CYBERNOT
CYBERSECURITY NOTFALLPLAN

Berndt Jesenko, MSc
DI Harris Gerzic

Department IT & Wirtschaftsinformatik

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Vorstellung

Berndt Jesenko, MSC

Stv. **Department Leiter**
Forschung & Lehre
an der **FH Campus 02**

DI Harris Gerzic

Forschung & Lehre
an der **FH Campus 02**

Technik & Wirtschaft

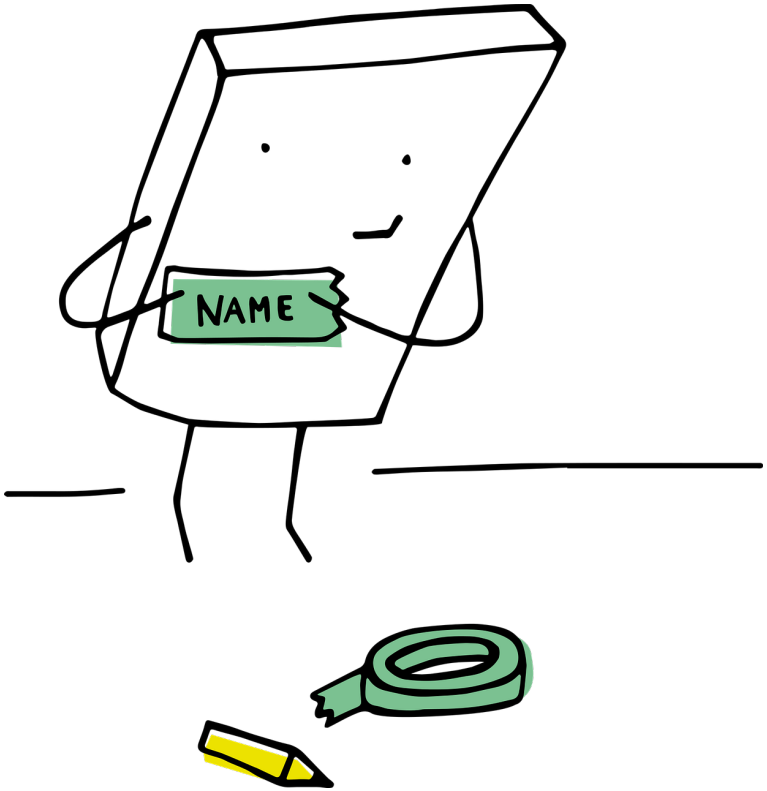
Studieren

Forschen

Department IT & Wirtschafts-informatik

Fortbilden

Vorstellung



- **Wir wollen Sie auch kennenlernen:**
  - Name
  - Unternehmen
  - Erwartungen an WS

Cyberangriff Szenario

…sofortige Reaktion erforderlich!

Es ist ein ganz normaler Arbeitstag in Ihrem Unternehmen. Plötzlich bemerken Sie, dass Ihre Systeme ungewöhnlich langsam reagieren. Kurz darauf erhalten Sie eine Nachricht, dass Ihre Daten verschlüsselt wurden und Sie nur durch Zahlung eines Lösegelds wieder Zugriff erhalten.

Welche ersten Schritte würden Sie unternehmen, um auf diesen Angriff zu reagieren? Wie würden Sie Ihre Daten und Ihr Unternehmen schützen?

Brainstorming 3-5 min. & Diskussion

Cyberangriff Szenario

…Fazit & Workshop Vorwort

- **Realität der Cyberangriffe**
  - Kein seltenes Ereignis!
- **Vorsorge und Reaktion**
  - Vorbereitung und Kenntnis über potenzielle Bedrohung
  - Proaktive Maßnahmen zur Risikominimierung
- ***Harvest now, decrypt later***
  - Verschlüsselung alleine reicht nicht → Strategie muss her!
- **Teamwork** → gemeinsam Handeln und Lernen
- **Empfehlung** → Leitfaden lesen und Empfehlungen ernst nehmen

Aktuelle Bedrohungen

…der Schaden ist schnell angerichtet

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

AGENDA

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

HEUTIGER FOKUS & OUTPUT

Wie können wir uns bestmöglich vorbereiten?

