IT und Cybersicherheit

DIH- Süd

Forschung Burgenland

Agenda

- Organisatorisches
- Vorstellrunde der Teilnehmer
- Vorstellung des Vortragenden
- IT und Cybersicherheit allgemein
- Cyberthreats/Angriffvektoren
- Security Konzepte
- Spam und Phishing
- Schadsoftware/Malware
- Cyber-Resilienz
- Netzwerksicherheit
- Endpoint Security
- Nützliche Links und Quellen

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Organisatorisches

- **Kurze Kaffeepause (5min) um ca. 15:00 Uhr**
- **Fragen**
  - bitte in den Chat schreiben
  - oder bitte die Hand heben
- **Mikros und Videos**
  - Störungsvermeidung bitte Stummschalten und Abschalten der Videos
- **Folien**
  - Der Foliensatz wird auf Anfrage nach der Präsentation gerne zugesendet.

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Vorstellrunde

- **Bitte stellen Sie sich kurz vor:**
  - Name und Firma
  - Backround (Erfahrung) im Bereich IT und Cybersicherheit
  - Erwartungen an den Workshop

Vorstellung Vortragender

- **Clemens Gnauer**
- **Studium an der FH Burgenland**
  - Master Cloud Computing Engineering
  - Master Business Process Engineering – laufend
  - davor Bachelor WU
- **Forschung Burgenland**
  - seit 2018
  - seit April 2022 – Research Area Sustainable Innovation
  - davor CCPSS- Center für Cyber-Physical System Security
  - Schwerpunkte: Infrastrukturmanagement, Verteilte Netze, Cloud und IoT-Systeme, IT-Security
  - Projekte: AgriTec 4.0, BESTE-AB, Civis4Patria, DigTwin, etc.

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Forschung Burgenland

Standort
Pinkafeld

Standort
Eisenstadt

GEBÄUDE-TECHNIK

ENERGIE & UMWELT

SMART COMPUTING

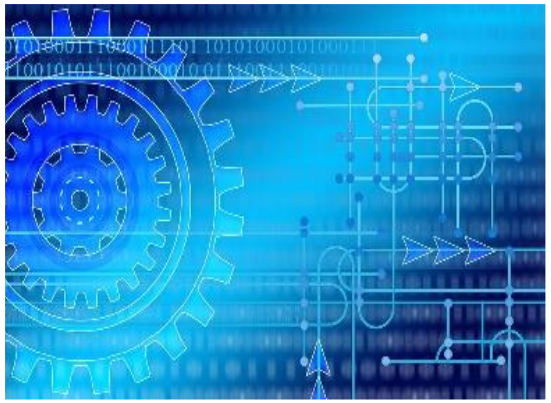
FORSCHUNG AN DER FH

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Sustainable Innovation - Themen

Digitalisierung



- Digitale Transformation
- Datenerfassung und Sensorik
- Cloudsysteme
- IT und Cyber Security
- IoT
- …

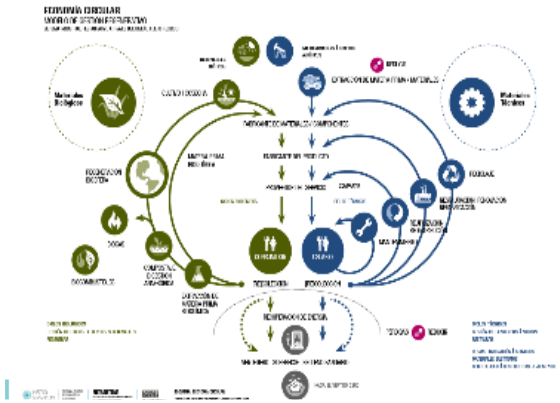
Energie

- Energieeffizienz & EE
- Energiemanagement
- Energiemonitoring
- Modellierung und Kennzahlenberechnung
- Messung & Verifizierung
- …

Klima

- Klimaneutralität
- Nachhaltigkeit
- THG Bilanzierung
- ..

Kreislaufwirtschaft

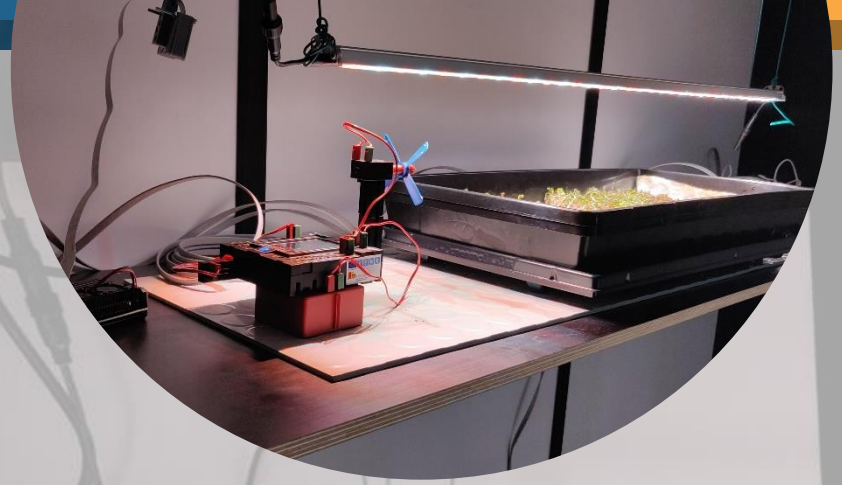


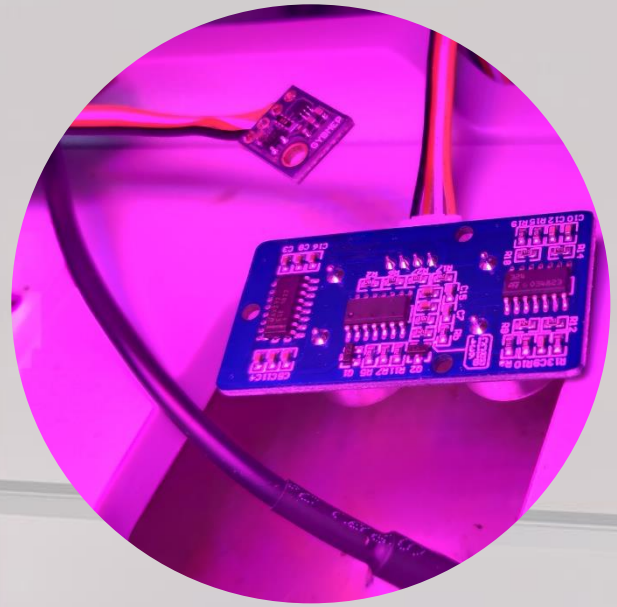
- Begrenzte Rohstoffe:
  - Reuse/Redistribute, Refirbish/Remanufacture, Recycle
- Erneuerbaren Rohstoffe:
  - Vertical Farming
  - Aquaponik

