CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# DIGITAL & SICHER IN DIE ZUKUNFT

## CYBER SECURITY: VORBEREITUNG AUF UND VERHALTEN IM ANGRIFFSFALL

Mag. Angelika Höber
Department IT & Wirtschaftsinformatik

# Vorstellung

## Mag. Angelika Höber

Hauptberuflich Lehrende
an der
**FH Campus 02, Graz**

Department
**IT & Wirtschaftsinformatik**

# Technik & Wirtschaft


Studieren

Forschen

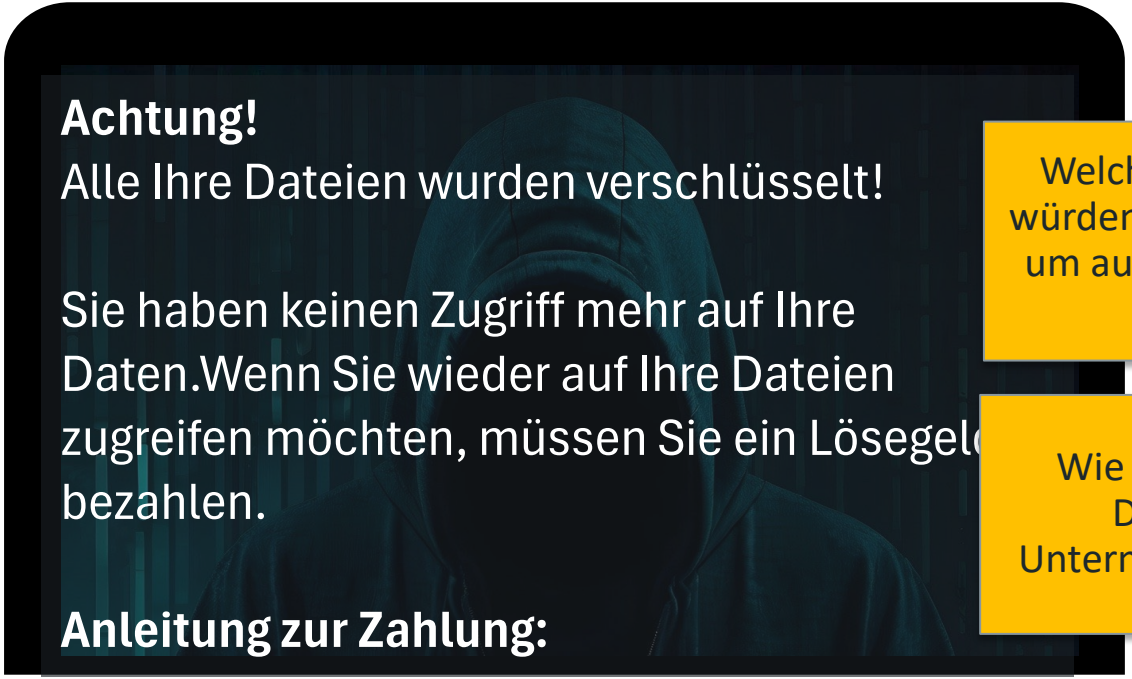
Department IT & Wirtschafts-informatik

Fortbilden

# Cyberangriff Szenario

## Ein ganz normaler Tag ….

# Cyberangriff Szenario




Welche ersten Schritte würden Sie unternehmen, um auf diesen Angriff zu reagieren?

Wie würden Sie Ihre Daten und Ihr Unternehmen schützen?

# Einleitung

- **Realität Cyberangriffe**
  - Kein seltenes Ereignis! 2022 bis 2023 + 9,4%

- **Was tun? Vorsorge und Reaktion vorbereiten**
  - Vorbereitung und Kenntnis über potenzielle Bedrohung
  - Proaktive Maßnahmen zur Risikominimierung

# Aktuelle Bedrohungen

- **Phishing (Nr. 1. Problem in Österreich)**
  - Angriffe auf Zugangsdaten
  - Per E-Mail, SMS oder über betrügerische Anrufe (Social Engineering)
- **Man-in-the-Middle Attacken**
- **Denial of Service Attacken**
- **Malware**
  - z.B. Ransomware