Heutiger Fokus

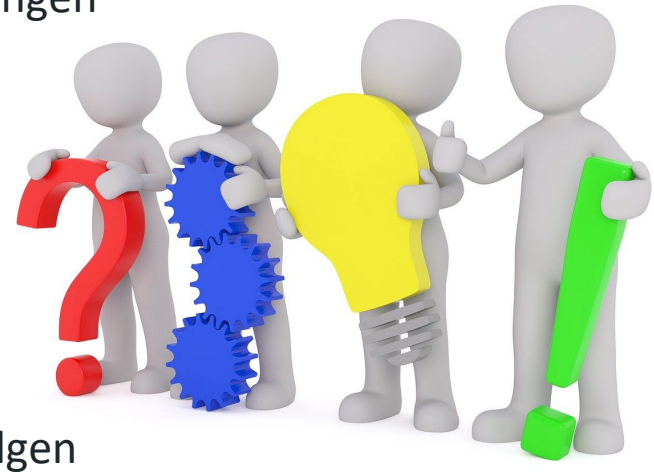
…wozu und wie vorbereiten?

- **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

Heutiger Output

…kommt ganz auf Ihren Input an

- **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



CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

DER LEITFADEN

Die Ergänzung zu Ihrem technischen Sicherheitskonzept

Der Leitfaden

…eine Empfehlung

- **Gefördert durch DIH-Süd Kooperation**
  - **Ziel**: Unterstützung von KMUs gegen Cyberkriminalität
  - **Basis**: Interviews mit Expert*innen und Betroffenen
- **Intention**
  - Bewusstseinsbildung und Dringlichkeit der Thematik
  - Schaffung von Interesse für präventive Maßnahmen
- **Disclaimer**
  - Regelmäßige individuelle Prüfung und Anpassung
  - Leitfaden Ergänzung zum techn. Sicherheitskonzept
  - Professionelle Unterstützung im Angriffsfall wird empfohlen

Der Leitfaden

…eine Empfehlung

Der Leitfaden

…zentrale Geschäftsprozesse absichern

- **Intro zur Aufgabe**
  - Als Unternehmen im Angriffsfall handlungsfähig bleiben
  - Im Vorfeld diesbezüglich Gedanken machen
- **Erklärung & Durchführung**
  - Kritische Systeme & Geschäftsprozesse identifizieren
  - Risikoanalyse aller IT-bezogenen Komponenten
  - Diese Liste priorisieren → *„Was muss täglich laufen?!“*
- **Diskussion der Ergebnisse**

Der Leitfaden

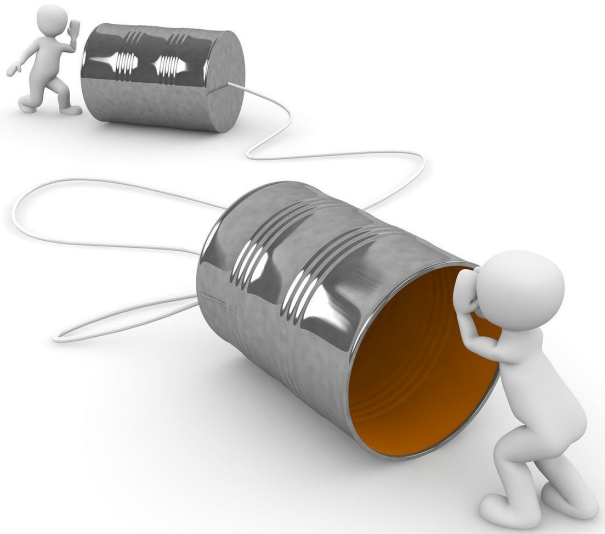
…Dokumentation offline bereitstellen

- **Intro zur Aufgabe**
  - Habe ich im Angriffsfall Zugang zu Dokumenten und wichtigen Informationen?
    - Dokumenten, Auftragslisten, Kontaktdaten, Services, Tools, …
- **Erklärung & Durchführung**
  - 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!
- **Diskussion der Ergebnisse**