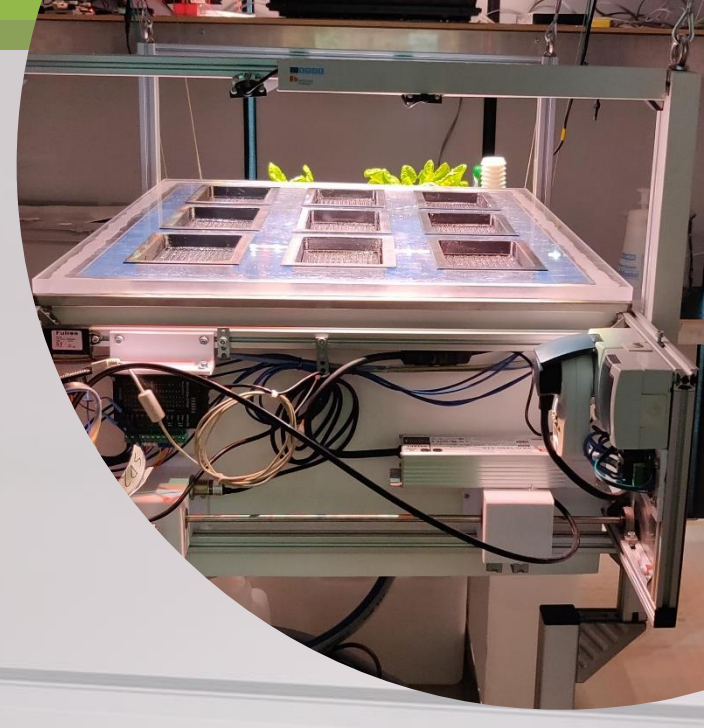
DIH SÜD

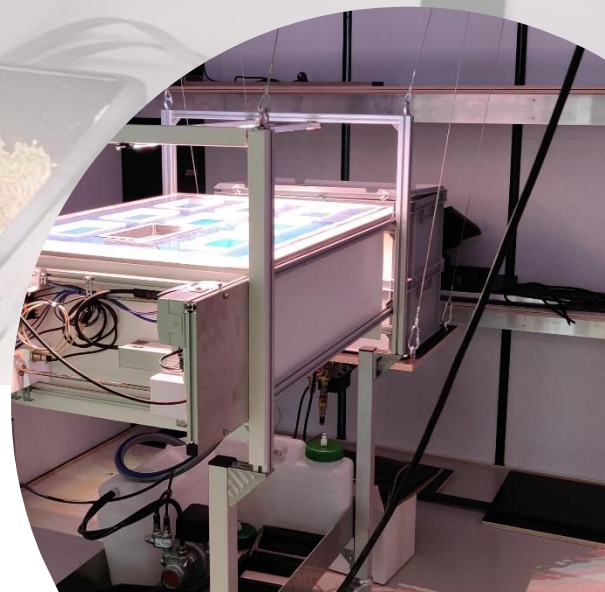
FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Verwendeten Technologien, Methodiken und Tools









Verwendeten Technologien, Methodiken und Tools

Logistics

Transport

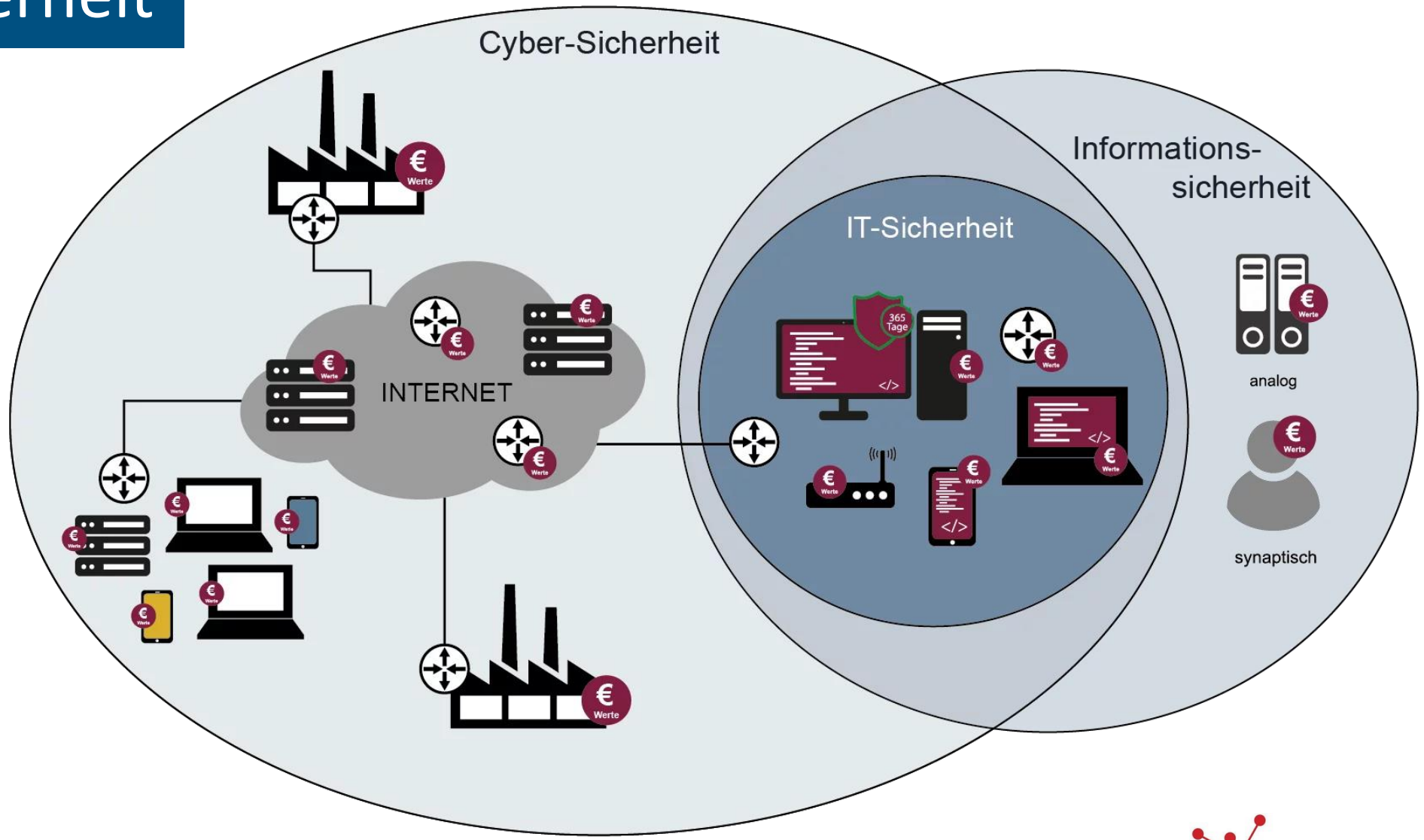
Agriculture

Surveillance and Inspection

Verwendete Technologien, Methoden und Tools

Construction

IT-Sicherheit



Quelle: https://norbert-pohlmann.com/wp-content/uploads/2022/02/it-sicherheit-zusammenhang.png

