Cybercrime- & Security im Unternehmenskontext

Vorstellung

Univ. Lect. Michael Walchshofer MSc MA MBA MBA MBA akad.BM

- **Studium** :

  MSC - Information und Security Management

  MA - Wirtschafts- und Organisationspsychologie

  akad. BM - Finanzmanagement

  MBA- General Management

- **Internationales Studium:**

  MBA - Corporate Governance & Management **(Boulder Universität Colorado)**

  MBA - Communication and Leadership – **(Pazifik University Anchorage Alaska)**

  PhD - Buddhistische Philosophie und Ethik PhD (**World Buddhist University Tibet, Nepal)**

Werdegang

Univ. Lect. Michael Walchshofer MSc MA MBA MBA MBA akad.BM

- Geschäftsführer / Eigentümer NAAC (New Age Audit & Consulting e.U)
- Head of Riskmanagment / Aufsichtsrat TMIA / Nodeventure (Crypto / Finanzsektor)
- Univ. Lect. Donau Universität Krems / Alpen Adria Universität Klagenfurt
- Lektor Fachhochschule Hagenberg (IEM)

ÜBERBLICK

- WHAT THE HELL IS CYBER CRIME ?
- AWARENESS – BEWUSSTSEIN SCHAFFEN
  - **Story Telling :** SICHERHEITSBEWUSSTSEIN AM ARBEITSTAG
- HERAUSFORDERUNGEN FÜR UNTERNEHMEN
  - **Beispiele aus der Praxis (live)**
- MITARBEITER = MIT ARBEITEN
- ZUSAMMENFASSUNG

WHAT THE HELL IS CYBER CRIME?

Eine *allgemein gültige* Definition dieses Begriffs **gibt es nicht**.

Üblicherweise versteht man darunter **alle Straftaten**, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden.

Wie kann es mich treffen?

Erpressung
Denial-of-Service Attacken
Ransomware

Reputationsverlust
Website Defacement
Fake News

Datendiebstahl
Hacking

Spionage
Social Engineering
Phishing

Missbrauch der IT
Crypto Mining

Sabotage
Stören des Geschäftsbetriebs
Ransomware

Betrug
CIO-Fraud
Fake President

Zahlen Daten Fakten

[Cybercrime Report 2021 (bundeskriminalamt.at)]

[Internetkriminalität (bundeskriminalamt.at)]

Können wir das mit Sicherheit sagen?

Ausprägungen von Cyberangriffen

Cyberrisiken - Haftungsszenarien für betroffene Unternehmen
PwC Österreich

März 2019
4

UNTERNEHMER AKADEMIE

Opfer ohne es zu wissen?

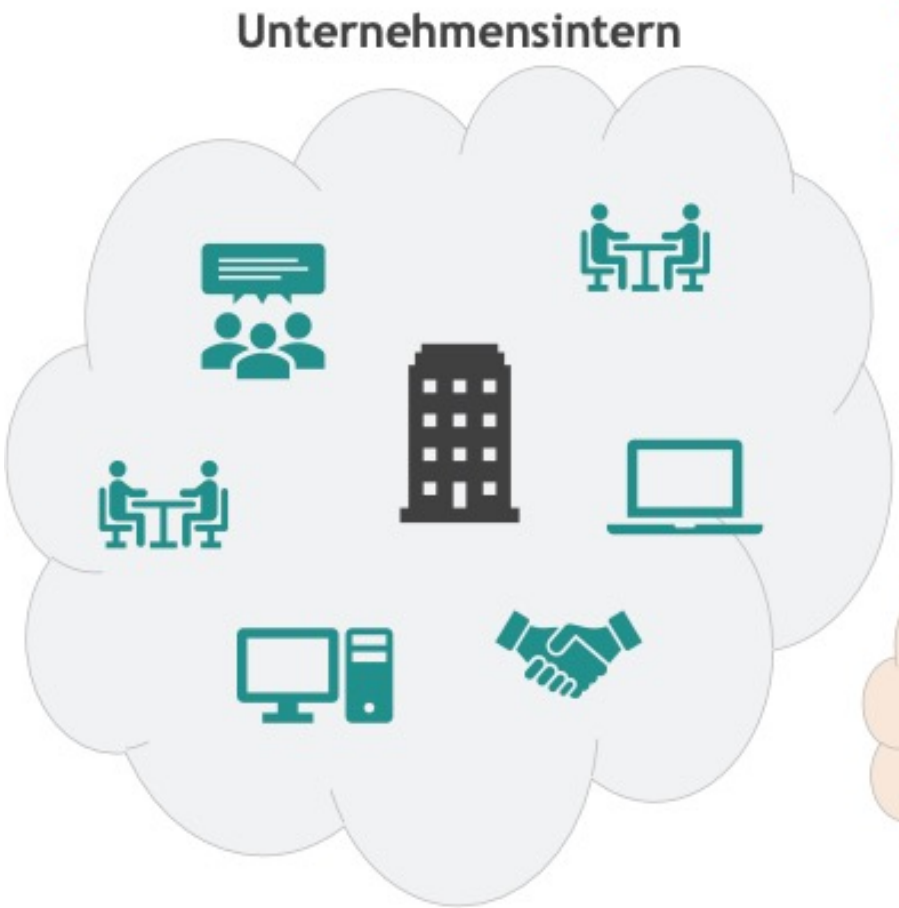
Nicht immer wissen wir Bescheid wenn unsere Daten oder Informationen verloren gehen:

