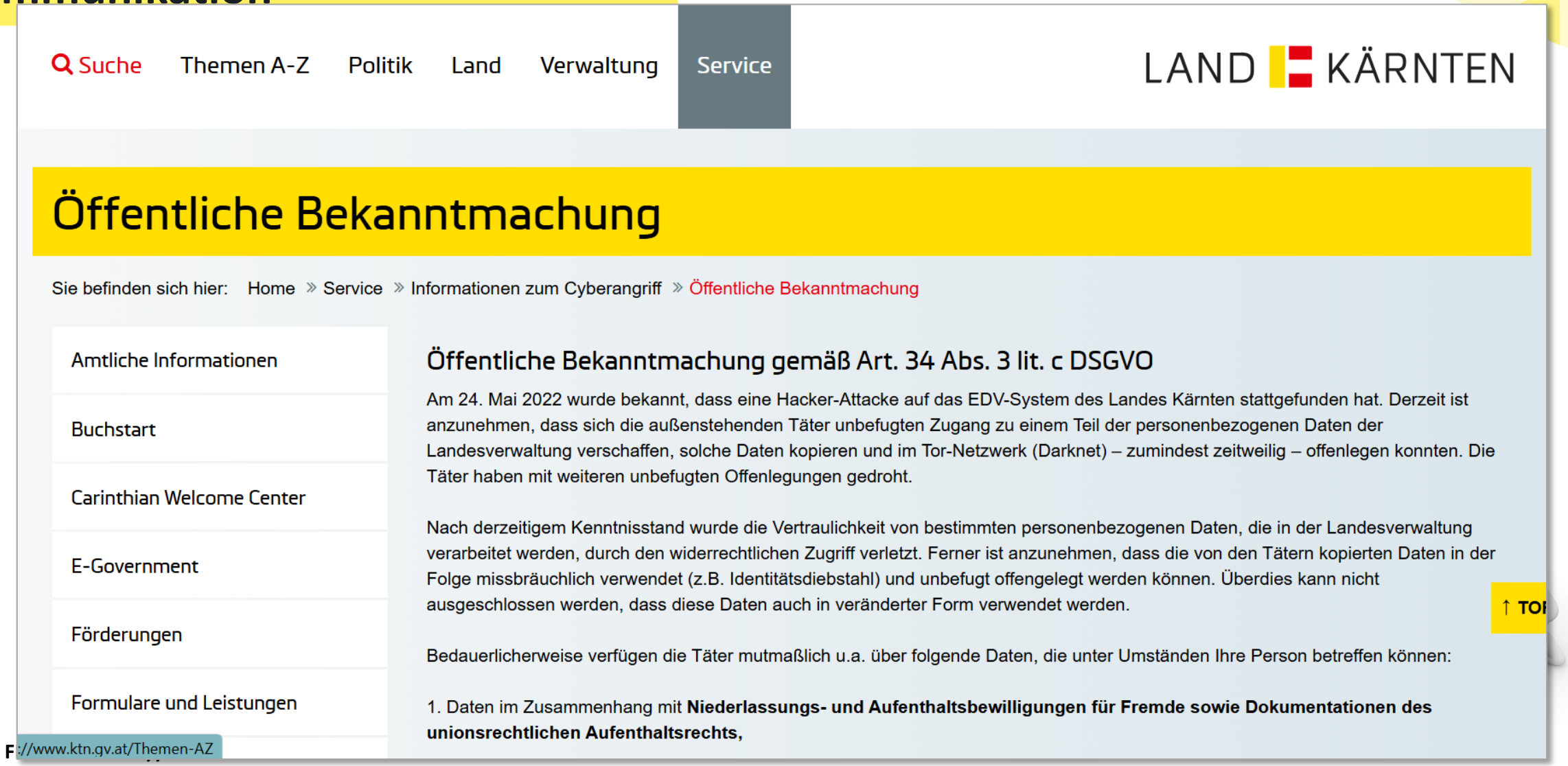
Kommunikation

Wie wird kommuniziert?
Was wird kommuniziert?
Mit wem?