IT-Sicherheit

- Die IT-Sicherheit (IT-Security) bezieht sich auf die **Gewährleistung von Sicherheit aller** eingesetzten **Informationstechniken bzw. -technologien** (IT), d.h. aller Hardware- und Softwaresysteme bzw. aller Rechner- und Netzsysteme.
- Ziel ist die **Sicherheit der Informationsverarbeitung** und der **Kommunikation**, **die korrekte Abläufe** der **Hardwareoperationen** und der **Software- bzw. Programmsysteme** voraussetzt.
- Somit soll auch die **Daten- bzw. die Informationssicherheit** durch die IT-Sicherheit **gegeben** sein. Die **IT-Sicherheit** soll schließlich die **Sicherheit** bzw. **Korrektheit** aller Anwendungen **gewährleisten**, die durch IT unterstützt bzw. ausgeführt werden.

Quelle: https://www.gabler-banklexikon.de/definition/it-sicherheit-70719

Cybersicherheit

- Cyber-Sicherheit befasst sich mit allen **Aspekten der Sicherheit** in der **Informations- und Kommunikationstechnik**.
- Das **Aktionsfeld** der Informationssicherheit wird dabei auf den **gesamten Cyber-Raum** ausgeweitet. Dieser umfasst sämtliche mit dem **Internet** und **vergleichbaren Netzen** verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.
- Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132798

CIA-Triade

Confidentiality
(Vertraulichkeit)

Availability
(Verfügbarkeit)

Integrity
(Integrität)

CIA-Triade

- **Confidentiality (Vertraulichkeit)**
  - Zugriff auf und Änderung von Daten nur durch autorisierte Benutzer und Prozesse möglich
- **Integrity (Integrität)**
  - Versehentliches oder mut-/böswilliges ändern von Daten sollte unterbunden werden
  - Die Daten sollten immer im korrekten Zustand gehalten werden
- **Availability (Verfügbarkeit)**
  - Zugriff auf Daten sollte jederzeit für autorisierte Benutzer möglich sein

Oft erweitert um

- **Authentifizierung**
  - Feststellung der Identität (Echtheit) von Benutzern
- **Autorisierung**
  - Ermöglicht Benutzern (nach bestätigter Identität) für sie festgelegten Zugriff auf Daten

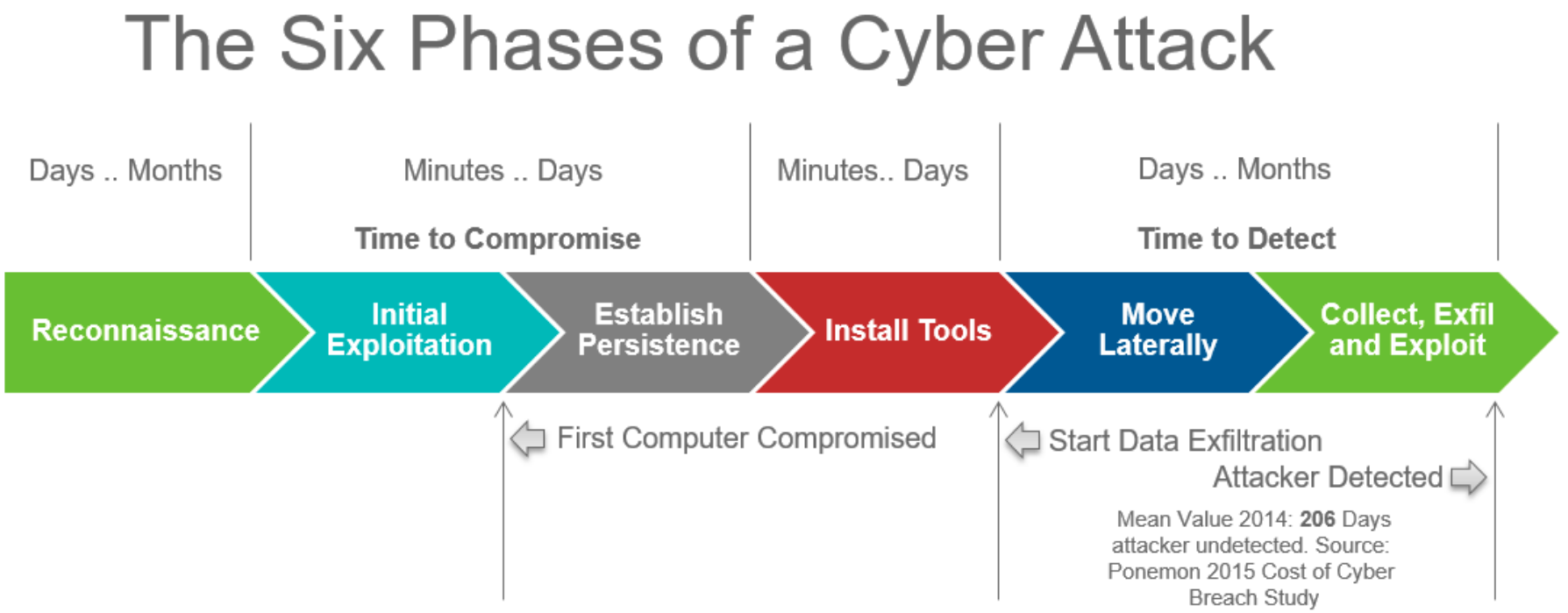
Cyberattacke - Attacken

- **Netzwerk Hacking**
- **Passwort Hacking**
- **Backdoors**
- **Viren, Würmer, Malware etc.**
- **Denial of Service / Distributed DoS**
- **IP-Spoofing**
- **Man-in-the-Middle**
- **SQL-Infections**

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Cyberattacke - Phasen



Quelle: https://klausjochemdotme.files.wordpress.com/2016/04/sixphasescyberattack.png

