

CYBERSECURITY NOTFALLPLAN: SORGEN SIE FÜR IHRE SICHERHEIT

Mag. Angelika Höber | Department IT & Wirtschaftsinformatik

AGENDA

- ❖ Einleitung
- ❖ Inhalte des Leitfadens
- ❖ Abschluss & Ausblick

CYBERANGRIFF
NOTFALLPLAN

für Ihr
Unternehmen

Vorstellung aktueller Fördermöglichkeiten (Hr. Silen Bosch, SFG)

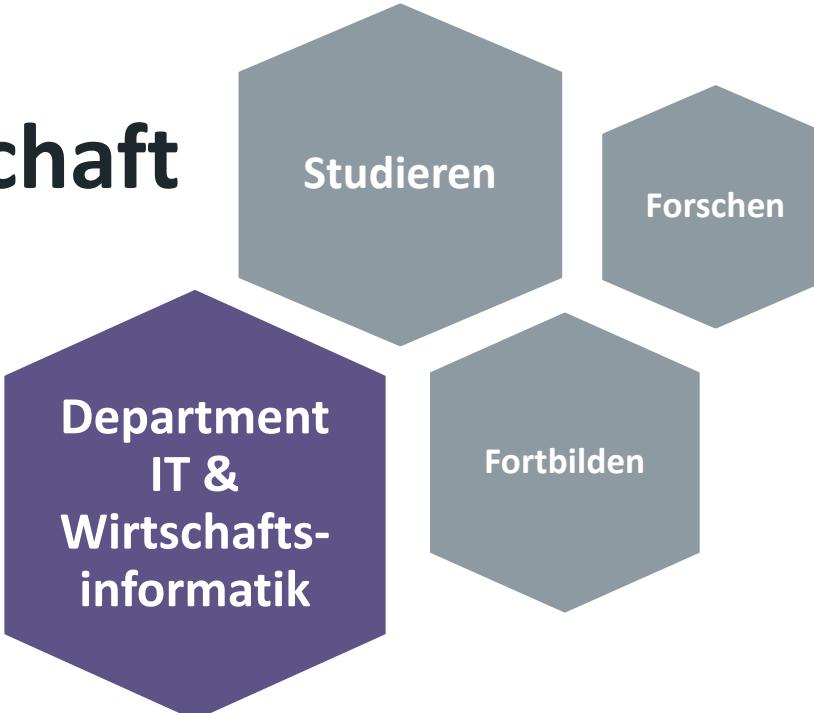
Vorstellung

Mein Name ...

Mein Unternehmen / das
Unternehmen, für das ich
arbeite ...

Meine Erfahrungen mit
Internet-Kriminalität ...

Technik & Wirtschaft







Was würden Sie tun?