Der Leitfaden

Kommunikation



Suche Themen A-Z Politik Land Verwaltung Service

LAND KÄRNTEN

Öffentliche Bekanntmachung

Sie befinden sich hier: Home » Service » Informationen zum Cyberangriff » Öffentliche Bekanntmachung

- Amtliche Informationen
- Buchstart
- Carinthian Welcome Center
- E-Government
- Förderungen
- Formulare und Leistungen

Öffentliche Bekanntmachung gemäß Art. 34 Abs. 3 lit. c DSGVO

Am 24. Mai 2022 wurde bekannt, dass eine Hacker-Attacke auf das EDV-System des Landes Kärnten stattgefunden hat. Derzeit ist anzunehmen, dass sich die außenstehenden Täter unbefugten Zugang zu einem Teil der personenbezogenen Daten der Landesverwaltung verschaffen, solche Daten kopieren und im Tor-Netzwerk (Darknet) – zumindest zeitweilig – offenlegen konnten. Die Täter haben mit weiteren unbefugten Offenlegungen gedroht.

Nach derzeitigem Kenntnisstand wurde die Vertraulichkeit von bestimmten personenbezogenen Daten, die in der Landesverwaltung verarbeitet werden, durch den widerrechtlichen Zugriff verletzt. Ferner ist anzunehmen, dass die von den Tätern kopierten Daten in der Folge missbräuchlich verwendet (z.B. Identitätsdiebstahl) und unbefugt offengelegt werden können. Überdies kann nicht ausgeschlossen werden, dass diese Daten auch in veränderter Form verwendet werden.

↑ TOP

Bedauerlicherweise verfügen die Täter mutmaßlich u.a. über folgende Daten, die unter Umständen Ihre Person betreffen können:

1. Daten im Zusammenhang mit **Niederlassungs- und Aufenthaltsbewilligungen für Fremde sowie Dokumentationen des unionsrechtlichen Aufenthaltsrechts,**

