

CYBER- SICHERHEIT NOTFALLPLAN

HANDLUNGSFÄHIG BLEIBEN
IM ANGRIFFSFALL

Mag. Angelika Höber

FH CAMPUS 02
Department IT & Wirtschaftsinformatik

**CYBERANGRIFF
NOTFALLPLAN**

für Ihr
Unternehmen



Technik & Wirtschaft

Studieren

Forschen

Department
IT &
Wirtschafts-
informatik

Fortbilden



Ein ganz normaler Tag



IHRE DATEIEN WURDEN VERSCHLÜSSELT

Sie haben keinen Zugriff mehr.

Wenn Sie wieder darauf zugreifen möchten, müssen Sie Lösegeld bezahlen.

Welche ersten Schritte würden Sie unternehmen?

GLOBAL THREAT INDEX MAP

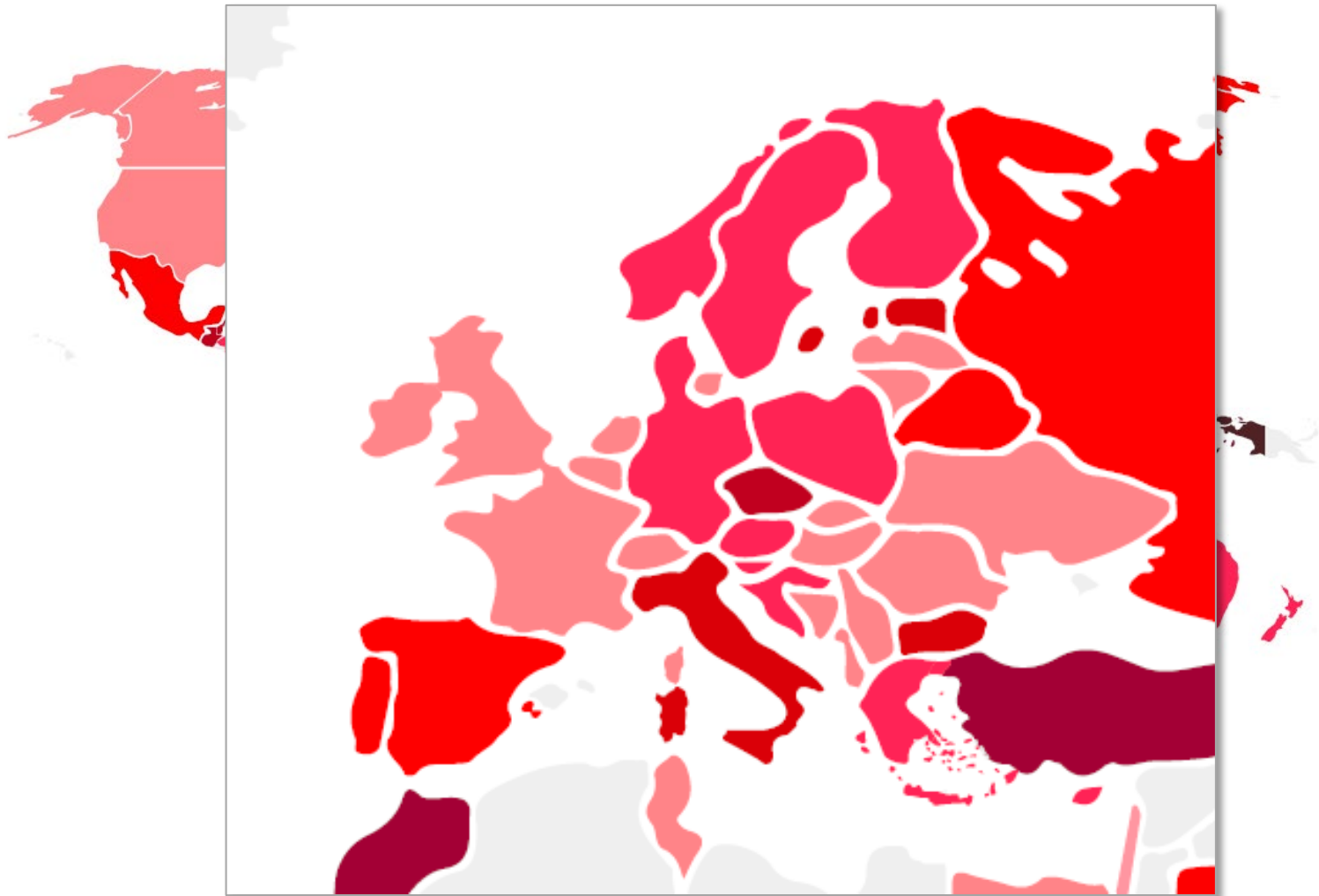


Figure 2 - The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.



EMEA

42%

Multipurpose Malware

20%

Infostealer

6%

Mobile

2%

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.



WARNUNGEN

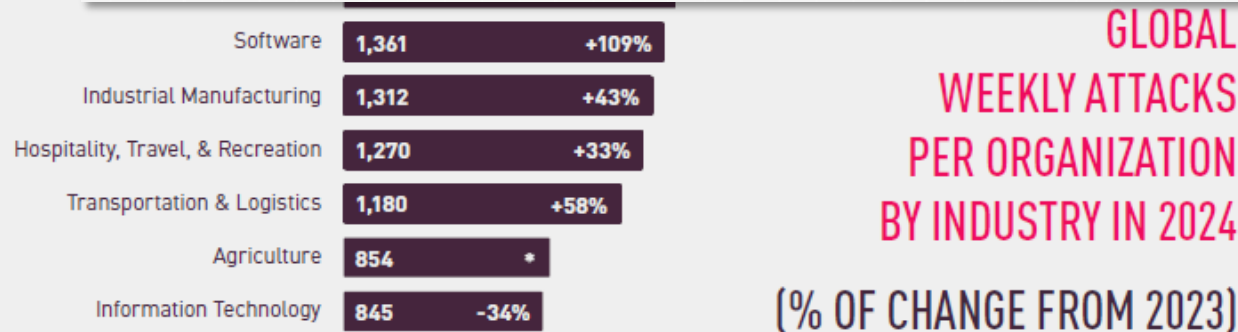
24.10.2025 Angriffe gegen Microsoft WSUS Installationen - Update verfügbar

Microsoft hat eine kritische Sicherheitslücke in Windows Server Update Service (WSUS) veröffentlicht, die es unauthentifizierte 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.

AKTUELLES

17.11.2025 Kritische Sicherheitslücke in Fortinet FortiWeb wird aktiv ausgenutzt

Eine kritische Sicherheitslücke (CVE-2025-64446) in Fortinet FortiWeb erlaubt es unauthentifizierte 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.