GLOBAL THREAT INDEX MAP

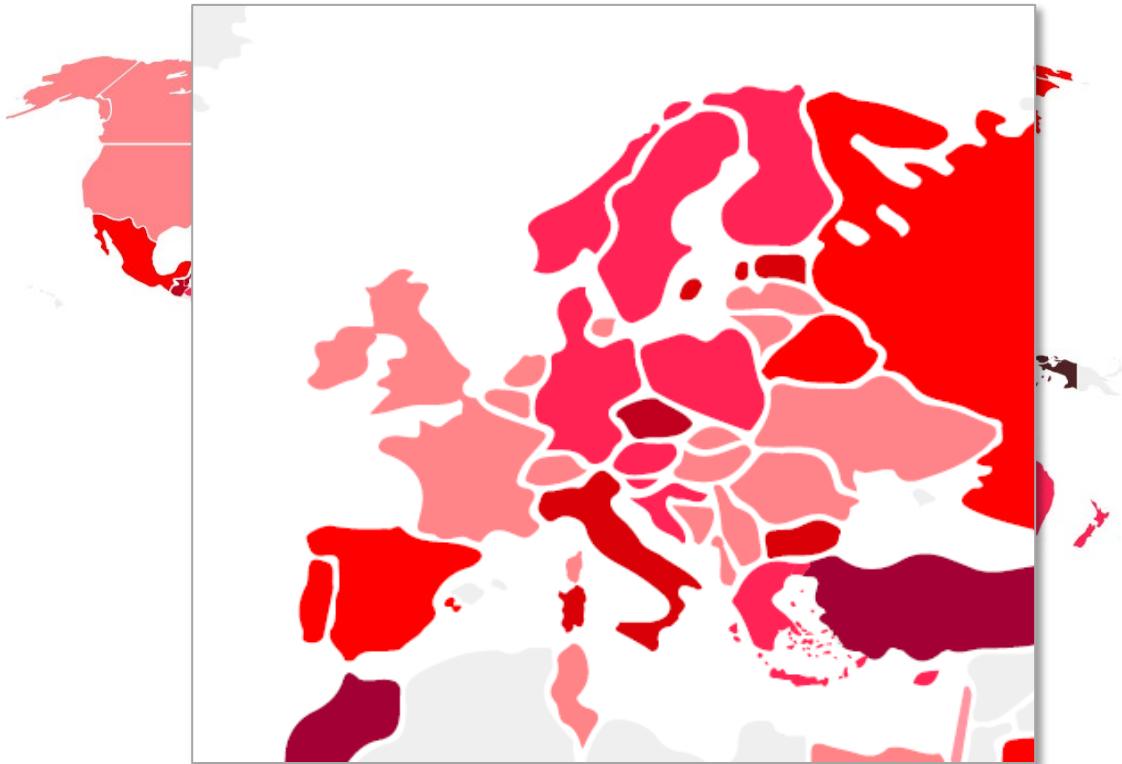
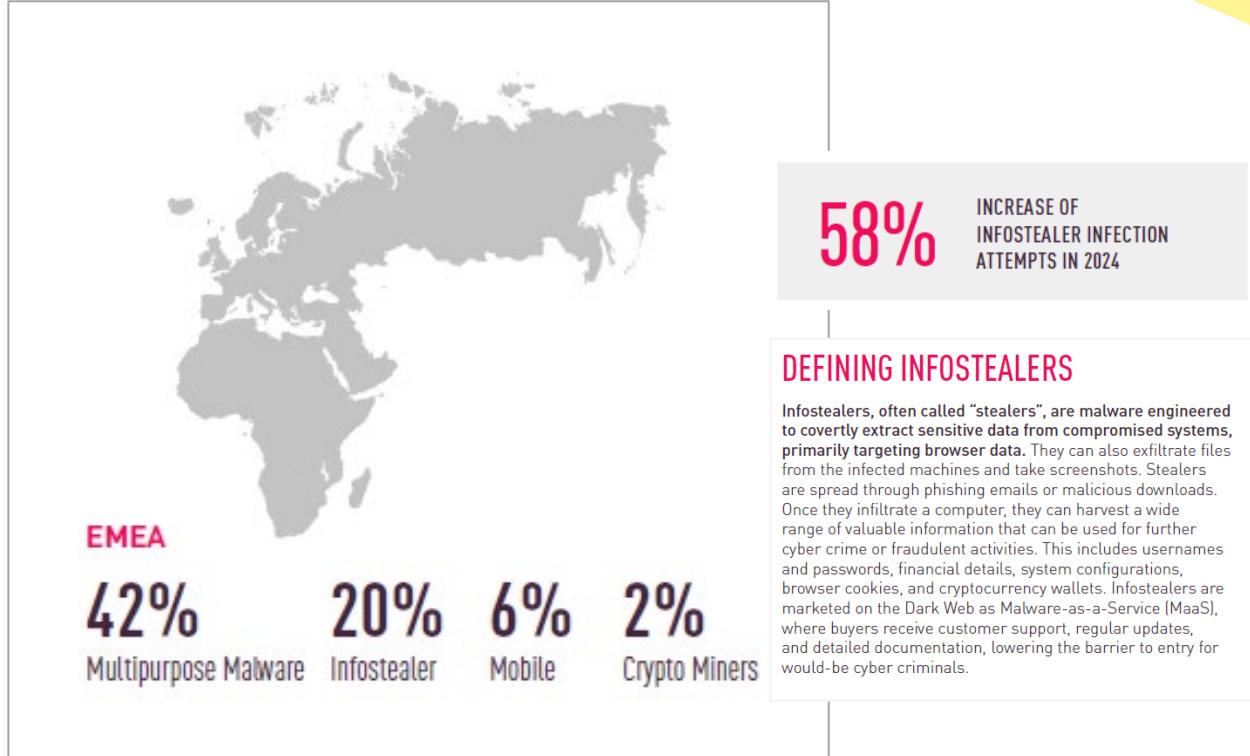


Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.