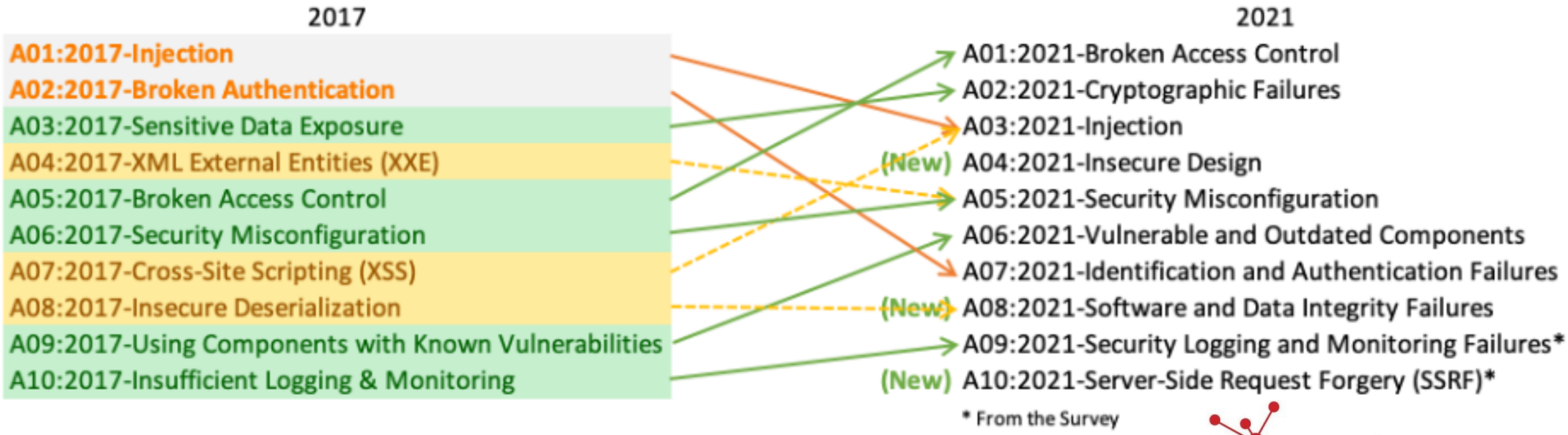
Cyberthreats - allgemein

- **Angriffe auf IT-Systeme**
  - DOS-Attacke, Phishing, Malware
  - IoT-Systeme
- **Angriff auf Endgeräte**
  - Datendiebstahl
  - Datenverlust
- **Kompromittierte Authentifizierung**
- **Account hijacking**
- **Social Engineering/Social Hacking**
  - Angriffe durch Insider
- **Bedienfehler durch User/Böswilligkeit**
- **Applikation/System-Fehler**

OWASP -Open Web Application Security Project

OWASP

- **Verbesserung der Security von Software**
- **Open-Source**
- **Fokus auf Cybersecurity und Webdevelopment**



OWASP – TOP 10 2021

- **Broken Access Control**
- **Cryptographic Failures**
- **Injection**
- **Insecure Design**
- **Security Misconfiguration**
- **Vulnerable and Outdated Components**
- **Identification and Authentication Failures**
- **Software and Data Integrity Failures**
- **Security Logging and Monitoring Failures**
- **Server Side Request Forgery (SSRF)**

Cyberattacke - Angreifer

- **Cyber-Aktivisten**
- **Cyber-Kriminelle**
- **Script Kiddies**
- **Gezielte Spionage**
- **Geheimdienste**
- **Staatliche Angriffe**
- **Cyber-Terroristen**

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Basiselemente der IT-Sicherheit

- **Updates**
  - Regelmäßig
  - Umfassend
- **Passwörter**
- **Zwei-Faktor-Authentisierung**
- **Virenschutzprogramm**
- **Firewall**