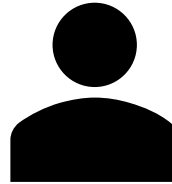
**GLOBAL
 WEEKLY ATTACKS
 PER ORGANIZATION
 BY INDUSTRY IN 2024**

(% OF CHANGE FROM 2023)

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

Was können Sie tun?

PRÄVENTION



REAKTION

1. Adopt a multi-layered approach within your security stack
Organizations should implement a multi-layered security strategy that includes regular vulnerability scanning, endpoint protection, and secure email filtering to mitigate malware and phishing threats. Strong endpoint detection and response (EDR) tools can help identify and isolate threats and block malware from spreading. Additionally, the use of cloud security posture management (CSPM) tools can help identify and remediate misconfigurations in cloud environments. Regular security assessments and incident response drills are essential to ensure preparedness against attacks.

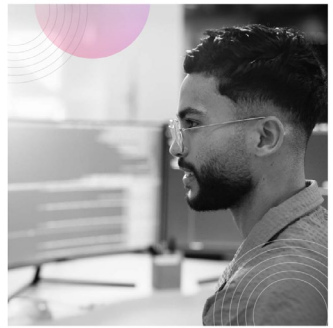
2. Prioritize advances
Organizations should give top priority to addressing the most critical vulnerabilities. Strong endpoint protection and EDR tools are essential for detecting and responding to threats. Regular security posture management (CSPM) tools can help identify and remediate misconfigurations in cloud environments.

