ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

# IT-SICHERHEIT

Karl Machan, CRM
Graz, 25.09.2020

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- Neue Schlagwörter -> neue Risiken?
- Wie relevant sind diese Risiken für mein Unternehmen?
- „Für die Daten, die ich im Unternehmen verwende, interessiert sich eh kein „Hacker“!“
- „Für die Geschäftstätigkeit im Unternehmen spielt die IT keine wesentliche Rolle.“
- „Um die IT kümmert sich mein IT-Mann bzw. IT-Dienstleister. Der kümmert sich auch um die Sicherheit“

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

## Passwörter von österreichischen Politikern im Internet gelandet

**3,3 Millionen Österreicher - darunter sieben Minister - sind von einem Datenleck betroffen, bei dem E-Mail-Adressen und Passwörter gestohlen wurden.**

In dem gestohlenen Datensatz sollen sich knapp 7800 E-Mail-Adressen und dazugehörige Passwörter von Mitarbeitern der öffentlichen Hand befinden. – APA/ROLAND SCHLAGER

09.05.2019 um 07:17 2 Kommentare

Quelle: https://diepresse.com/home/techscience/5625105/Passwoerter-von-oesterreichischen-Politikern-im-Internet/

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO


## Hotel zum vierten Mal von Hackern lahmgelegt

Das Seehotel Jägerwirt auf der Turracher Höhe ist bereits zum vierten Mal von Hackern heimgesucht und erpresst worden. Die elektronischen Zimmerschlüssel wurden lahmgelegt. Daher will man jetzt zu normalen Schlüsseln zurückkehren.

Quelle: https://kaernten.orf.at/news/stories/2821290/

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

## Cyberattacken: 2 von 3 Unternehmen in Österreich betroffen

**53 Prozent der heimischen Unternehmen betrachten Cyber Security nicht als fixen Bestandteil von Digitalisierungsinitiativen und nur sieben Prozent glauben, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen treffen. Zu diesen Ergebnissen kommt die Studie „Cyber Security in Österreich" vom Beratungsunternehmen KPMG.**

**Zwei Drittel (66 Prozent) der österreichischen Unternehmen erlitten in den vergangenen zwölf Monaten einen Cyberangriff. (c) pixabay**

Zwei Drittel (66 Prozent) der österreichischen Unternehmen erlitten in den vergangenen zwölf Monaten einen Cyberangriff. Das sind fünf Prozent mehr als im Vergleich zum Vorjahr (61 Prozent). 2016 gab lediglich die Hälfte an, Opfer einer Cyberattacke gewesen zu sein (49 Prozent). Phishing und Malware sind und bleiben die häufigsten Angriffsarten aus der virtuellen Welt. Knapp die Hälfte der befragten Unternehmen (jeweils 47 Prozent) kam mit diesen Attacken in Berührung. Hier lässt sich ein eindeutiger Anstieg gegenüber dem Vorjahr erkennen: 2018 waren 24 Prozent der Unternehmen von Phishing und 22 Prozent von Malware betroffen.

Quelle: https://computerwelt.at/news/topmeldung/cyberattacken-2-von-3-unternehmen-in-oesterreich-betroffen/

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- Jeder kann Opfer eines Cyberangriffs werden!
- Die Größe eines Unternehmens ist nicht relevant, sondern die Art und Anzahl der Sicherheitsmängel in einem Unternehmen!
- Sobald IT-Infrastrukturen in einem Unternehmen verwendet werden, sind die damit verbundenen Risiken zu berücksichtigen!
- IT-Fachmann ≠ IT-Sicherheitsexperte

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Aktuelle Trends aus dem Bericht Cyber Sicherheit 2019 - Bundeskanzleramt:**

- DDoS - Distributed-Denial-of-Service (DDoS)
  - Bei einer DoS-Attacke wird ein IT-System absichtlich mit so vielen Anfragen belastet, bis das System zusammenbricht
- Ransomware
  - Hierbei handelt es sich um Schadprogramme, die Dateien auf der Festplatte und eventuell auch auf verbundenen USB- oder Netzwerk-Laufwerken verschlüsseln und wird danach aufgefordert für die Entschlüsselung der Daten einen entsprechenden Betrag zu zahlen.
- Phishing
  - Der Angreifer versucht über gefälschte E-Mails, Internetseiten, SMS usw. an persönliche Daten eines Nutzers heranzukommen (z.B. Nachbau der Online-Banking-Webseite)

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Aktuelle Trends aus dem Bericht Cyber Sicherheit 2019 - Bundeskanzleramt:**

- CEO-Fraud/Fake Invoice/SCAM:
  - Beim CEO-Fraud geben sich Täter beispielsweise als Geschäftsführer (CEO) des Unternehmens aus und veranlassen einen Unternehmensmitarbeiter zum Transfer eines größeren Geldbetrages ins Ausland.
  - Fake Invoice – Hier werden falsche Rechnungen an Unternehmen oder auch Privatpersonen versendet, in der Hoffnung, dass diese bezahlt werden
  - Scam-Mails enthalten Gewinnversprechen bzw. das Versprechen, schnell und mit einfachen Mitteln reich zu werden. Allerdings wird man zuvor aufgefordert, selbst einen bestimmten Geldbetrag zu überweisen.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Aktuelle Trends aus dem Bericht Cyber Sicherheit 2019 - Bundeskanzleramt:**