# Ziel des Workshops

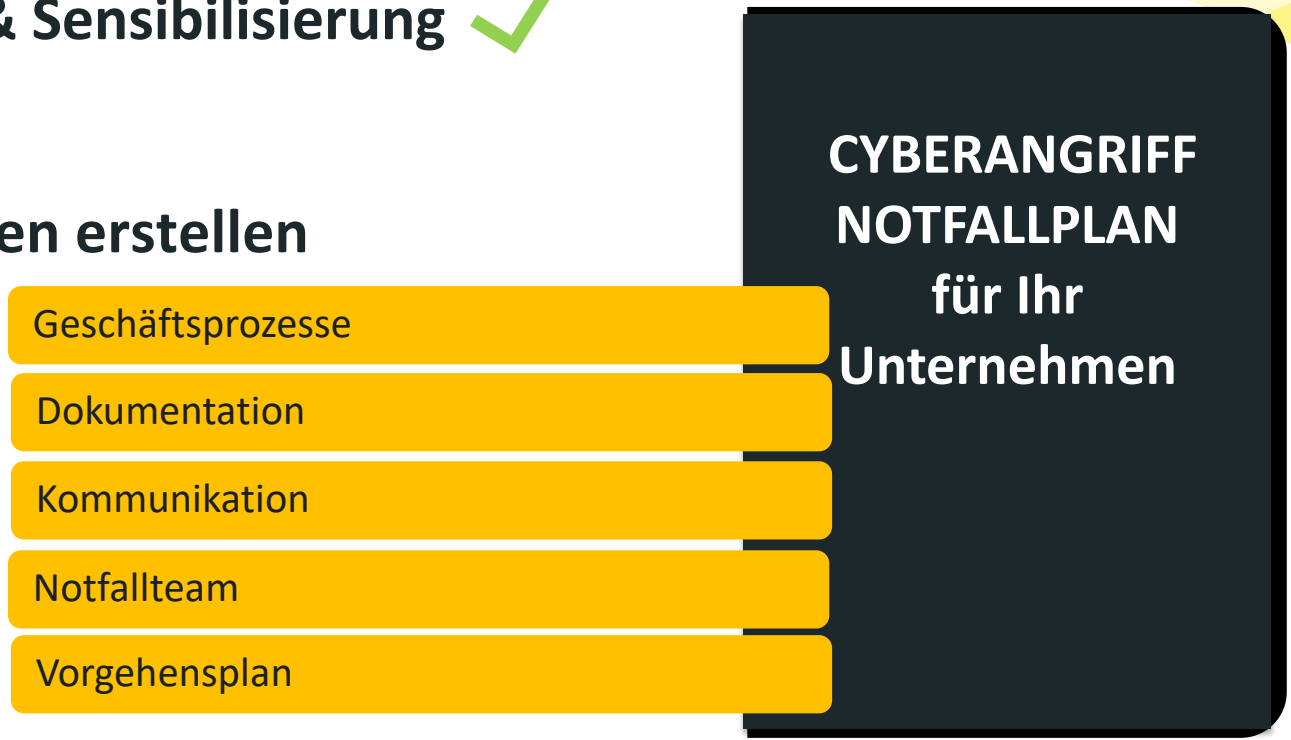
**CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen**

**HEUTE**
gemeinsam für Situation vorbereiten

**NACH DEM WORKSHOP**
Notfall-Leitfaden weiterentwickeln und lesen

# AGENDA

- Vorstellung & Sensibilisierung ✓
- Einleitung
- Ihren Leitfaden erstellen




- Abschluss & Ausblick

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# EINLEITUNG

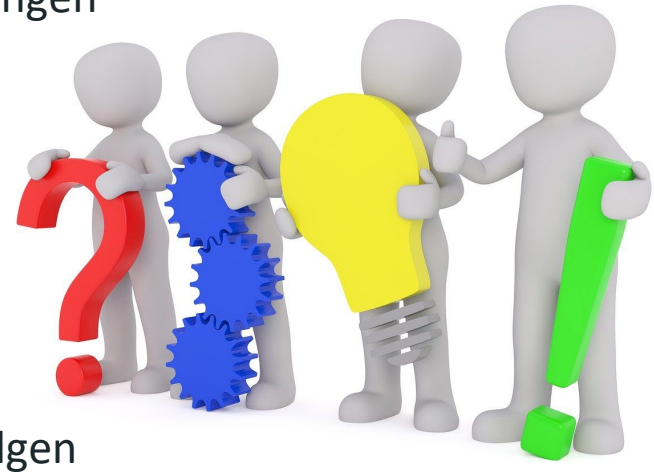
*Wie können wir uns bestmöglich vorbereiten?*