3. Leverage AI for protection
Harness the power of artificial intelligence (AI) to enhance threat detection and response. AI can effectively identify and respond to threats in real-time. AI-powered security solutions can analyze vast amounts of data to identify patterns and anomalies, enabling security teams to respond more quickly to threats.

4. Gain 360 visibility
Obtain a comprehensive view of your organization's security posture across all assets and systems. This includes monitoring network traffic, endpoint activity, and cloud security posture. Regular security assessments and incident response drills are essential to ensure preparedness against attacks.

5. Develop a customer-trust program to ensure compliance
Organizations must establish a customer trust program to ensure compliance in today's rapidly changing regulatory landscape.

6. Implement Vulnerability and Risk Management Programs
The rapid emergence of new vulnerabilities, particularly in cloud environments, poses a significant challenge for vulnerability management. EDR tools, which are often used for incident response, can also be used to detect and respond to threats. Regular security assessments and incident response drills are essential to ensure preparedness against attacks.



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

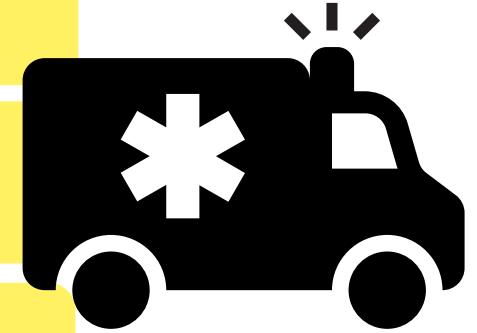
Geschäftsprozesse

Dokumentation

Kommunikation

Notfallteam

Vorgehensplan



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
---	--	----	----



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

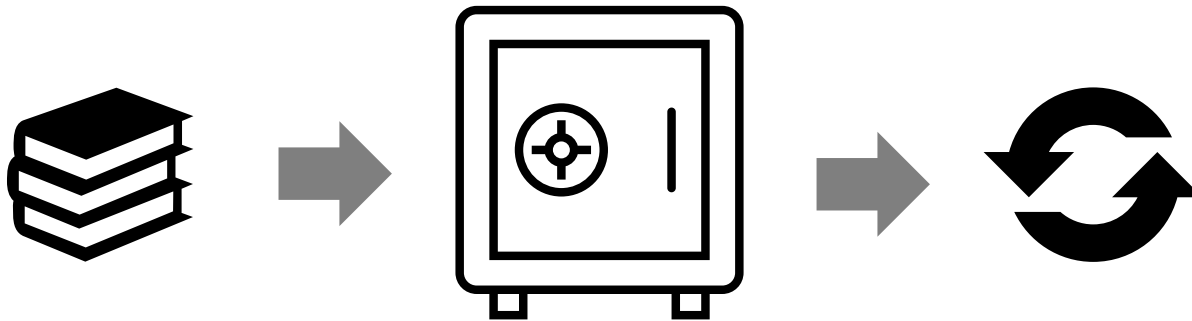
*Auf welche Dokumente muss immer
zugegriffen werden können?*



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
------------------	--



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:

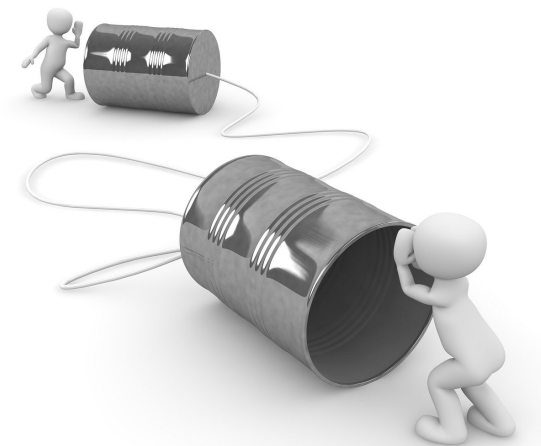
Lieferantenliste mit Namen, Telefonnummern	Büro, Safe	Halbjährlich (1.12., 1.6.)	Frau Huber	Unbedingt auch Handynummern für Erreichbarkeit im Notfall!
--	------------	----------------------------	------------	--



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.