F ://www.ktn.gv.at/Themen-AZ

Der Leitfaden

Kommunikation

Der Leitfaden

Kommunikation

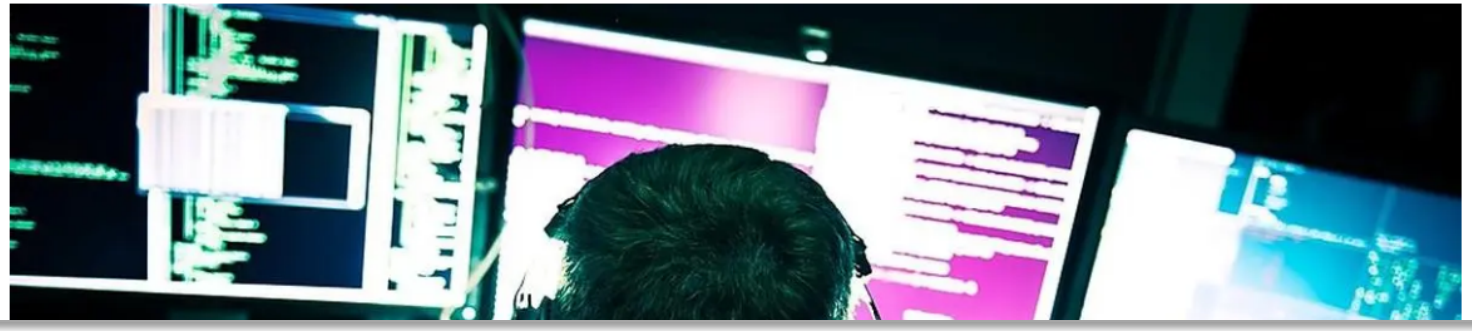
Jakob Illek

4. November 2022,
16:27 Uhr

CYBERATTACKE AUF FELDBACH

Gemeinde arbeitet fieberhaft, wird Lösegeld an Hacker aber nicht bezahlen

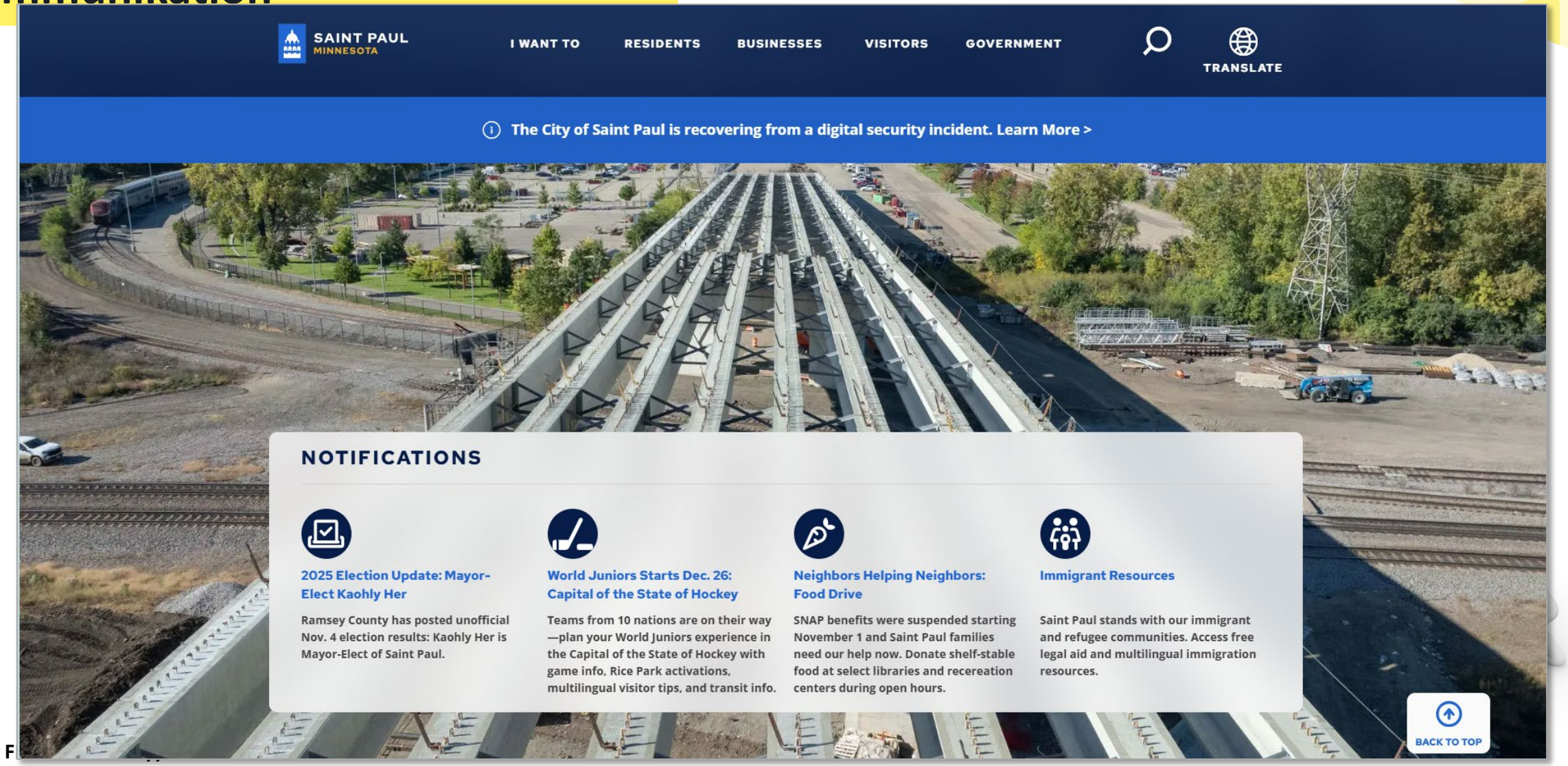
Mit einem Verschlüsselungstrojaner haben Hacker die Stadtgemeinde Feldbach angegriffen. Bis zu 10 Terabyte an Daten auf dem Verwaltungsserver könnten betroffen sein. Dies ist die erste erfolgreiche Attacke auf eine steirische Gemeinde.



Wer hinter dem Angriff steckt und welche Daten betroffen sind, ist noch unklar (Symbolbild)

Der Leitfaden

Kommunikation



Der Leitfaden

Kommunikation

Der Leitfaden

Kommunikation planen

- **Fragen:**
  - Wen rufen Sie ohne ein Telefon oder MS Teams an bzw.*WIE?*
  - Wer darf Informationen weiterleiten?
  - Welche Informationen dürfen wohin?
    - Mitarbeitende, Kunden & Partner, Medien, …