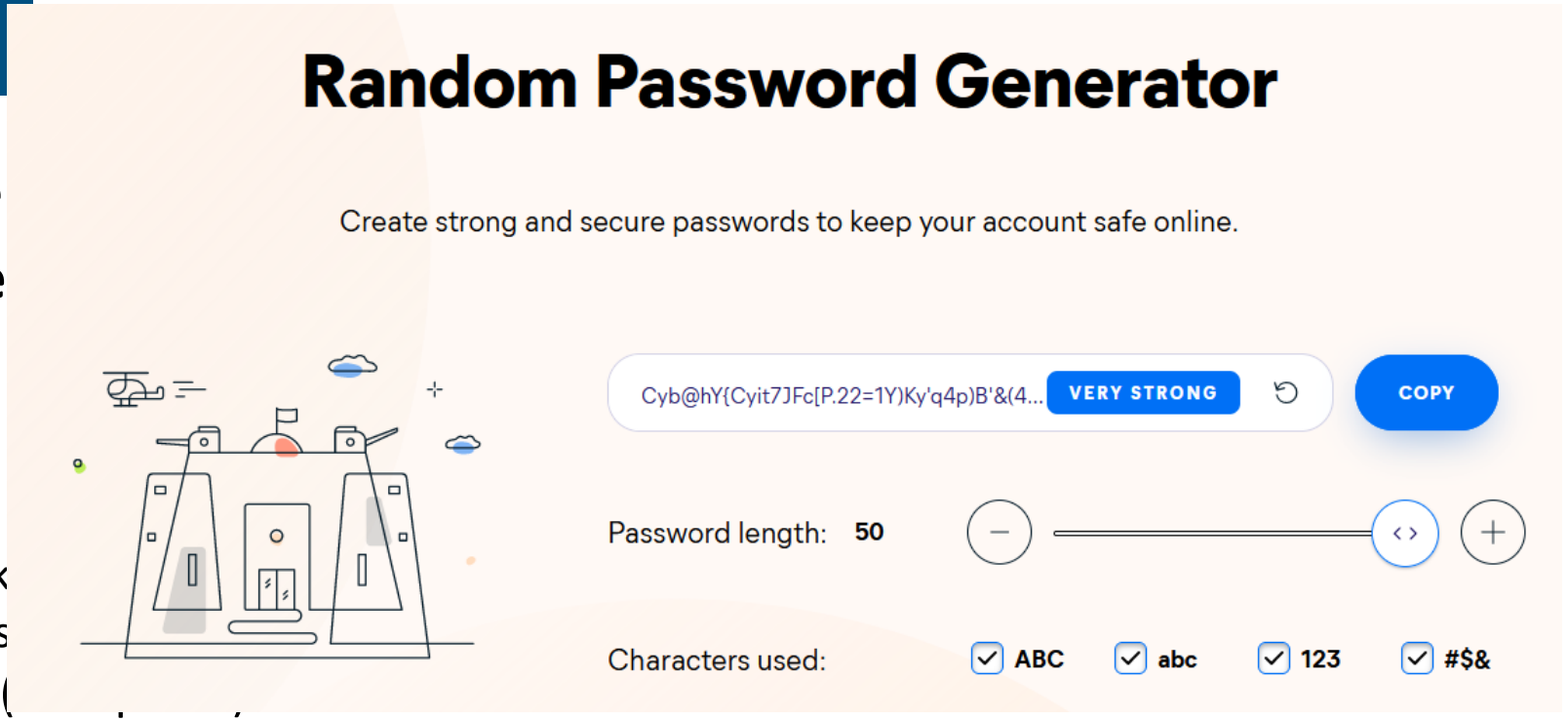
- **BSI – Link**

Maßnahmen - allgemein

- **4-Augen-Prinzip einhalten – Fehlervermeidung/No-Trust**
- **Passwort Regeln festlegen und einhalten**
  - Mindestens 12 Zeichen, 1 Klein- und 1 Großbuchstabe, 1 Ziffer, 1 Sonderzeichen
  - Eine Möglichkeit:
    - Mein Name ist Fritz und ich habe 4 Kinder 2 Hunde und hätte gerne 7 Autos. MniFuIh4K2huhg7A!%
    - „relativ“ einfach zu merken
    - Starkes, individuelles Passwort
  - Schulung der Mitarbeiter (Akzeptanz)

Maßnahmen - allgemein

- **4-Augen-Prinzip einhalte**
- **Passwort Regeln festlege**
  - Mindestens 12 Zeichen, 1
  - Eine Möglichkeit:
    - Mein Name ist Fritz und
      MniFuIh4K2huhg7A!%
    - „relativ“ einfach zu merk
    - Starkes, individuelles Pas
  - Schulung der Mitarbeiter (
  - Noch besser Passwort-Generatoren:
    - https://www.avast.com/random-password-generator#pc
    - https://delinea.com/resources/password-generator-it-tool
- **Password Manager verwenden**
  - Keepass, Lastpass, Dashlane, Bitwarden, KeyStore, uvm
- **Multifaktor-Authentifizierung**



Spam und Phishing

- **Spam:**
  - Formen von unerwünschten E-Mails (Werbung)
  - Massenhaft versandt
  - Oft mit „bösen“ Absichten

- **Phishing:**
  - Form von Spam
  - Häufig (Ph)Fischen nach Passwörtern
  - Betrugsversuche aller Art (Kontodaten/abbuchungen, Trickbetrug, Datendiebstahl)
  - Häufig „perfekt“ kopierte Mail Templates

Aktuelle Beispiele

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangerheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

Mit freundlichen Grüßen
Ihr PayPal Kundensupport

Volksbanken Raiffeisenbanken

Sehr geehrte Damen und Herren,

eider kam es in letzter Zeit vermehrt zu Problemen
nit den hinterlegten Kontaktdaten unserer Kunden,
daher bitten wir sie ihre bereits hinterlegten angaben
n unserem Kundencenter abzugleichen.

Jm einer vorsorglichen Abgleichs Sperrung ihres Kontos
unsererseits entgegenzuwirken, empfehlen wir ihnen
den Abgleich schnellstmöglich selbst durchzuführen.

Klicken Sie dafür einfach auf »Zum Formular« und folgen
anschließend den Anweisungen die ihnen im Kundencenter
angezeigt werden.

Mit freundlichen Grüßen,
hre **»Volksbanken-Raiffeisenbanken«**

»Zum Abgleich«

amazon

Sehr geehrt [redacted]

wir, das Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst.
Aus diesem Grund ist es vonnöten eine routinemäßige Sicherheitskon

Der Datenabgleich dient dazu, dass Ihre persönlichen Daten fortdauer
So können wir Sie unter anderem vor Missbrauch durch Dritte schütze

Sollte einer Abweichung der hinterlegten Daten vom System erkannt
gesperrt und von einem Mitarbeiter schriftlich informiert.