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

Die Presse

ABO

Rätsel ePaper Player Newsletter Ever

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 yessser

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 **+ CYBERATTACKE AUF FELDBACH**

4. November 2022,
16:27 Uhr

f x ↻

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.

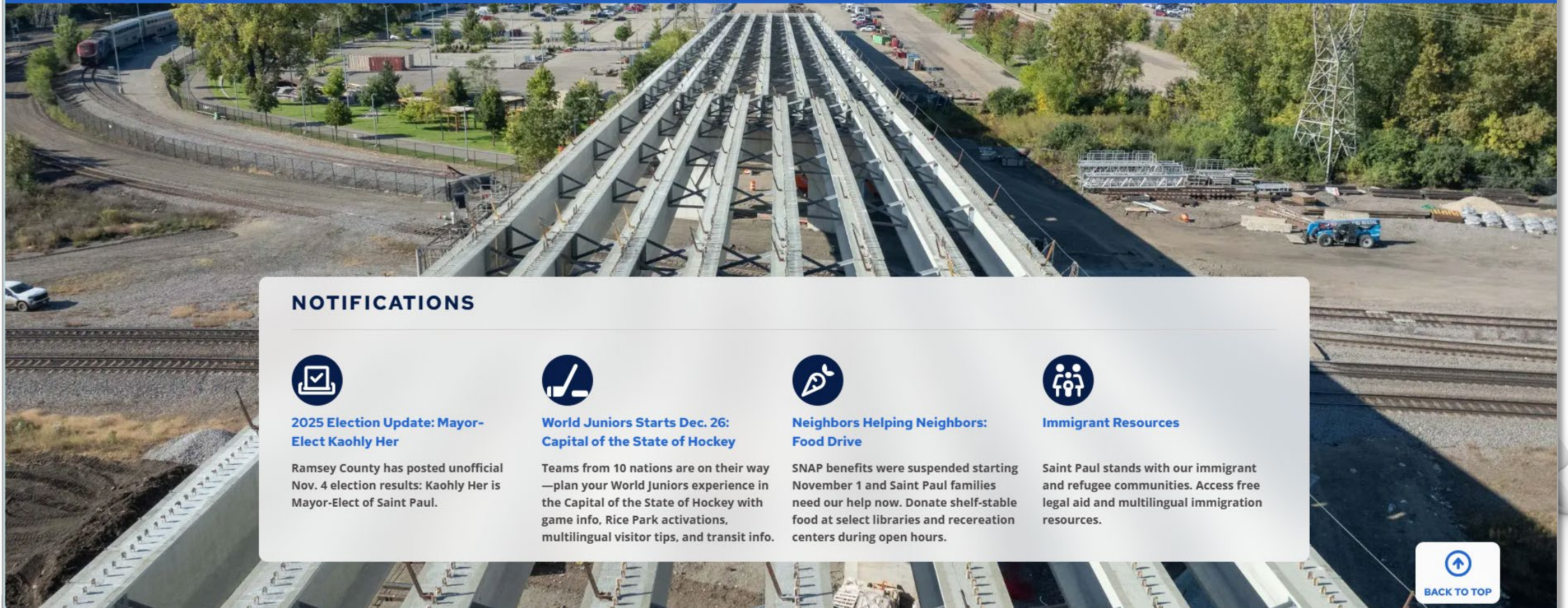


Wer hinter dem Angriff steckt und welche Daten betroffen sind, ist noch unklar (Symbolbild)

Der Leitfaden

Kommunikation

 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

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:

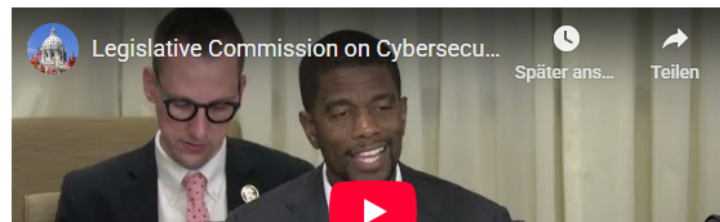
- Protect core City services, including emergency response and public safety.
- Take significant and proactive steps to defend our City and limit the impact of this incident.
- Securely recover and restore City systems.

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

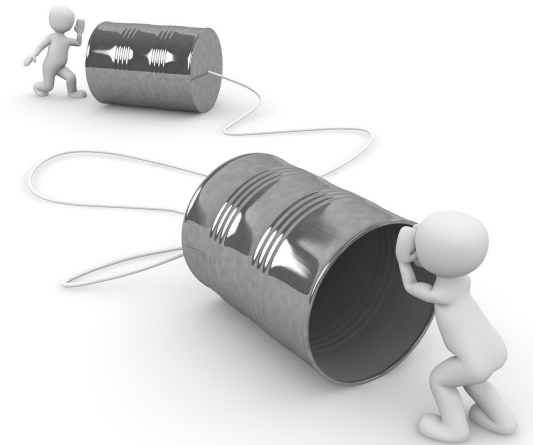


Der Leitfaden

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?

<i>Kommunikationsweg</i>	<i>Technische Voraussetzungen</i>	<i>Mögliche Alternativen</i>



Der Leitfaden

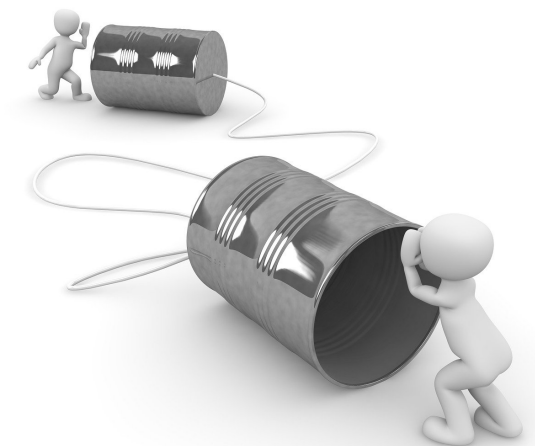
Schritt 2: Kommunikation planen

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	<p>Liebe Kolleginnen und Kollegen,</p> <p>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.</p> <p>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.</p> <p>Vielen Dank! xxx</p>	Personalabteilung	ALLE Mitarbeitenden
So schnell als möglich	<p>Liebe Kundenbetreuende,</p> <p>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</p>	Geschäftsführung	Kundenbetreuende
So schnell als möglich	<p>Liebe Kolleginnen und Kollegen,</p> <p>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</p>	Geschäftsführung	Kundenbetreuende, Hotline- bzw. Office-Mitarbeitende



**CYBERANGRIFF
NOTFALLPLAN
für Ihr
Unternehmen**



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen



Notfallteam

*Wer wird kontaktiert?
Wer koordiniert?
Wer entscheidet?*

Der Leitfaden

Notfallteam aufstellen

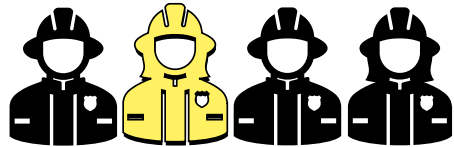
❖ Fragen

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



Der Leitfaden

Notfallteam aufstellen



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):	<input type="text"/>
	Vertretung (V):	<input type="text"/>
Rechtliche Themen (z.B. Anzeige bei Polizei, DSGVO, NIS, etc.):	H:	<input type="text"/>
	V:	<input type="text"/>
Forensik:	H:	<input type="text"/>
	V:	<input type="text"/>
Wiederherstellung:	H:	<input type="text"/>
	V:	<input type="text"/>
Interne Kommunikation (an Mitarbeitende)	H:	<input type="text"/>
	V:	<input type="text"/>
Externe Kommunikation (an Kunden und Presse)	H:	<input type="text"/>
	V:	<input type="text"/>
Sonstiges	H:	<input type="text"/>
	V:	<input type="text"/>