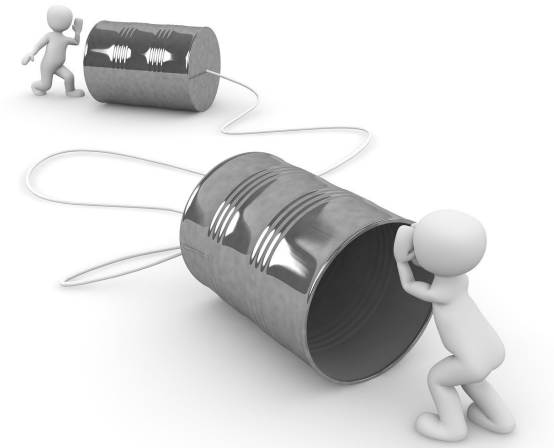
Der Leitfaden

Schritt 1: **Kommunikationswege**

Arbeitsblatt *Kommunikationswege*

Welche Kommunikationswege inkl. technischer Voraussetzungen werden aktuell genutzt und welche Alternativen könnten sie stattdessen nutzen?

Kommunikationsweg	*Technische Voraussetzungen*	*Mögliche Alternativen*



Der Leitfaden

Schritt 2: **Kommunikation** planen

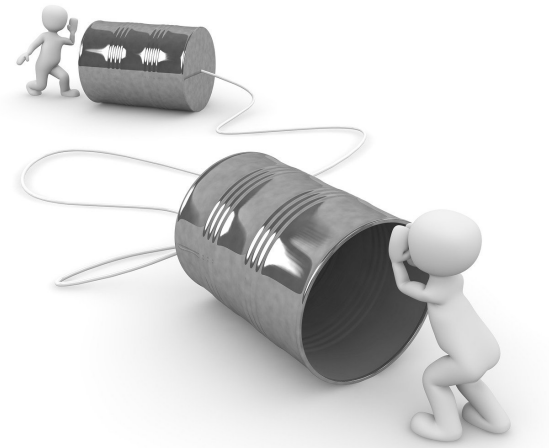
Arbeitsblatt *Kommunikationsplan* *(1/3)*

Erstellen Sie ihre eigenen Vorlagen und Textteile, damit es im Notfall schneller geht und Sie nicht erst nach den richtigen Worten suchen müssen.

Beispiele:

Wann	*Was*	*Wer (von wem?)*	*An wen?*
So schnell als möglich	Liebe Kolleginnen und Kollegen, am dd.mm. um ca. hh:mm ereignete sich eine Cyber Attacke auf unsere IT-Infrastruktur. Im Moment können wir noch nicht abschätzen, was alles betroffen ist, wir halten Sie/euch jedoch auf dem Laufenden. Bis auf weiteres dürfen keine Informationen nach außen gegeben werden (weder an Kunden noch an Freunde oder Verwandte)! Wir bereiten eine offizielle Stellungnahme vor und werden euch diese so schnell als möglich für notwendige Informationsweitergaben zur Verfügung stellen. Vielen Dank! xxx	Personalabteilung	ALLE Mitarbeitenden
So schnell als möglich	Liebe Kundenbetreuende, um unsere Kunden proaktiv zu informieren und etwaigen Unsicherheiten und Gerüchten vorzubeugen, bitten wir euch um Weitergabe folgender Informationen von den jeweiligen Kundenverantwortlichen an unsere Kunden: <xxxx> Vielen Dank! xxx	Geschäftsführung	Kundenbetreuende
So schnell als möglich	Liebe Kolleginnen und Kollegen, um den Wiederherstellungsprozess der IT-Infrastruktur und den aktuellen polizeilichen Ermittlungen nicht zu gefährden, dürfen wir auf Anfrage von extern ausschließlich folgende Informationen weitergegeben werden: <xxxx> Vielen Dank! xxx	Geschäftsführung	Kundenbetreuende, Hotline- bzw. Office-Mitarbeitende

- 15 -



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

FH CAMPUS 02 / Mag. Angelika Höber / Department für IT & Wirtschaftsinformatik

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Notfallteam

Wer wird kontaktiert?
Wer koordiniert?
Wer entscheidet?