Wir bitten Sie Ihre Daten binnen 48 Stunden vollständig zu verifizieren

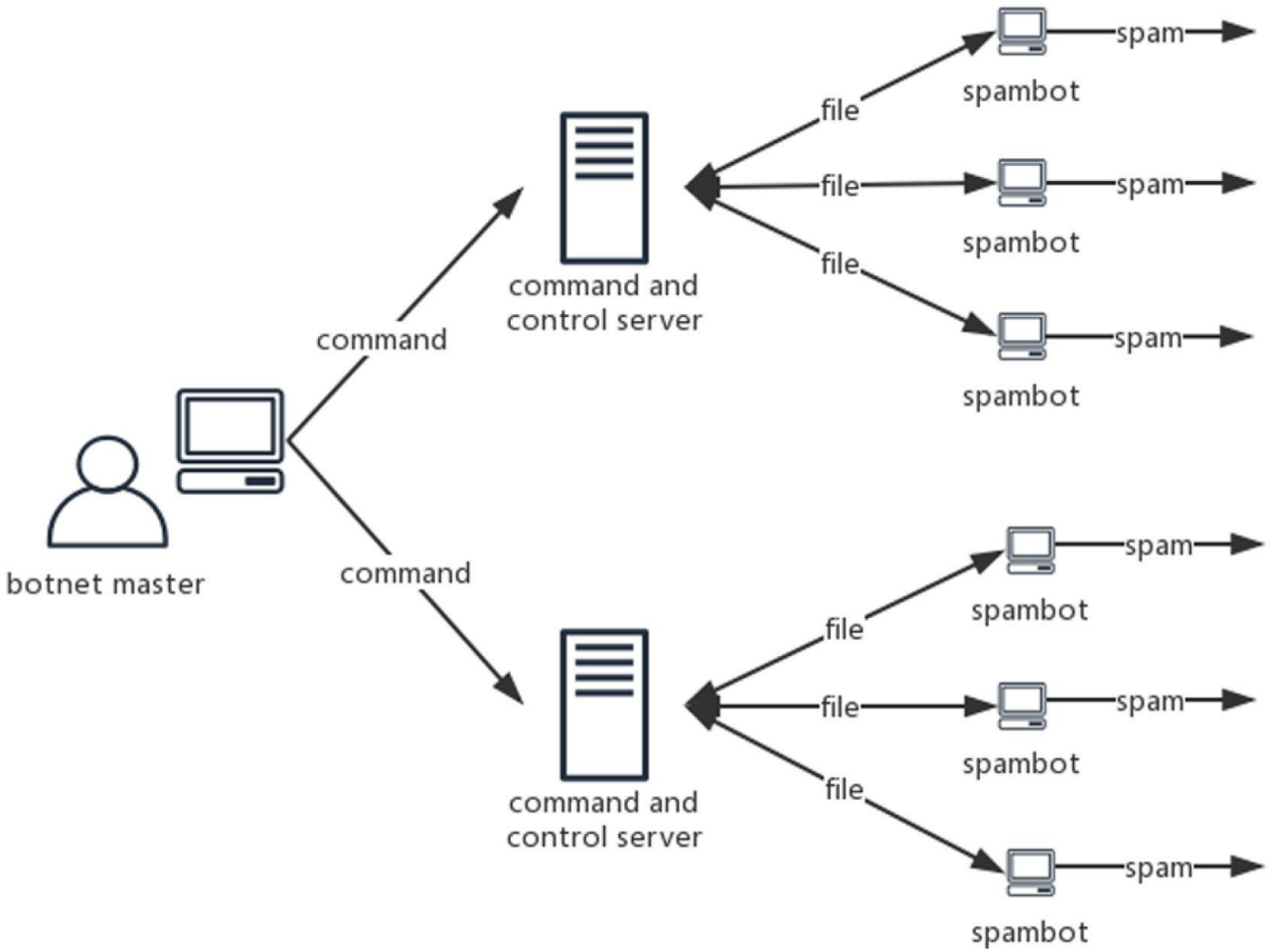
Weiter zur Verifizierung

mit freundlichen Grüßen,
Ihr Amazon-Kundenservice

Dies ist eine automatisch versendete Nachricht. Bitte antworten Sie nicht auf dieses
Versendung von E-Mails eingerichtet ist.

Prime Day ist Montag, 15. Juli
& Dienstag, 16. Juli
Ein zweitägiges Feuerwerk voller toller Angeb
Entertainment-Events und vieles mehr
Machen Sie sich bereit

Spambot-Netz



Quelle: Wang, M., & Song, L. (2021). Efficient defense strategy against spam and phishing email: An evolutionary game model. *Journal of Information Security and Applications*, *61*, 102947.

Phishing- Maßnahmen

- **Software regelmäßig updaten**
- **Installation von Antivirensoftware**
- **Skepsis bei E-Mails (Schulung der Mitarbeiter)**
  - Absender nicht bekannt
  - Bank, Diensteanbieter oder Behörden bitten niemals um persönliche Daten per Mail (über Link)
- **Änderungen von Passwörtern/Überweisungen nie über Links in E-Mails durchführen**
  - Immer direkt auf der Website des Diensteanbieters einloggen (nie über Link)
- **Bei Zweifel Absender extra, z.B. telefonisch kontaktieren und nach Echtheit fragen**
  - Telefonnr. Nie aus E-Mails übernehmen, sondern selbst googlen
- **Vorsicht bei Anhängen mit .exe oder .scr Ändungen**
  - Oftmals Endungen wie **wichtigesdokument.pdf.exe**
- **2-Faktor Authentifizierung verwenden**

Was tun bei einem Phishing - Vorfall?

- **Sperren des Bank- oder Emailkontos**
- **Umsätze kontrollieren und mit Bank/Anbieter in Verbindung setzen**
- **Vergeben eines komplett neues Passwort oder 2-Faktor Authentifizierung verwenden**
- **Kein Geld an kriminelle zahlen**
- **An Polizei oder Verbraucherzentrale (und Rechtsberatung) wenden**
- **Anzeige erstatten**

Ransomware

- **Malware**
  - Abkürzung für „Malicious (bösartige) Software“
  - Computerwürmer, Trojaner, Ransomware, etc.
- **Ransomware**
  - Eine Art Schadprogramm
  - Schränkt den Zugriff auf Daten und Systeme ein
    - durch Zugriffssperre der Nutzer – Locker-Ransomware
    - durch Verschlüsselung der Daten – Crypto-Ransomware
  - Betrüger verlangen Lösegeld für die Freigabe der Daten
  - Grundsätzlich können alle Systeme betroffen sein
  - Beispiele: wannacry (Mai 2017), petya (2016–2017), locky

Ransomware- Maßnahmen

- **Top 10 Ransomware Maßnahmen**
  - Patches und Updates
  - Remote Zugänge
  - E-Mails und Makros
  - Ausführen von Programmen
  - Virenschutz
  - Administrator Accounts
  - Netzwerk segmentieren
  - Backups und Datensicherheitskonzept
  - Netzlaufwerke
  - Notfallplan
- **Maßnahmenkatalog BSI**

BSI - Top 10 Ransomware Maßnahmen

- **Patches und Updates**
  - Ausnutzung von Schwachstellen in Software gehört zu drei häufigsten Einfallsvektoren von Ransomware
  - Updates sollten unverzüglich nach Bereitstellung durch Softwarehersteller eingespielt werden
  - Idealerweise über zentrale Softwareverteilung
  - Hohe Priorisierung von Updates von Schwachstellen mit hoher Kritikalität (Firewall, Webserver)
- **Remote Zugänge**
  - Zugriff von Außen absichern über VPNs und Zwei-Faktor-Authentisierung
- **E-Mails und Makros**
  - Darstellung von E-Mails als Text („Nur-Text“ bzw. „reiner Text“)
  - Webadressen werden in der Textdarstellung nicht verschleiert
  - Unterdrückung der Ausführung von aktiven Inhalten über HTML-Mails
  - Folgende Einstellung unter MS-Office
    - JS/VBS: automatisches Ausführen bei Doppelklick verhindern
    - Makros im Client (per Gruppenrichtlinie) deaktivieren
    - Vertrauenswürdige Orte für Makros im AD konfigurieren
    - Signierte Makros verwenden

BSI - Top 10 Ransomware Maßnahmen

- **Ausführen von Programmen**
  - Application Whitelisting ermöglicht nur das Ausführen von freigegebenen Programmen
  - Ausführen von Programmen nur in Verzeichnissen, die nicht durch den Benutzer beschreibbar sind (Execution Directory Whitelisting)
- **Virenschutz**
  - Lokale Antiviren-Software meist nicht effektiv gegen neue Varianten von Ransomware
  - Daher nutzen von Intrustion Prevention (IPS)-Modulen und Cloud Diensten von Anti-Virussoftware
- **Administrator Accounts**
  - Privilegierte Accounts sollten nur Admintätigkeiten durchführen (Kein Lesen von Mails, kein Surfen im Internet)
  - Technische Trennung von normalen Nutzerkonten und Adminkonten
  - Zwei-Faktor-Authentisierung sollte immer bei Adminkonten verwendet werden
  - Keine Domain-Adminkonten für die Administration von Clients