Der Leitfaden

…Kommunikation planen

- **Intro zur Aufgabe**
  - Oft wird auf die Kommunikation vergessen!
  - Wen rufen Sie ohne ein Telefon oder MS Teams an?
  - ..bzw. **WIE** rufen Sie irgendwen an?
- **Erklärung & Durchführung**
  - Wichtig zu wissen, wen man wie kontaktieren kann
  - Wer darf Informationen weiterleiten?
  - Welche Informationen dürfen wohin?
    - Kolleg*innen, Kunden & Partner, Medien, …
- **Diskussion der Ergebnisse**



Der Leitfaden

…Verantwortlichkeiten klären (Notfallteam)

- **Intro zur Aufgabe**
  - Wer muss im Angriffsfall sofort Bescheid wissen?
  - Wer koordiniert die weiteren Abläufe?
  - Wer trägt die Verantwortung und entscheidet?
- **Erklärung & Durchführung**
  - Notfall-Erstkontakt identifizieren und abholen
  - Krisenstab vorab bilden und Ersatz definieren
  - Leitung des Notfallteams definieren
- **Diskussion der Ergebnisse**

Der Leitfaden

…Vorgehensplan vorbereiten

- **Intro zur Aufgabe**
  - Damit nichts vergessen wird, Checkliste erstellen
- **Erklärung & Durchführung**
  1. Analyse
     - Was ist passiert, was ist betroffen
  2. Angriff stoppen
     - Ausbreitung verhindern, Risko minimieren
  3. Krisenstab einberufen
     - Kommunikation & weiteres Vorgehen
- **Diskussion der Ergebnisse**

Der Leitfaden

…Versicherungen & Rechtliche Maßnahmen

- **Intro zur Aufgabe**
  - Je nach Branche, Versicherungsangebot in Betracht ziehen
  - Diese kann in allen Bereichen sofort unterstützen
  - Verantwortung kann hier abgegeben werden
- **Erklärung & Durchführung**
  - Versicherung im Angriffsfall immer sofort einbinden!
  - Nie ohne Versicherer auf eigene Faust handeln!
  - ..sonst droht möglicher Leistungsverlust
- **Diskussion der Ergebnisse**

ABSCHLUSS & AUSBLICK

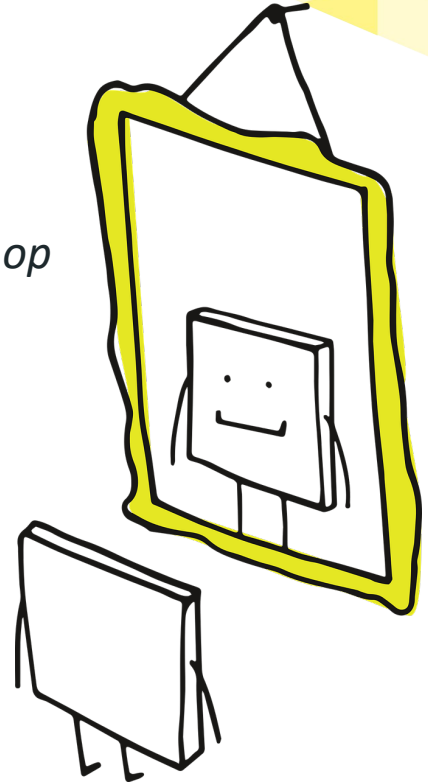
Die Ergänzung zu Ihrem technischen Sicherheitskonzept

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)
  - Die Büropflanzen Frage (Perspektivenwechsel)
- **Reflexion mit dem Rest**
  - Die *Happiness Door – Methode*
  - Fragebogen (Online oder Analog)
  - Aufruf um Rückmeldung per Mail oder Gespräch



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