# Einleitung

- **Keine Frage mehr ob man angegriffen wird, sondern wann!**
  - JEDES Unternehmen ist ein potenzielles Ziel
- **Maßnahmen setzen um…**
  - Risiko eines erfolgreichen Angriffs zu minimieren
  - schnell und zielgerichtet zu reagieren
  - Auswirkungen eines Angriffs zu minimieren
- **Dem Chaos vorbeugen…**
  - mit organisatorischen Maßnahmen

# Einleitung

- **Offene Diskussion**
  - Mitmachen erwünscht
  - Individuelle Probleme erfordern individuelle Lösungen
- **Ihr Input ist für den Output wichtig**
  - Eigene Problemstellungen
  - Verschiedene Lösungen und ToDo‘s
- **Erarbeiten Sie Ihren individuellen Plan**
  - Arbeitsblätter für jedes Kapitel vorhanden
  - Wichtig: intern mit verantwortlichen weiter verfolgen



# DER LEITFADEN

*Die Ergänzung zu Ihrem technischen Sicherheitskonzept*

**CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen**

# Der Leitfaden

- **Zweck des Leitfadens**
  - Als Unternehmen im Angriffsfall handlungsfähig bleiben
  - Im Vorfeld diesbezüglich Gedanken machen
- **Gefördert durch DIH-Süd Kooperation**
  - **Ziel**: Unterstützung von KMUs gegen Cyberkriminalität
  - **Basis**: Interviews mit Expert*innen und Betroffenen
- **Disclaimer**
  - Regelmäßige individuelle Prüfung und Anpassung
  - Leitfaden ist eine Ergänzung zum techn. Sicherheitskonzept, kein Ersatz!
  - Professionelle Unterstützung im Angriffsfall wird empfohlen

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

## Geschäftsprozesse

# Der Leitfaden

## …Geschäftsprozesse identifizieren

- **Ziel**
  - Kritische Systeme & Geschäftsprozesse identifizieren
  - Risikoanalyse aller IT-bezogenen Komponenten
  - Diese Liste priorisieren → *„Was muss täglich laufen?!“*

## 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* |

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.<br>Zulieferer anfragen, ob Anlieferung verzögert werden kann. |

# Der Leitfaden

## …Arbeitsblatt Geschäftsprozesse

- **Gruppen:** 2-4 Personen
- **Zeit:** 15 min.
- **Angabe:**
  - Gehen Sie die aktuellen Arbeitsblätter allein oder gemeinsam in der Gruppe durch und versuchen Sie alle Fragen bestmöglich zu beantworten.
  - Versuchen sie Ihre eigenen individuellen Probleme und möglichen Lösungen zu identifizieren

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

## Geschäftsprozesse

## Dokumentation

# Der Leitfaden

## …Dokumentation offline bereitstellen

- **Frage**

  Habe ich im Angriffsfall Zugang zu Dokumenten und wichtigen Informationen?

  - Dokumenten, Auftragslisten, Kontaktdaten, Services, Tools, …

- **Ziel**

  - Essenzielle Dokumente und Informationen offline sichern
  - z.B.: wichtige Telefonnummern, Vorgehen im Angriffsfall, …
  - Am besten in Papierform an sicherer Stelle ablegen
  - Auf Zugänglichkeit und Aktualität der Dokumente achten!

## Arbeitsblatt *Dokumentation* (1/2)

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

| *Wen* | *Wofür* |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

Beispiel:

| | |
|---|---|
| Milchlieferanten | Änderung Anlieferungszeiten/-modalitäten |



## 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! |





# Der Leitfaden

## …Arbeitsblatt Dokumentation

- **Gruppen:** 2-4 Personen
- **Zeit:** 5 min.
- **Angabe:**
  - Gehen Sie die aktuellen Arbeitsblätter allein oder gemeinsam in der Gruppe durch und versuchen Sie alle Fragen bestmöglich zu beantworten.
  - Versuchen sie Ihre eigenen individuellen Probleme und möglichen Lösungen zu identifizieren

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- **Kommunikation**

# Der Leitfaden

## …Kommunikation planen

- **Fragen**
  - Wen rufen Sie ohne ein Telefon oder MS Teams an?
  - ..bzw. **WIE** rufen Sie irgendwen an?