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

BSI - Top 10 Ransomware Maßnahmen

- **Netzwerk segmentieren**
  - Hilft zur lokalen Eindämmung von Ransomware angriffen
  - Wichtig: Verwendung von Admin-Accounts
- **Backups und Datensicherheitskonzept**
  - Schutzmaßnahme zur Wiederherstellung von Daten bei Ransomwarevorfall
  - Sicherung der Daten in Offline-Backup
  - Nach Backupvorgang Trennung der Backups von den Netzwerken
  - Wichtig: Planung des Wiederanlaufs und der Rücksicherung der Daten (Praxistests)
- **Netzlaufwerke**
  - Wichtige Daten immer auf Netzlaufwerk ablegen mit zentraler Datensicherung
  - Wichtige Dokumente nie nur lokal
  - Nutzerrechteverwaltung(Schreib/Leserechte)
- **Notfallplan**
  - Plan für den Worst-Case
  - Wiederherstellung kritischer Infrastruktur regelmäßig üben
  - Alternative Kommunikationsmöglichkeiten

Cyber-Resilienz

- **Widerstandsfähigkeit gegen**
  - Gefahren aus dem Internet und ähnlichen Netzen und Protokollen
  - Ausfall von Systemen/Services
  - Herausforderungen der Zukunft
- **Ausfallsicherheit gegen Angriffe durch**
  - Business Continuity
  - Desaster Recovery
  - Prozesse für Resilienz einführen
- **Maßnahmen**
  - Backup
  - Netzwerksegmentierung (Eindämmung der Ausbreitung)
  - Regelmäßige Übungen von Desaster Recovery
    - Bsp.: Chaos Monkey - Netflix

IT- Sicherheitshandbuch

- **Behandelt gesamten Bereich der Informationssicherheit**
- **Sicherheit von Hardware und Software**
- **Zur Speicherung , Verarbeitung und Übertragung von Informationen**
- **Bauliche und personelle Fragen zum Thema Sicherheit im IKT-Bereich**

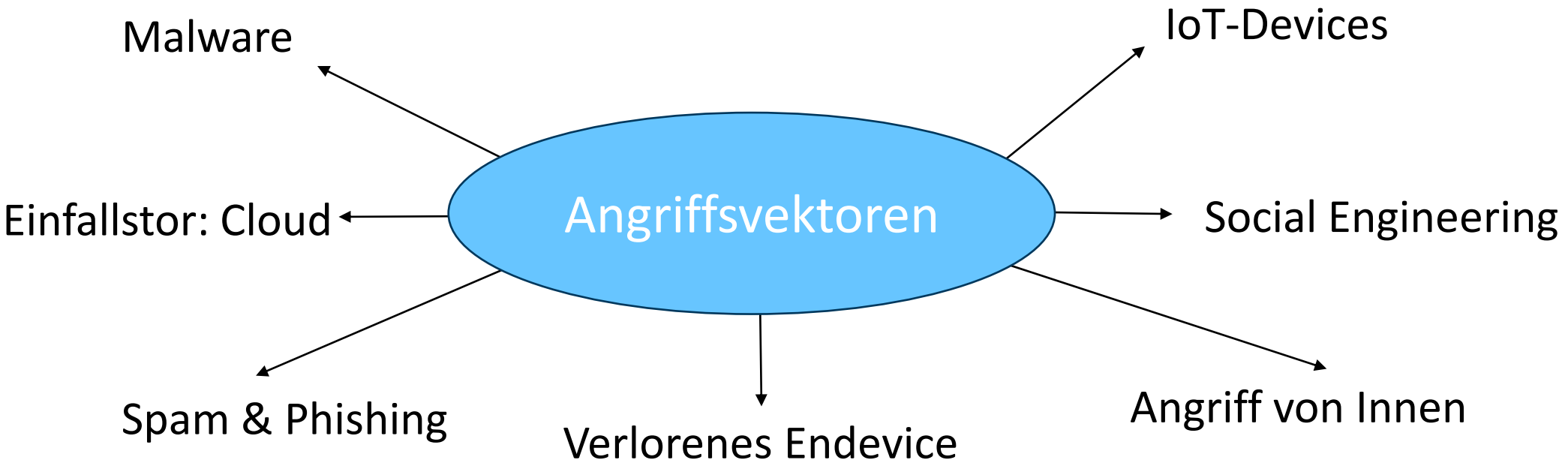
- Link zum PDF
- Link zur Website
- **Checklisten**
  - IT-Sicherheit auf einen Blick
  - Sicherheit im Home-Office
  - Sichere Passwörter

CHECKLISTE SICHERE PASSWÖRTER

Sichere Auswahl und Handhabung von Passwörtern
Für Behörden, Institutionen, Unternehmen und auch Privatanwender/innen

ID	AKTIVITÄT	STATUS	
I	PASSWORT-FESTLEGUNG		
01	Auswählen starker und zufälliger Passwörter die schwer zu erraten sind.	OK	KO
02	Das Passwort sollte trotz Komplexität gut merkbar sein.	OK	KO
03	Im Idealfall Passwörter mittels geeigneter Hilfsprogramme automatisch generieren.	OK	KO
04	Das Passwort soll Großbuchstaben enthalten.	OK	KO
05	Das Passwort soll Kleinbuchstaben enthalten.	OK	KO
06	Das Passwort soll Ziffern enthalten.	OK	KO
07	Das Passwort soll Sonderzeichen enthalten.	OK	KO
08	Die Passwortlänge sollte dem Einsatzzweck angemessen sein, also mindestens neun Zeichen für Online-Dienste und entsprechend mehr für sensible Online-Dienste (z.B. solche mit personenbezogenen oder finanziellen Daten, Cloud-Dienste) und Offline-Anwendungen/-Verschlüsselung.	OK	KO
09	Keine Standard-Passwörter oder gängige Muster bzw. leicht zu erratende Wörter verwenden (z.B. 123456, passwort, qwertz, asdfgh, admin).	OK	KO
10	Kein triviales Passwort mit einer simplen Ergänzung verwenden, z.B. durch Anhängen eines Rufzeichens oder Ziffern.	OK	KO
11	Keine persönlichen Details verwenden, die Dritten bekannt sein können (z.B. Name, Geburtsdatum, Adresse, Name des Haustiers); auch nicht als Teil des Passworts.	OK	KO
12	Keine Wörter verwenden die auch in einem Wörterbuch vorkommen, auch nicht mehrfach hintereinander.	OK	KO
13	Keine direkten Referenzen oder Bezeichnungen für den jeweiligen Dienst im Passwort verwenden.	OK	KO
14	Falls das Passwort möglicherweise auch auf anderssprachigen Tastaturen eingegeben werden muss, sollte bei der Passwortauswahl auf darauf fehlende Umlaute und Sonderzeichen verzichtet werden. Es ist zu berücksichtigen, dass Sonderzeichen dabei eventuell auf andere Tasten kodiert sind.	OK	KO
15	Keine einem einheitlichen Muster folgenden Passwörter verwenden, durch die bei Kenntnis eines Passworts auf weitere Passwörter geschlossen werden kann.	OK	KO
II	PASSWORT-VERWENDUNG		
16	Passwort geheim halten und mit niemandem teilen.	OK	KO