Have I Been Pwned: Check if your email has been compromised in a data breach

Welche Herausforderungen haben Unternehmen?

HERAUSFORDERUNGEN FÜR UNTERNEHMEN

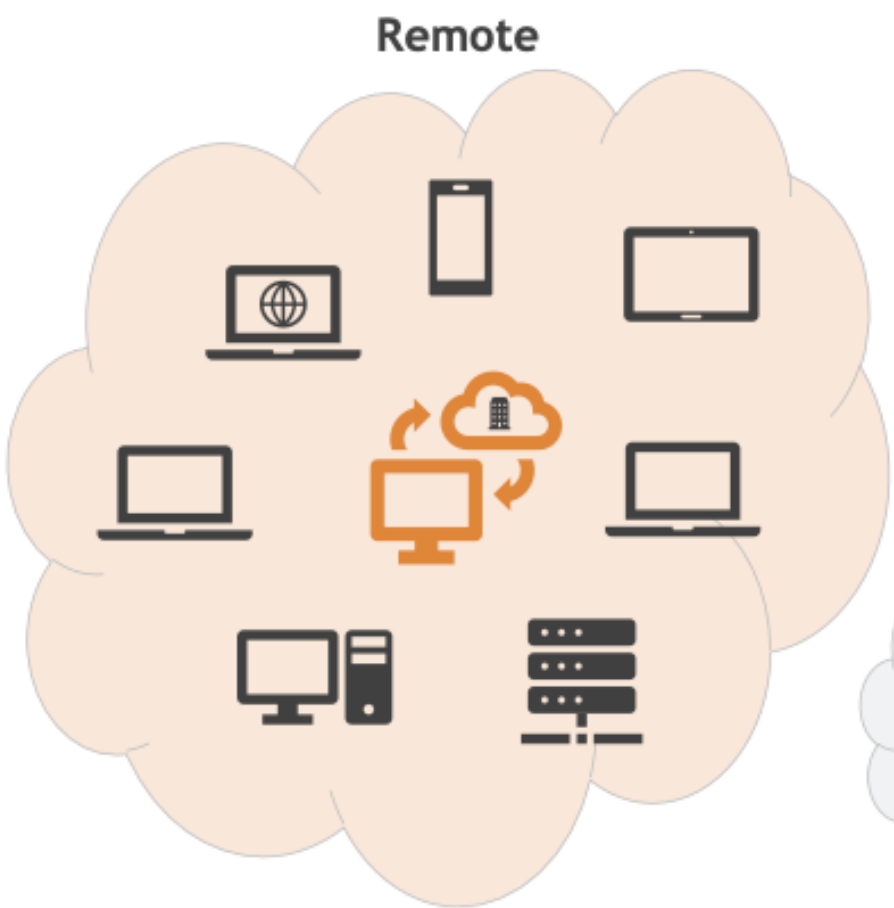
Das Unternehmen vor Covid 19



- Viele Mitarbeiter im internen Netzwerk
- Wenig Mitarbeiter extern
- Begrenzte Anzahl an Kanälen in das Unternehmensnetzwerk hinein
- Externe Zugänge:
  - Website, zum Teil von externen Dienstleistern gehostet
  - Webmail
  - Restriktives VPN