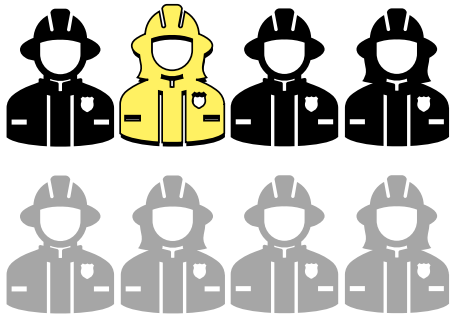
Der Leitfaden

Notfallteam aufstellen

- **Fragen**
  - Wer muss im Angriffsfall sofort Bescheid wissen?
  - Wer koordiniert die weiteren Abläufe?
  - Wer trägt die Verantwortung und entscheidet?

Der Leitfaden

Notfallteam aufstellen



- Krisenstab vorab bilden
- Ersatzmitglieder definieren
- Leitung bestimmen

- *Im Ernstfall:* Notfall-Erstkontakt identifizieren und abholen

Der Leitfaden

Notfallteam aufstellen (intern)

Arbeitsblatt *Mögliches Notfallteam* (1/2)

Haben Sie ein Notfall-Team, das im Ernstfall weiß, was zu tun ist und vor allem wer was zu tun hat? Schreiben Sie hier möglichen auf, die im Ernstfall eingebunden werden können. Besetzen Sie jede Position mit einer möglichen Vertretung. Ziehen Sie diese Liste im Ernstfall heran, um die Aufgaben entsprechend zu verteilen.

Verantwortungsgebiet	*Personen*	*Telefon (Firma, Privat)*
NOTFALL **ERSTKONTAKT** bzw. **Leitung des Krisenstabs** *– ruft das Krisen-Team zusammen und leitet die ersten Schritte ein* *– ist primäre Ansprechperson für alle Fragen* *– (optional) leitet die regelmäßigen Krisen-Team Sitzungen oder benennt eine Person dafür*	Hauptverantwortlich (H):	
	Vertretung (V):	
Rechtliche Themen (z.B. Anzeige bei Polizei, DSGO, NIS, etc.):	H:	
	V:	
Forensik:	H:	
	V:	
Wiederherstellung:	H:	
	V:	
Interne Kommunikation (an Mitarbeitende)	H:	
	V:	
Externe Kommunikation (an Kunden und Presse	H:	
	V:	
Sonstiges	H:	
	V:	

- 20 -

Der Leitfaden

Notfallteam aufstellen (extern)

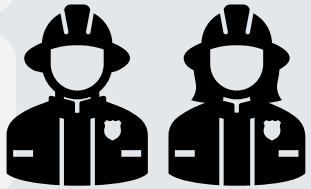
Arbeitsblatt *Mögliche externe Dienstleister* (2/2)

Haben Sie Kontakte zu externen Dienstleistern, die Ihnen im Fall eines Angriffs helfen können? Schreiben Sie hier Ihre Partner-Firmen auf, mit denen Sie bereits in Kontakt sind und die Ihnen im Notfall helfen können:

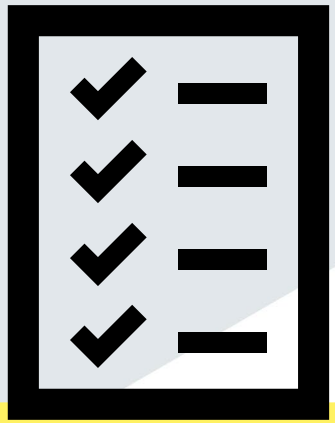
Verantwortungsgebiet	*Firma*	*Kontaktperson (wenn vorhanden), Telefonnummer*
Forensik (um herauszufinden was überhaupt passiert ist)		
Wiederherstellung:		
Arbeitskräfte (zur Hilfe bei der Wiederherstellung)		
Hardware (Notebooks, Internet-Cube, Server, etc.)		
Versicherung		
Sonstiges		

- 21 -

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen



Vorgehensplan

Der Leitfaden

Vorgehensplan vorbereiten

- **Schritte:**
  1. Analyse
     - Was ist passiert, was ist betroffen
  2. Angriff stoppen
     - Ausbreitung verhindern, Risko minimieren
  3. Krisenstab einberufen
     - Kommunikation & weiteres Vorgehen

Der Leitfaden

Vorgehensplan vorbereiten

Vorgehensplan vorbereiten –

im Notfall an aktuelle Gegebenheiten anpassen

Nachdem Mario über den Erst-Kontakt das Notfall-Team aktiviert hat, ist das externe Forensik-Team gerade dabei herauszufinden was passiert ist. Johannes (53) der Geschäftsführer von EiLand wurde schon vor 30min telefonisch informiert und ist gerade auf dem Weg zum Firmengelände. Auch wenn der Schock tief sitzt, während IT-Mitarbeitende den Angriff stoppen, ruft Johannes aus dem Auto heraus gerade alle für den Notfall vorgesehenen Personen für eine erste Krisenbesprechung zusammen.