24.10.2025 Angriffe gegen Microsoft WSUS Installationen - Update verfügbar

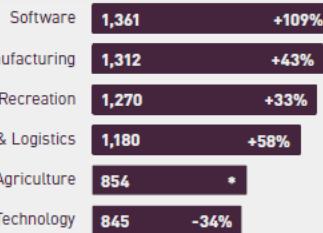
Microsoft hat eine kritische Sicherheitslücke in Windows Server Update Service (WSUS) veröffentlicht, die es unauthentifizierten Angreifern ermöglicht, aus der Ferne beliebigen Code auf betroffenen Servern auszuführen. Ein bereits öffentlich verfügbarer Proof-of-Concept (PoC) Exploit erhöht die Wahrscheinlichkeit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

WARNUNGEN

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.

AKTUELLES



GLOBAL
 WEEKLY ATTACKS
 PER ORGANIZATION
 BY INDUSTRY IN 2024

(% OF CHANGE FROM 2023)

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

Was können Sie tun?

PRÄVENTION



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



REAKTION



Was können Sie tun?

PRÄVENTION



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



REAKTION



CYBERANGRIFF NOTFALLPLAN

für Ihr Unternehmen

Ziel des Workshops

**CYBERANGRIFF
NOTFALLPLAN
für Ihr
Unternehmen**

HEUTE
gemeinsam für Situation vorbereiten

NACH DEM WORKSHOP
Notfall-Leitfaden weiterentwickeln und lesen

Was bringt das?

- ▶ schnell und zielgerichtet reagieren
- ▶ Auswirkungen eines Angriffs minimieren
- ▶ Dem Chaos mit organisatorischen Maßnahmen vorbeugen



**CYBERANGRIFF
NOTFALLPLAN
für Ihr
Unternehmen**

handlungsfähig bleiben

CYBERANGRIFF NOTFALLPLAN

für Ihr Unternehmen

Geschäftsprozesse



Dokumentation

Kommunikation



Notfallteam



Vorgehensplan

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

**CYBERANGRIFF
NOTFALLPLAN**
für Ihr
Unternehmen

Geschäftsprozesse

Was muss täglich laufen?



Der Leitfaden

1. Schritt: kritische **Geschäftsprozesse** identifizieren

- ▶ Kritische Geschäftsprozesse identifizieren

- ▶ Liste erstellen und dann nach Priorität sortieren



Der Leitfaden

1. Schritt: kritische **Geschäftsprozesse** identifizieren

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

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, ...
- ❖ Handhabung planen:
 - ▶ An sicherer Stelle ablegen
 - ▶ Regelmäßig aktualisieren



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:

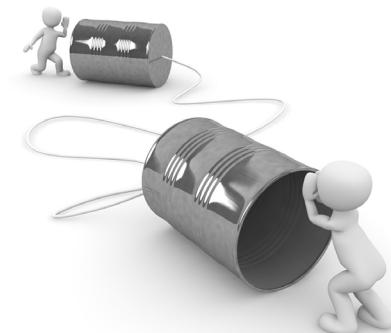
| | | | | |
|--|------------|----------------------------|------------|--|
| Lieferantenliste mit Namen, Telefonnummern | Büro, Safe | Halbjährlich (1.12., 1.6.) | Frau Huber | Unbedingt auch Handynummern für Erreichbarkeit im Notfall! |
|--|------------|----------------------------|------------|--|



**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,**

Der Leitfaden

Kommunikation

Wien 2°C

NACHRICHTEN MEINUNG MAGAZIN Österreich International European Voices Geld & Finanzen Über Geld spricht man Young Finance Die Bilanz

Stillstand

Cyberangriff auf SalzburgMilch: "Wir kriegen die Produkte nicht raus"

Die drittgrößte Molkerei des Landes steht still. Hacker kaperten das gesamte EDV-System.

Artikel verschenken



yesss! macht mein Leben yesser

Dein Tarif spricht fließend EU.