Netzwerksicherheit - Angriffsvektoren



Netzwerksicherheit - Sicherheitrisiko

- **BYOD – Bring your own device**
- **Zertifizierungen**
  - Vertrauen von Zertifizierungsstellen
- **Authentisierung**
- **Schlüsselgenerierung**
- **Fernwartungsfunktionen**
- **Web Access (Outlook)**
- **Veraltete Betriebssysteme**
- **Alte Verschlüsselungen**

Präventiver Schutz – Netzwerk

- **Regelmäßige Updates**
- **Schulung der Mitarbeiter**
- **Verschlüsselung mobiler Endgeräte (Smartphones, Notebooks etc.)**
- **Zentralisierte Überwachung aller Clients (auch mobile Endgeräte)**
- **Zugang von Außen via VPN**
- **Security Scans (Ports Scan, Passwortkontrolle, Exploit Scans)**
- **Externer Penetration-Test**

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Präventiver Schutz – Netzwerk

- **Physikalische Sicherheit**
  - Zutritt
  - Brandschutz
  - Etc.
- **Datenverkehr überwachen**
- **Datenverkehr verschlüsseln**
- **Verwendung von physischen Firewalls**
- **Sichere Backup-Lösung (Configs)**
- **Information über aktuelle Bedrohungen**

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Präventiver Schutz – Netzwerk

- **Inventory Management**
- **Risikoabwägungen**
- **Incident Management**
- **Audits**
  - ISO 27001
  - weitere ISMS Systeme (siehe auch https://www.sicherheitshandbuch.gv.at/)

Zero Trust

- **Wer darf wann, wo, warum und wie auf Daten zugreifen?**
- **Grundsätzlich: Vertraue niemandem im Netzwerk, verifiziere immer**
  - Egal ob intern oder extern
  - Verändert die gesamte IT-Security-Architektur
  - Hoher Aufwand bei der Umsetzung
    - Monitoring aller (Daten)dienste, User, Geräte
    - Intrusion Detection Systems (IDS)
    - Firewalls
  - Authentifizierung aller Geräte, User, Dienste notwendig
    - Identitätsprinzip
- **Konzeptbeispiele**
  - BeyondCorp - Google
  - NIST Zero Trust Architecture - National Institute of Standards and Technology
  - NCSC Netzwerk Architektur – National Cyber Security Center - Großbritannien

Security as a Service – Security Lösungen aus der Cloud

- **Geeignet vor allem für Firmen ohne ausreichendes Personal bzw. mit zu geringen (auch finanziellen) Kapazitäten**
- **Managed Services aus der Cloud**
  - Monitoring von Systemen
  - Verwenden Künstliche Intelligenz zur Erkennung von Anomalien
  - Zeigen Schwachstellen im Netzwerk auf
  - Patchen Updates und offene Sicherheitslücken
- **Security Detection Services**
  - Beispiele: cipher, Datadog, intruder, uvm.
  - Breite Bandbreite an Anbietern und Services

Endpoint Security

- **IT-Sicherheit für Endgeräte**
  - PCs, Laptops, Handys
  - Tablets, POS-Systeme, Drucker, etc.
- **Einfluss durch**
  - BYOD - Bring your own Device
  - Home office
    - Kein Zero-Trust im Unternehmensnetzwerk
    - Corona hat übernacht 1000e Netze unsicher gemacht

Endpoint Security

- **Beinhaltet**
  - Zentrales Security Management
  - Netzwerk-Security
  - Machine Learning/Künstliche Intelligenz
  - Dynamic Thread Identification
  - Plattformübergreifend
  - Software/Hardware-Update Möglichkeiten
- Beispiele:
  - Checkpoint, Withsecure Protection,
  - Avast Business, Bitdefender, Kaspersky, Avira, ESET, etc.

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Endpoint Security –Mobile Device Management

- **Zentrale Management Platform**
  - Security features
  - Monitoring
  - Management von Berechtigungen
- **Sichere Authentication**
- **Sperr-Management**
- **Over-the-air Updates**
- **App-Berechtigungen**
- **Location-based Compliance**

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

IT- Security im Unternehmen

- **Chefsache**
  - Top-Down
  - Management
  - Jeder einzelne Mitarbeiter (steht und fällt IT Security)
- **Ressourcen**
  - Personell
  - Finanziell
- **Security Policies**
  - abgestimmt auf organisationelle Struktur

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES


DIH SÜD
FH Burgenland
Fragen?

Hacking – Tools

- nmap (Portscan)
- Kali linux
  - hydra (Passwort cracker)
- Wireshark (Sniffing)
- tcpdump (Sniffing)
- Airmon (WLAN)
- Netcat (HTTP)
- Sparta (Pentesting→ Hydra, nmap, nikto)
- OpenVAS (Scanner, Offene Ports und Software Überprüfung)
- Metasploit (Framework für Suche von Sicherheitslücken)
- Social Engineering Toolkit (SET)

Weitere nützliche Links

- https://haveibeenpwned.com/ Check Leaks von Passwörtern
- https://www.shodan.io/ Check von Offenen Ports und Schwachstellen
- https://getgophish.com/ Open Source Phishing Framework
- Notfallplan – Verhalten bei IT-Notfällen (Mitarbeiter)
- https://cloudsecurityalliance.org/ - Aktuelle Ereignisse im Bereich Cybersecurity
- https://www.elektronik-kompendium.de/ - Netzwerktechnik Grundlagen

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Quellen

- Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: a threat to cyber security. *CS Journals*, *7*(1).
- Lundberg, J. (2020). Dynamic Risk Management in Information Security: A socio-technical approach to mitigate cyber threats in the financial sector.
- Bedner, M., & Ackermann, T. (2010). Schutzziele der IT-sicherheit. *Datenschutz und Datensicherheit-DuD*, *34*(5), 323-328.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.
- Parkin, S., Fielder, A., & Ashby, A. (2016, October). Pragmatic security: modelling it security management responsibilities for SME archetypes. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (pp. 69-80).
- Abbas, J., Mahmood, H. K., & Hussain, F. (2015). Information security management for small and medium size enterprises. *Sci. Int*, *27*, 2393-2398.
- Park, J. Y., Robles, R. J., Hong, C. H., Yeo, S. S., & Kim, T. H. (2008). IT Security Strategies for SME's. *International journal of software engineering and its applications*, *2*(3), 91-98.
- https://www.sicherheitshandbuch.gv.at/
- OWASP

DIH SÜD

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

IT und Cybersicherheit

DIH- Süd
Forschung Burgenland
clemens.gnauer@fh-burgenland.at