Remote

Das Unternehmen nach Covid 19



- Weniger Mitarbeiter direkt im Unternehmen
- Viele Mitarbeiter extern mit Zugängen zum internen Netzwerk
- Externe Zugänge:
  - Webmail für alle Mitarbeiter
  - Remote-Desktop-Verbindungen für alle Mitarbeiter
  - VPN oder ähnliches (z.B. Citrix) für alle Mitarbeiter
  - FTP-Server oder andere Lösungen für den Datenaustausch
- Mehrere Wege in das Unternehmensnetzwerk
  - Erhöhtes Risiko im Home-Office durch Phishing bzw. unbefugten Zugriff

Unternehmensintern

Beispiele aus der Praxis

Cyberangriffe aktuell heute 2022 - eine Übersicht | KonBriefing.com

FireEye Cyber Threat Map

Beispiele für Cyber-Schäden | KOSMICON

Aktuelle Angriffsvektoren

Faktor Technologie

- Schadsoftware (Ransomware)
- Denial of Service
- Schwachstellen in IT-Systemen

Faktor Mensch

- Social Engineering
- Phishing & Credential Fraud
- Fake-President Attack

Datensicherheit auch außerhalb der sicheren Mauern?

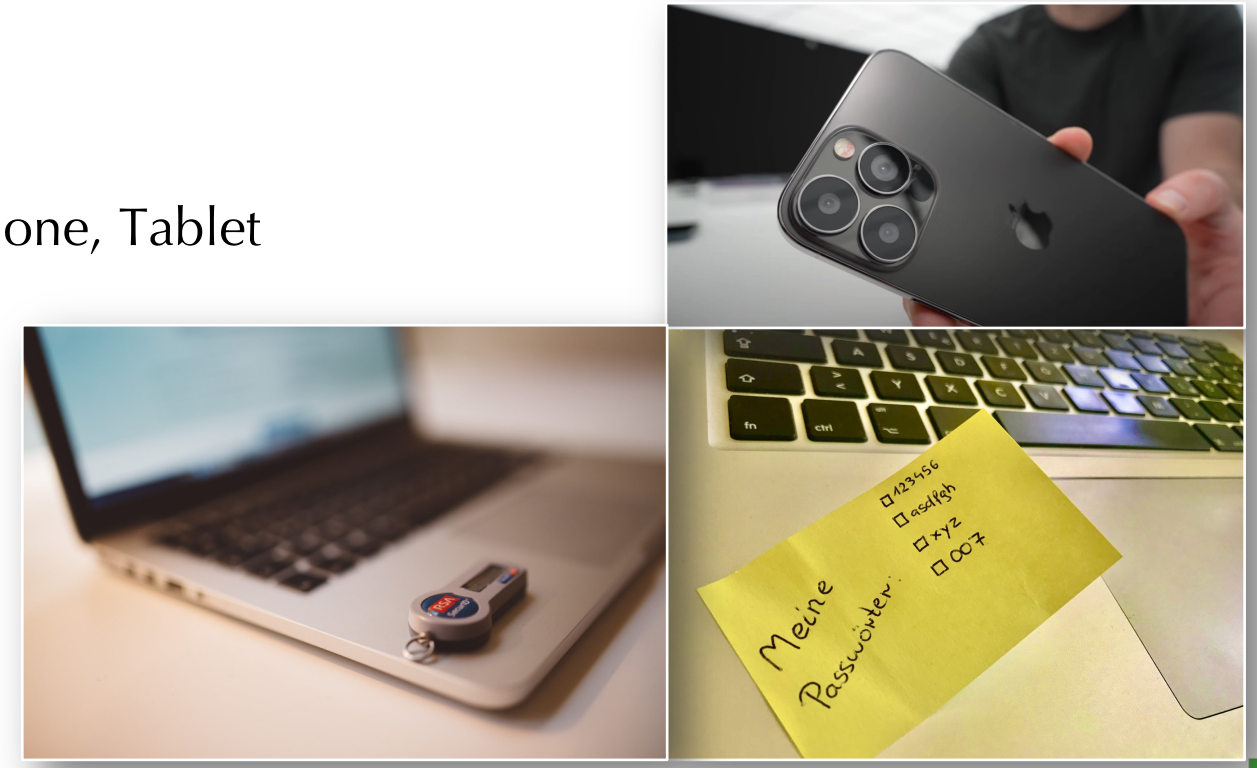
Das Home Office lässt für viele Unternehmen in Zeiten der Krise die Arbeitsabläufe fortsetzen. Es gilt aber die Risiken die daraus entstehen zu beachten und ernst zu nehmen:

- **Welche Unterlagen dürfen das Unternehmen überhaupt verlassen?**
- **Wie ist gesichert, dass die Dokumente nicht verloren gehen oder von Dritten eingesehen werden?**
- **Welches Gerät wird zum Arbeiten verwendet ? (berufliches / privates)**
- **Erfüllen die eingesetzten Geräte die Sicherheitsstandards wie im Unternehmen?**
- **Ist der Datentransfer gesichert und verschlüsselt?**
- **Wie erfolgt die Datenlöschung von Privatgeräten?**

AWARENESS – BEWUSSTSEIN SCHAFFEN

Security Awareness im beruflichen Arbeitsalltag = Ein **Sicherheits*bewusst*sein** wird entwickelt und gelebt, um Daten und Informationen **jeglicher Art** zu schützen:

- Am PC, Arbeitsplatz
- Auf mobilen Datenträgern
- Auf mobilen Devices: Laptop, Smartphone, Tablet
- Dokumente in Schriftform
- Mündliche Informationen
- Know-How



UNTERNEHMER AKADEMIE WIFI WKO

AWARENESS – BEWUSSTSEIN SCHAFFEN

Fakten zum **Sicherheits*bewusst*sein**:

- ***Risikofaktor Mensch:***
  Mehr als ***80% der Sicherheitsvorfälle*** resultieren aus dem Fehlverhalten der Mitarbeiter
- ***Grund:***
  Mitarbeiter sind meist unwissentlich die häufigste Schwachstelle
- ***Betroffen sind:***
  alle Unternehmen, in welchen Daten und Informationen ver- bzw. bearbeitet

AWARENESS – BEWUSSTSEIN SCHAFFEN

SICHERHEITSBEWUSSTSEIN AM ARBEITSPLATZ?

7:00 UHR: Ein Mitarbeiter sucht nach seiner Keycard und betritt das Unternehmen.

- ***Wer ist noch mit Ihm ins Gebäude gegangen?***
- ***Kennt er die Richtlinien zu den Zutrittssystemen?***
- ***Wie muss man sich bei Diebstahl oder Verlust der Zugangskarte verhalten soll?***
- ***Wie wäre die Weitergabe der Zugangskarte geregelt ?***

7:12 UHR: Der Mitarbeiter meldet sich am PC an und beginnt, E-Mails zu beantworten.

- ***Verwendet er das Passwort für mehrere Anwendungen? Etwa auch für private Anwendungen?***
- ***Wurde ein sicheres Passwort laut Passwort-Policy gewählt?***
- ***Wann haben Sie das Kennwort das letzte Mal gewechselt?***

AWARENESS – BEWUSSTSEIN SCHAFFEN

SICHERHEITSBEWUSSTSEIN AM ARBEITSPLATZ?

7:32 UHR: Der Mitarbeiter nimmt sich eine Kundenakte und beginnt zu arbeiten

- ***Warum liegt die Kundenakte auf dem Schreibtisch? Gibt's es eine Clear Desk Policy?***
- ***Wäre der Aktenschrank mit den Kundenakten verschlossen gewesen?***
- ***Gibt es hier Inhalt dieser Akte der als „vertraulich" zu behandeln ist?***

8:27 UHR: Er versendet ein Angebot per Mail.

- ***Handelt es sich um das aktuelle Angebot?***
- ***Hat er in der Eile die richtige E-Mail Adresse erwischt?***

AWARENESS – BEWUSSTSEIN SCHAFFEN

SICHERHEITSBEWUSSTSEIN AM ARBEITSPLATZ?

10:27 UHR: Der Mitarbeiter macht sich auf den Weg in den Besprechungsraum, wo in 3 Minuten ein Meeting mit dem Chef stattfindet.