Der Leitfaden

Kommunikation

Wetter Abo E-Paper Club Shop Gutscheine Trauerportal Werbung

Steiermark Kärnten

MENÜ



STEIERMARK LEBEN SPORT

KLEINE
ZEITUNG

GRAZ & UMGEBUNG

EINLOGGEN

STEIERMARK > SÜDOST & SÜD

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 planen

❖ Fragen:

- ▶ Wen rufen Sie ohne ein Telefon oder MS Teams an bzw. *WIE*?
- ▶ Wer darf Informationen weiterleiten?
- ▶ Welche Informationen dürfen wohin?
 - **Kolleg*innen, 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

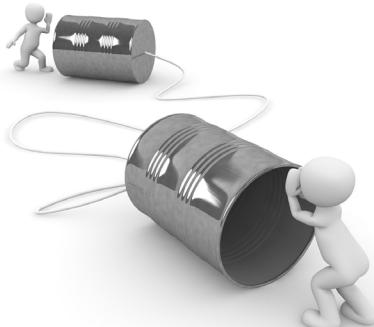
Schritt 2: Kommunikation planen

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.

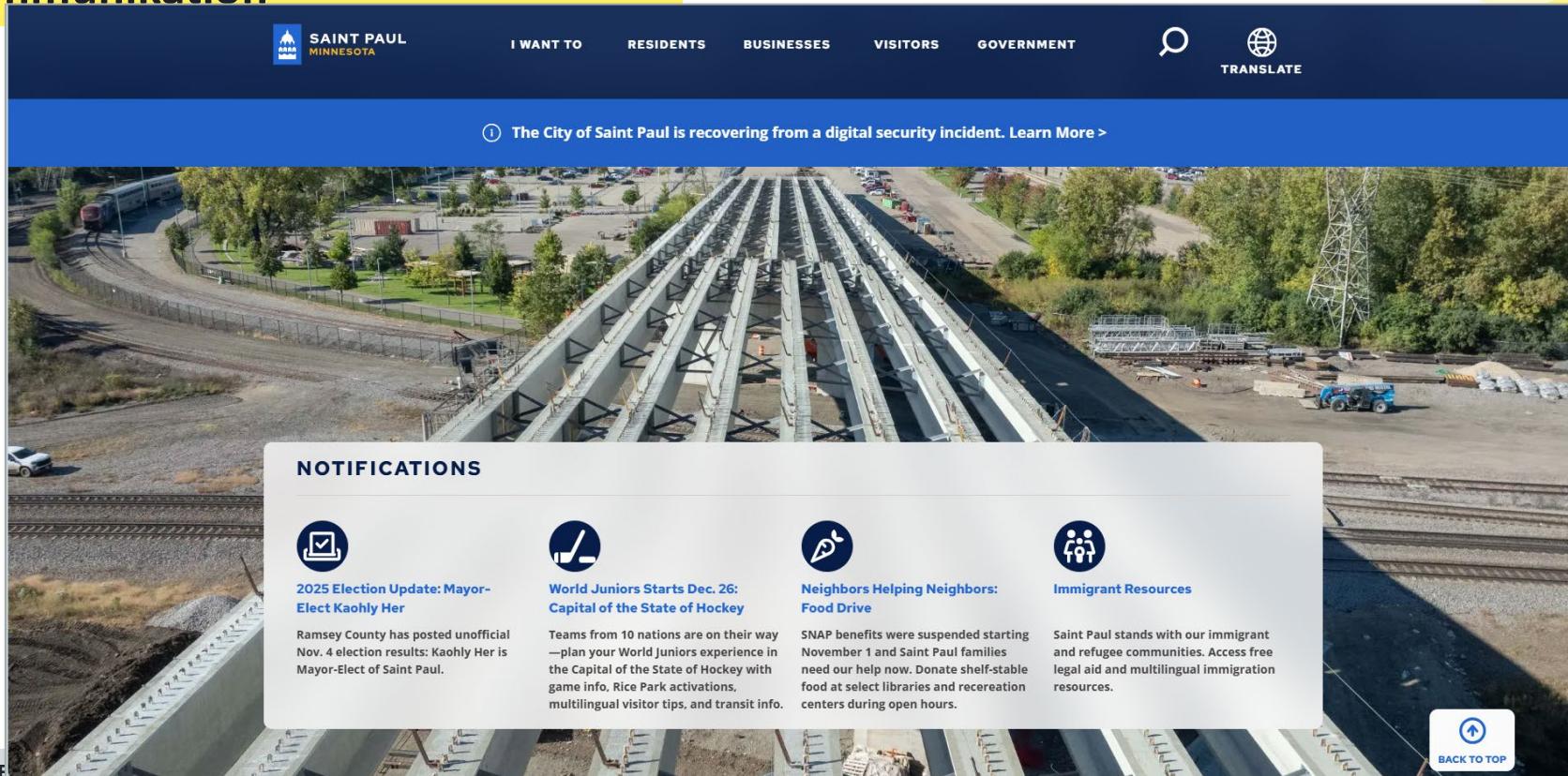
Beispiele:

| 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 |



Der Leitfaden

Kommunikation



The City of Saint Paul is recovering from a digital security incident. Learn More >

NOTIFICATIONS

 [2025 Election Update: Mayor-Elect Kaohly Her](#)
Ramsey County has posted unofficial Nov. 4 election results: Kaohly Her is Mayor-Elect of Saint Paul.

 [World Juniors Starts Dec. 26: Capital of the State of Hockey](#)
Teams from 10 nations are on their way —plan your World Juniors experience in the Capital of the State of Hockey with game info, Rice Park activations, multilingual visitor tips, and transit info.

 [Neighbors Helping Neighbors: Food Drive](#)
SNAP benefits were suspended starting November 1 and Saint Paul families need our help now. Donate shelf-stable food at select libraries and recreation centers during open hours.

 [Immigrant Resources](#)
Saint Paul stands with our immigrant and refugee communities. Access free legal aid and multilingual immigration resources.

 BACK TO TOP

Der Leitfaden

Kommunikation

The screenshot shows the official website of the City of Saint Paul, Minnesota. The top navigation bar includes links for "I WANT TO", "RESIDENTS", "BUSINESSES", "VISITORS", "GOVERNMENT", and "TRANSLATE". Below the main content area, there is a secondary navigation bar with links for "OUR RESPONSE", "MILESTONES", "PAYMENT UPDATES", "HOW TO CONTACT US", "DIRECTORY", and "FAQ".

Our Response to the Digital Security Incident

Since July 25, the City of Saint Paul has been responding to a digital security incident. We've partnered with state and federal agencies - including the FBI, Minnesota Department of Public Safety, Minnesota IT Services, Minnesota National Guard, and other cybersecurity experts. Together, our teams have worked tirelessly to:

- Protect core City services, including emergency response and public safety.
- Take significant and proactive steps to defend our City and limit the impact of this incident.
- Securely recover and restore City systems.

Digital security is a global issue. This is one of a growing number of recent ransomware attacks, including on other major U.S. cities. We're not unique in being targeted by criminal threat actors. Because we acted swiftly and decisively, we were able to limit the impact, safeguard critical services, and position our systems for a safe and secure recovery operation.

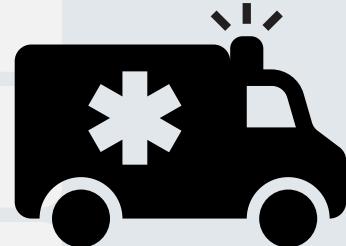
What's Next

We are prioritizing restoration of critical applications and continue to safely and securely bring our systems back online. Full restoration is expected soon.

Watch: Mayor Carter and City Leaders Provide Overview of Incident and Response on August 27



**CYBERANGRIFF
NOTFALLPLAN**
für Ihr
Unternehmen



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

Umsetzung

- ▶ Krisenstab vorab bilden und Ersatz definieren
- ▶ Leitung des Notfallteams definieren

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



Der Leitfaden

Notfallteam aufstellen (intern)

Arbeitsblatt Mögliche 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.

| Verantwortungsbereich | 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:

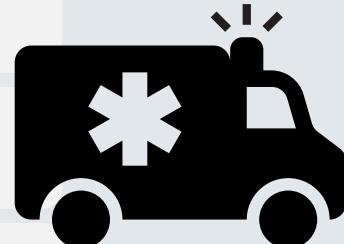
| Verantwortungsgebiet | Firma | Kontaktperson (wenn vorhanden), Telefonnummer |
|---|-------|---|
| Forensik (um herauszufinden was überhaupt passiert ist) | | ✉ 📞 |
| Wiederherstellung: | | ✉ 📞 |
| Arbeitskräfte (zur Hilfe bei der Wiederherstellung) | | ✉ 📞 |
| Hardware (Notebooks, Internet-Cube, Server, 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, Risiko 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 einem 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?
 - Welches System?
 - Welche Assets?
 - Netzwerk? Hardware?
 - Welche Firmenstandorte?
- Was ist passiert? (Ext. hier bereits externe Forensik hinzuziehen)
- Wohin 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 Mitarbeiter zugeordnet werden können?

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

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

bzw. wieder aktivieren! Verkehr und führen Sie Antivirencalls 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. und zur Vorsicht aufrufen! Reinspielen, lassen sie diese ggf. von externen Forensikern prüfen, nicht kompromittiert sind. Party-Pros, weitere Maßnahmen, die für Ihr Unternehmen sinnvoll verhindern.

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

tern:
Gunden:
Fresse:
Organisieren Sie die Liste oder streichen Sie Themen, die für Ihr Unternehmen nicht relevant sind!

Mazige Polizei:

DSGVO:

BS-Meldung:

Organisieren Sie die Liste oder streichen Sie Themen, die für Ihr Unternehmen nicht relevant sind!

angriff ist immer eine Momentaufnahme und kann sich gerade es wichtig, sich im Krisentab in regelmäßigen Abständen bestanden (Stundentabach) und später in immer längeren alle Beteiligten ihre Bedürfnisse oder Fragen und diese und die Voraussetzungen ständig angepasst. Schreiben Sie diese auf und prüfen Sie den Fortschritt im nächsten Terminstruktur wiederhergestellt ist.

verständlich in dieser komplexen Situation. Scheuen Sie nicht diese können Sie vor allem in der akuten Phase unterstützen, teien.

n

polizei gemeldet wurde, ist diese aktuell am Firmengelände und wegbringen für eine mögliche Töterschafft. Maria ist in erstem und will eigentlich nur helfen, dass Unternehmen wieder rüder er sich in einer Polizeibefragung und fühlt sich sichtlich

et nicht für die Sicherung, dann...

Lösegeld-Zahlungen sind nur der allerletzte Ausweg, denn...

- Sie haben keine Garantie, dass verschlüsselte Dateien entschlüsselt werden, oder abgezogene Daten gelöscht.
- Sie wissen nicht, wen Sie das Lösegeld zahlen. Werdegängig überzeugen Sie damit eine terroristische Organisation und machen sich selbst strafbar.
- 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 Anwendungen für die Sicherung, dann...

oder bei Anwendungen für die Sicherung, dann...</

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse



Dokumentation

Kommunikation

Notfallteam



Vorgehensplan



Ziel: handlungsfähig bleiben



ABSCHLUSS & AUSBLICK



FACHHOCHSCHULE DER WIRTSCHAFT

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

CYBERSECURITY NOTFALLPLAN: SORGEN SIE FÜR IHRE SICHERHEIT

Mag. Angelika Höber | Department IT & Wirtschaftsinformatik

AGENDA

- ❖ Vorstellung & Sensibilisierung
- ❖ Ihren Leitfaden erstellen
- ❖ Abschluss & Ausblick

CYBERANGRIFF
NOTFALLPLAN

für Ihr
Unternehmen

Vorstellung aktueller Fördermöglichkeiten (Hr. Silen Bosch, SFG)

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 punktuell Wissen, welches aktuell in der Wirtschaft gefordert wird.

Requirements Engineering →

Design-Patterns →

DevOps →

AI-Fundamentals →

IT-Projektmanagement →

Strategisches IT-Management →

Moderne Software Architektur →

VIELEN DANK!

AGENDA

- ✓ Vorstellung & Sensibilisierung
- ✓ Ihren Leitfaden erstellen
- ✓ Abschluss & Ausblick

CYBERANGRIFF
NOTFALLPLAN

für Ihr
Unternehmen

Vorstellung aktueller Fördermöglichkeiten (Hr. Silen Bosch, SFG)