Sie haben bereits wichtige Maßnahmen gelernt, damit Sie für den Ernstfall besser vorbereitet sind. Dennoch gibt es für den Ernstfall kein Koch-Rezept und Sie müssen ihre Aktivitäten der aktuellen Situation anpassen. D.h. in diesem Teil erstellen Sie einen Leitfaden mit Fragen und Aufgaben, die auf Ihr Unternehmen abgestimmt sind, um am Tag X strukturiert vorgehen zu können. Es macht Sinn diesen Leitfaden z.B. mit Ihrem aktuellen IT Dienstleister durchzugehen, oder wie bereits erwähnt mit einen potentiellen IT Dienstleister durchzugehen.

Im folgenden Abschnitt finden Sie Ideen zu Fragen und Aufgaben. Überlegen Sie welche Fragen könnten für die Analyse der Situation, den ersten Schritten und der weiteren iterierenden Vorgehensweise helfen.

Schritt 1 – Analyse

- Was ist betroffen?
  a) Welches System? _____
  b) Welche Assets? _____
  c) Netzwerk? Hardware? _____
  d) Welche Firmenstandorte? _____
- Was ist passiert? (Evtl. hier bereits externe Forensik hinzuziehen)
- Woher kam der Angriff? (Parallel zu allen weiteren Schritten)

Schritt 2 – Angriff stoppen, Ausbreitung verhindern

Überlegen Sie gemeinsam mit Ihren internen und externen Expert*innen, wie sie eine weitere Ausbreitung verhindern können. **Folgende Punkte dienen nur als Idee:**

- Clients und Server isolieren z.B. vom Netz trennen (Kabel abstecken, WLAN ausschalten), Server herunterfahren
- Nicht mit privilegierten Benutzerkonten (Administratorkonten) bei einem potenziell infizierten System anmelden, während es sich in einem internen Produktionsnetzwerk befindet oder mit dem Internet verbunden ist!
- Verifizierung aller Konten (vor allem Administratoren).
  - Sind alle Administratorkonten legitim angelegt oder gibt es Konten, die keinem Mitarbeitenden zugeordnet werden können?

- 22 -

...nutzerkonten, die nicht nur Benutzerrechte, sondern auch ... haben? Die Malware könnte diese Konten ändern und ...

...che auf Clients oder fehlgeschlagenen DNS-Auflösungsversuchen ...r? Diese könnten auf Schadsoftware hinweisen. Prüfen Sie die ...betroffenen Systeme (z. B. auf neue RDP-Freigaben). ...nbedingt erforderliche Remoteverbindungen (RDP, SSH, Terminal-...

... bzw. wieder aktivieren!

...erkverkehr und führen Sie Antivirenscans durch, um weitere ... Zugriffe zu erkennen bzw. zu verhindern. Dies umfasst u. a. ..., RDP/VNC-Verbindungen, Benutzer-Logins, Passwörter für ... Anwendungen wie PuTTY, FileZilla, WinSCP, etc.

...nd zur Vorsicht aufrufen!

...r einspielen, lassen sie diese ggf. von externen Forensikern prüfen, ...cht kompromittiert sind.

...rity-Profis, weitere Maßnahmen, die für Ihr Unternehmen sinnvoll ... verhindern.

_____

_____

_____

...en Notfallkontakte einen Krisenstab! Wer vom vorgesehenen ... in den nächsten Stunden/Tagen für folgende Themen zuständig?

...ntern: ...unden: ...resse: *...ergänzen Sie die Liste oder streichen Sie Themen, die für ihr ...Unternehmen nicht relevant sind)*
...nzeige Polizei: ...SGVO: ...IS-Meldung: *...ergänzen Sie die Liste oder streichen Sie Themen, die für ihr ...Unternehmen nicht relevant sind)*

- 23 -

...ngriff ist immer eine Momentaufnahme und kann sich gerade ...t es wichtig, sich im Krisenstab in regelmäßigen Abständen ...bständen (im Stundenbereich) und später in immer längeren ... alle Beteiligten Ihre Erkenntnisse oder Fragen und ...eilt und die Vorgehensweise ständig angepasst. Schreiben Sie ...Phase auf und prüfen Sie den Fortschritt im nächsten Termin. ...rastruktur wiederhergestellt ist.