- **Ziel**
  - Wichtig zu wissen, wen man wie kontaktieren kann
  - Wer darf Informationen weiterleiten?
  - Welche Informationen dürfen wohin?
    - Kolleg*innen, Kunden & Partner, Medien, …

# Der Leitfaden

## …Kommunikation planen - *Beispiele*

| WANN | WAS | WER (von wem?) | An WEN |
|---|---|---|---|
| So schnell als möglich | • Kurze Information das ein Hackerangriff passiert ist<br>• Vorläufige Stillschweige-Vereinbarung | z.B. HR | ALLE Mitarbeitende |
| So schnell als möglich | • Welche Anwendungen/Prozesse betroffen sind (sofern man das schon weiß) | z.B. IT | ALLE Mitarbeitende |
| So schnell als möglich, sofern Kunden-anwendungen betroffen sind | • Kurze Information das ein Hackerangriff passiert ist<br>• Welche Kunden-Anwendungen betroffen sind (sofern man das schon weiß)<br>• Das an der Behebung gearbeitet wird und laufend über neueste Erkenntnisse informieren wird<br>• Man kann auch seine Kunden/Partner um Stillschweigen bitten, bis Situation intern klar ist | z.B. zuständige Kundenbetreuende | Partner XY, Partner AB |

# Arbeitsblatt *Kommunikationswege*

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

| *Kommunikationsweg* | *Technische Voraussetzungen* | *Mögliche Alternativen* |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## 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,<br><br>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.<br><br>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.<br><br>Vielen Dank!<br>xxx | Personalabteilung | ALLE Mitarbeitenden |
| So schnell als möglich | Liebe Kundenbetreuende,<br>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:<br><xxxx><br>Vielen Dank!<br>xxx | Geschäftsführung | Kundenbetreuende |
| So schnell als möglich | Liebe Kolleginnen und Kollegen,<br>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:<br><xxxx><br>Vielen Dank!<br>xxx | Geschäftsführung | Kundenbetreuende, Hotline- bzw. Office-Mitarbeitende |

# Der Leitfaden

## …Arbeitsblätter Kommunikation

- **Gruppen:** 2-4 Personen
- **Zeit:** 10 min.
- **Angabe:**
  - Gehen Sie die aktuellen Arbeitsblätter allein oder gemeinsam in der Gruppe durch und versuchen Sie alle Fragen bestmöglich zu beantworten.
  - Versuchen sie Ihre eigenen individuellen Probleme und möglichen Lösungen zu identifizieren

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- **Notfallteam**

# Der Leitfaden
## …Notfallteam aufstellen

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

- **Ziel**
  - Notfall-Erstkontakt identifizieren
  - Krisenstab vorab bilden und Ersatz definieren
  - Leitung des Notfallteams definieren

## Quickcheck *Verantwortlichkeit*

Welche Person in Ihrem Unternehmen fällt Ihnen spontan ein, wenn sie an die Begriffe unten denken?

Schreiben Sie pro Begriff spontan eine Person auf! (Mehrfach-Nennungen möglich)

Vertrauenswürdig _____

Gewissenhaft _____

IT bzw. EDV-affin _____

Sicherheit _____

Cybersicherheit _____

Es fällt immer wieder der gleiche Name? Perfekt! Sprechen Sie mit dieser Person und ernennen Sie sie zum/zur Cyber-Security Beauftragten:

_____

## 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**<br>*– ruft das Krisen-Team zusammen und leitet die ersten Schritte ein*<br>*– ist primäre Ansprechperson für alle Fragen*<br>*– (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: | |



## 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** | | |

# Der Leitfaden

## …Arbeitsblatt Notfallteam

- **Gruppen:** 2-4 Personen
- **Zeit:** 5 min.
- **Angabe:**
  - Gehen Sie die aktuellen Arbeitsblätter allein oder gemeinsam in der Gruppe durch und versuchen Sie alle Fragen bestmöglich zu beantworten.
  - Versuchen sie Ihre eigenen individuellen Probleme und möglichen Lösungen zu identifizieren

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- **Vorgehensplan**

# Der Leitfaden

## …Vorgehensplan vorbereiten

- **Wenn alle anderen Fragen beantwortet wurden:**
  - Checkliste für den Ernstfall erstellen

- **Ziel:**

  *Checkliste mit*

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

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- Vorgehensplan
- **Weiteres**

# Der Leitfaden

## …Weiteres

- **Intro zur Aufgabe**
  - Je nach Branche, Versicherungsangebot in Betracht ziehen
  - Diese kann in allen Bereichen sofort unterstützen

- **Erklärung & Durchführung**
  - Versicherung im Angriffsfall immer sofort einbinden!