10:28 UHR: Ein Kollege kommt ins Büro, sieht, dass sein Kollege wahrscheinlich bereits im Besprechungsraum ist und folgt ihr, um noch schnell ein Feedback einzuholen

- ***Warum weiß er das sein Kollege eine Besprechung hat? War der Bildschirm etwa nicht gesperrt?***
- ***Kann der Kollege im Besprechungsraum vertrauliche Daten erspähen, die nicht für ihn gedacht sind?***

12:45 UHR: Bei der Rückkehr vom Mittagessen wartet schon ein Kunde im Büro.

- ***Warum sitzt der Kunde schon allein in ihrem Büro?***
- ***Wer hat ihn hereingelassen?***
- ***Trägt der Kunde einen Besucherausweis?***

AWARENESS – BEWUSSTSEIN SCHAFFEN

SICHERHEITSBEWUSSTSEIN AM ARBEITSPLATZ?

15:55 UHR: Feierabend! Den Schlüssel legt der Mitarbeiter wie jeden Tag in die Schublade.

- ***Wo verstecken Sie ihre Schlüssel?***

16:00 UHR: Er verlässt das Unternehmen durch den Nebeneingang und lässt den freundlichen Handwerker herein, der vor der Tür wartet.

- ***Hat der Handwerker einen Auftrag, im Unternehmen zu arbeiten?***
- ***Wen hat er in der Vergangenheit bereits ins Unternehmen hereingelassen?***

AWARENESS – BEWUSSTSEIN SCHAFFEN

AUF EINEM BLICK:

UNTERNEHMER AKADEMIE

MITARBEITER = MIT ARBEITEN

- Was kann und was muss ich als MitarbeiterIn tun?
- Wie viel trage ich als MitarbeiterIn zur Sicherheit der Informationen bei?
- Worauf muss ich als MitarbeiterIn in Bezug auf Datensicherheit, Cyberbedrohungen in einer oft ungesicherten technischen und auch organisatorischen Umgebung besonders achten?

Was kann und was muss ich als MitarbeiterIn tun?

- Geheimhaltungspflicht und Datenschutz gelten IMMER - auch im Home-Office.
- Mitarbeiter sind verpflichtet, sich an die entsprechenden Weisungen des Arbeitgebers zu halten.
- Die Vorschriften des Arbeitsgesetzes zu Ruhezeiten, Verbot von Nacht- und Sonntagsarbeit gelten grundsätzlich uneingeschränkt auch im Home-Office
- Sicherheit geht uns ALLE an!!!!!

Zwei Prinzipien

1. „SICHERHEIT **DENKEN**, SICHERHEIT LEBEN“

2. „IMPLEMENTIERT ≠ VERSTANDEN ≠ GELEBT“

Wie viel trage ich als MitarbeiterIn zur Sicherheit der Informationen bei?

- Als Mitarbeiter haben sie einen wesentlichen Anteil zu Informationssicherheit.
- Ihr Home Office = Ihr Unternehmen. Richten Sie sich so ein dass Sie ungestört ohne „Zuhörer“ und „Zuseher“ arbeiten können.
- Nehmen Sie gelegentlich Kontakt mit der IT auf, um eventuelle Dinge zu klären oder auch um den Informationsfluss zu gewährleisten.
- Wenn Fehler passieren → **OFFENE Fehlerkultur**

Worauf muss ich als MitarbeiterIn achten?

- Besonders vorsichtig bei E-Mails von unbekannten Absendern zu sein.
- Keine Anhänge zu öffnen, nicht auf Links zu klicken und nur vertrauenswürdige Webseiten zu nutzen.
- Sofern sich anomales Verhalten Ihres IT Equipment bemerkbar macht (Smartphone, PC, Laptop) verständigen sie umgehend Ihren IT-Verantwortlichen.
- Keine ANGST vor Fehlern!
- Wenn Daten verloren gehen, ein Gerät nicht gefunden werden kann oder Informationen unabsichtlich geteilt wurden, melden Sie es der IT oder Ihrem Vorgesetzen.

Noch Fragen ?

Univ. Lect. Michael Walchshofer MSc MA MBA MBA MBA akad.BM
P: +43 664 1072288
M: michael.walchshofer@naac.eu
W: www.naac.eu

….cause we think business

UNTERNEHMER AKADEMIE