...erständlich in dieser komplexen Situation. Scheuen Sie nicht ...iese können Sie vor allem in der akuten Phase unterstützen, ...reffen.

...n

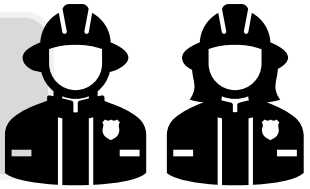
...olizei gemeldet wurde, ist diese aktuell am Firmengelände und ...weggründen für eine mögliche Täterschaft. Mario ist in erstem ...tion und will eigentlich nur helfen, dass Unternehmen wieder ...ndet er sich in einer Polizeibefragung und fühlt sich sichtlich

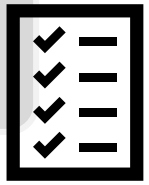
...t nicht ... für die ...cherung, ...ern.	**Lösegeld** Lösegeld-Zahlungen sind nur der allerletzte Ausweg, denn... 1. Sie haben keine Garantie, dass verschlüsselte Dateien entschlüsselt werden, oder abgezogene Daten gelöscht. 2. Sie wissen nicht an wen Sie das Lösegeld zahlen. Womöglich unterstützen Sie damit eine terroristische Organisation und machen sich selbst straftätig. 3. die Organisation der Übergabe (meist wird virtuelle Währung gefordert) sowie die Beschaffung des Geldes kann mehrere Tage dauern und sind somit auch keine schnelle Lösung.
...oder bei ..., wenden ...stelle für ...eschädigt ...n: ...richtsfest ...prechend	
...it der ...chtlinie ...ng des ...ittform	**DSGVO/Datenschutz** Sind sensible/persönliche Daten abgezogen worden oder besteht die Möglichkeit? Ziehen Sie einen DSGVO-Experten hinzu, um sicher zu gehen bei Bedarf Ihren rechtlichen Meldepflichten (meist innerhalb von 72h) nachzukommen.

- 24 -

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- Vorgehensplan





Ziel: handlungsfähig bleiben

ABSCHLUSS & AUSBLICK

Versicherungen & Rechtliches

- **Empfehlungen**
  - Je nach Branche, Versicherungsangebot in Betracht ziehen
  - Diese kann in allen Bereichen sofort unterstützen
  - Verantwortung kann hier abgegeben werden

- **Im Angriffsfall**
  - Polizeiliche Anzeige erstatten
  - Versicherung im Angriffsfall sofort einbinden
  - Nie ohne Versicherer auf eigene Faust handeln (sonst droht Leistungsverlust)

Aufarbeitung des Vorfalls

- **Reflexion mit dem Kern-Team**
  - Was hätte besser laufen können? → *Lessons learned – Workshop*
  - Weitere Empfehlungen im Leitfaden-Dokument

- **Reflexion mit dem Rest**
  - Siehe Leitfaden

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Gefördert durch DIH-Süd Kooperation

- **Ziel**: Unterstützung von KMUs gegen Cyberkriminalität
- **Basis**: Interviews mit Expert*innen und Betroffenen

Disclaimer

- Erfordert regelmäßige individuelle Prüfung und Anpassung
- Dienst als Ergänzung zum techn. Sicherheitskonzept
- Professionelle Unterstützung im Angriffsfall wird empfohlen

Weitere Weiterbildungen

https://www.campus02.at/wirtschaftsinformatik/weiterbildung/

KURZPROGRAMME

Unsere Weiterbildungsangebote sind modular aufgebaut. Die Module können auch einzeln als Hochschulkurse absolviert werden. Dadurch gehen wir flexibel auf die potenziellen Anforderungen von Unternehmen ein und bieten Teilnehmer*innen ein breites Spektrum an punktuellem Wissen, welches aktuell in der Wirtschaft gefordert wird.

- Requirements Engineering →
- DevOps →
- IT-Projektmanagement →
- AI-Fundamentals →
- Advanced Digital Management & Leadership →

Vielen Dank!

https://www.campus02.at/wirtschaftsinformatik/weiterbildung/