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- Vorgehensplan
- Weiteres

# ABSCHLUSS & AUSBLICK

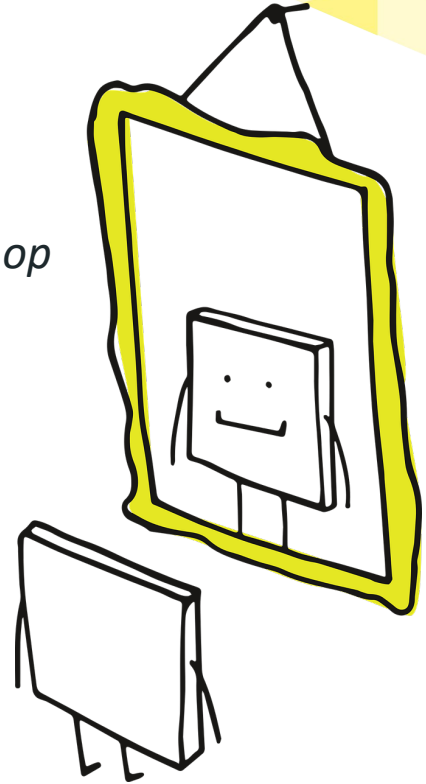
*Die Ergänzung zu Ihrem technischen Sicherheitskonzept*

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

# Abschluss & Ausblick

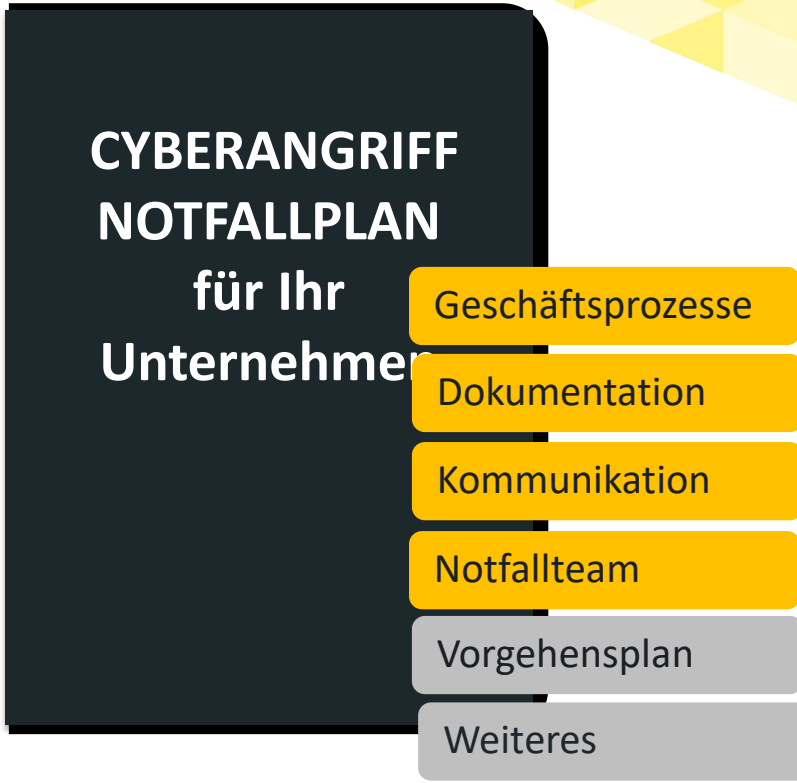
## …nach dem Angriff: Aufarbeitung des Vorfalls

- **Nach dem Angriff ist vor dem nächsten Angriff!**
- **Reflexion mit dem Kern-Team**
  - Was hätte besser laufen können? → *Lessons learned – Workshop*
  - Retrospektive (siehe Arbeitsblatt *Retrospektive* im Leitfaden)
  - Die Büropflanzen Frage (Perspektivenwechsel)
- **Reflexion mit dem Rest**
  - Siehe Leitfaden



# AGENDA

- Vorstellung & Sensibilisierung ✓
- Heutiger Fokus & Output ✓
- Der Leitfaden ✓
  - Geschäftsprozesse
  - Dokumentation
  - Kommunikation & Verantwortung
  - Vorgehen-Checklist
  - Versicherung & Rechtliches
- Abschluss & Ausblick ✓



# 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 →
- Design-Patterns →
- DevOps →
- AI-Fundamentals →
- IT-Projektmanagement →
- Strategisches IT-Management →
- Moderne Software Architektur →

# Vielen Dank