Der Leitfaden

Notfallteam aufstellen (extern)

Arbeitsblatt *Mögliche externe Dienstleister* (2/2)

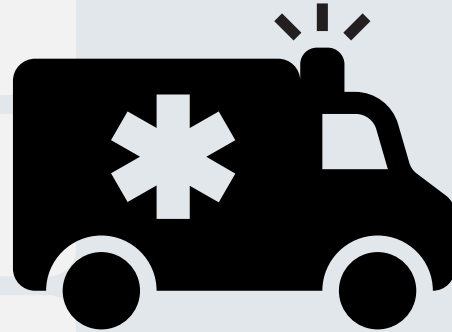
Haben Sie Kontakte zu externen Dienstleistern, die Ihnen im Fall eines Angriffs helfen können? Schreiben Sie hier Ihre Partner-Firmen auf, mit denen Sie bereits in Kontakt sind und die Ihnen im Notfall helfen können:

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?
 - 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?

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

prüfen Sie auf Clients oder fehlgeschlagenen DNS-Auflösungsversuchen. Diese könnten auf Schadsoftware hinweisen. Prüfen Sie die betroffenen Systeme (z. B. auf neue RDP-Freigaben).

Unbedingt erforderliche Remoteverbindungen (RDP, SSH, Terminal-Verbindungen) sind zu deaktivieren!

Netzwerke wieder aktivieren! Netzwerkverkehr und führen Sie Antivirenschans 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.

Bitte sind zur Vorsicht aufrufen! Testen Sie die Reaktionen, lassen sie diese ggf. von externen Forensikern prüfen, wenn diese nicht kompromittiert sind. IT-Sicherheits-Profis, weitere Maßnahmen, die für Ihr Unternehmen sinnvoll sind, um die Ausbreitung zu verhindern.

Überprüfen Sie die Notfallkontakte einen Krisenstab! Wer vom vorgesehenen Krisenstab in den nächsten Stunden/Tagen für folgende Themen zuständig?

Interne Medien: Presse: Ergänzen Sie die Liste oder streichen Sie Themen, die für Ihr Unternehmen nicht relevant sind) Zeige Polizei: DSGVO: Mithras-Meldung: Ergänzen Sie die Liste oder streichen Sie Themen, die für Ihr Unternehmen nicht relevant sind)

Der Angriff ist immer eine Momentaufnahme und kann sich gerade in der akuten Phase ändern. Es ist wichtig, sich im Krisenstab in regelmäßigen Abständen (im Stundenbereich) und später in immer längeren Abständen (im Tagesbereich) zu treffen. Alle Beteiligten ihre Erkenntnisse oder Fragen und die Vorgehensweise ständig angepasst. Schreiben Sie die aktuelle Phase auf und prüfen Sie den Fortschritt im nächsten Termin. Die IT-Struktur wiederhergestellt ist.

Bitte sind in dieser komplexen Situation. Scheuen Sie nicht diese können Sie vor allem in der akuten Phase unterstützen, wenn Sie helfen.

Die Polizei gemeldet wurde, ist diese aktuell am Firmengelände und weggerufen für eine mögliche Täterschaft. Mario ist in erster Linie ein Helfer und will eigentlich nur helfen, dass Unternehmen wieder normal läuft und er sich in einer Polizeibefragung und fühlt sich sich nicht

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 strafbar.
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.

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.



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 punktuelltem Wissen, welches aktuell in der Wirtschaft gefordert wird.

Requirements Engineering →

AI-Fundamentals →

DevOps →

Advanced Digital Management & Leadership →

IT-Projektmanagement →

Vielen Dank!



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