- Targeted Attack/Advanced Persistent Threat
  - ein technisch aufwendiger Angriff auf einzelne IT-Infrastrukturen und Netzwerke eines Unternehmens um Daten gezielt auszuspionieren (z.B. Industriespionage)
- Datendiebstahl
- Botnet/C2
  - Ein Bot (auch Zombie) ist ein an das Internet angeschlossener Computer, der durch ein Schadprogramm von Hackern kontrolliert und ferngesteuert wird. Bei einem Botnet handelt es sich um einen Verbund von mehreren ferngesteuerten Computern
- Defacements
  - Hierbei handelt es sich um das unberechtigte Verändern der Inhalte einer Website.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

## Wer sind die Angreifer?

- **White-Hat:** Das Hauptziel ist, die Verantwortlichen auf Sicherheitslücken im System aufmerksam zu machen.
- **Script Kiddies:** hacken zum Zwecke der Angeberei.
- **Grey-Hat:** kann sowohl zur Verbesserung der Systemsicherheit beitragen als auch schwerwiegende Schäden anrichten. Verstößt möglicherweise gegen Gesetze zur Erreichung eines höheren Ziels
- **Black-Hat:** hackt sich mit der Absicht Schaden anzurichten ein und hat kriminelle Absichten
- **Hacktivisten:** hackt sich für einen politischen oder sozialen Zweck ein, um auf eventuelle Machenschaften eines Unternehmens, Organisation oder Staat aufmerksam zu machen

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**WERTPAPIERAUFSICHTSGESETZ 2018:**

**Allgemeine organisatorische Anforderungen:**

- **§ 29. (4)** Ein Rechtsträger hat angemessene Vorkehrungen zu treffen, um die **Kontinuität** und **Regelmäßigkeit** der **Wertpapierdienstleistungen** und **Anlagetätigkeiten** zu **gewährleisten**. Zu diesem Zweck hat er geeignete und angemessene **Systeme**, **Ressourcen** und **Verfahren** einzurichten.
- **§ 29. (6)** …..hat ein Rechtsträger über solide **Sicherheitsmechanismen** zu verfügen, durch die die **Sicherheit** und **Authentifizierung** der **Informationsübermittlungswege** gewährleistet werden, das **Risiko** der **Datenverfälschung** und des **unberechtigten Zugriffs** minimiert und ein Durchsickern von Informationen verhindert wird, so dass die **Vertraulichkeit** der **Daten** jederzeit **gewährleistet** ist.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**GESETZLICHE VORGABEN FÜR WERTPAPIERUNTERNEHMEN:**

**DELEGIERTE VERORDNUNG (EU) 2017/565:**

- Art. 21 (2) Die Wertpapierfirmen richten Systeme und Verfahren ein, die die **Sicherheit**, die **Integrität** und die **Vertraulichkeit** der **Informationen gewährleisten**, …..
- Art. 21 (3) Die Wertpapierfirmen sorgen für die **Festlegung**, **Umsetzung** und **Aufrechterhaltung** einer angemessenen **Notfallplanung**, die bei einer **Störung** ihrer **Systeme** und **Verfahren** gewährleisten soll, dass wesentliche **Daten** und **Funktionen** erhalten bleiben und Wertpapierdienstleistungen und Anlagetätigkeiten fortgeführt werden ……
- Etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Unterteilung der IT-Risiken:**

- **IT-Sicherheitsrisiko**
- **Verfügbarkeits- und Kontinuitätsrisiko**
- **IT-Änderungsrisiko**
- **Datenintegritätsrisiko**
- **Outsourcingrisiko**

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **IT-Sicherheitsrisiko**
  - Das Risiko eines unbefugten Zugangs zu IT-Systemen und Datenzugriffs von innerhalb oder außerhalb (z. B. Cyber-Attacken).
  - Schutz vor Cyber- bzw. anderen IT-Attacken:
    - **Firewall**
    - **Netzwerksicherheit**
    - **Antivirus**
    - **Verschlüsselung**
    - **sichere Passwörter**

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **IT-Sicherheitsrisiko**
  - Schutz vor Cyber- bzw. anderen IT-Attacken:
    - **Benutzerberechtigungsvergaben (need-to-know-Prinzip)**
    - Umgang mit **Administrationsrechten**
    - **Awarness-Schulungen**
    - **Patchmanagement** (z.B. Microsoft Sicherheitsupdates, etc.)
    - Regelungen für den Einsatz **betriebsfremder Geräte**
    - Steuerung von **Softwareinstallationen** (z.B. nur genehmigte SW darf eingesetzt werden, Verbot der Selbstinstallation, etc.)
    - Etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Verfügbarkeits- und Kontinuitätsrisiko**
  - Das Risiko, dass IT-Systeme und -Daten nicht zur Verfügung stehen und die mangelnden Fähigkeit diese wieder rechtzeitig herzustellen
  - Verfügt das Unternehmen bei Ausfall von IT-Komponenten über eine adäquate **Notfallplanung**?
  - Entsprechende Dokumentation notwendig, in der folgendes definiert ist:
    - Mögliche Ausfallszenarien
    - Wer ist zu informieren (inkl. Kontaktdaten)
    - Wer welche Aufgaben zu erledigen hat, um den Normalbetrieb wiederherzustellen
    - Möglicher Work-around
    - Kontaktdaten IT-Dienstleister

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Verfügbarkeits- und Kontinuitätsrisiko**
  - **Backup/Restore** Konzept
    - Detaillierte Dokumentation, sodass im Fall eines Ausfalls des Systemadministrators ein anderer IT-Fachmann eine Wiederherstellung zeitnah und rasch durchführen kann
    - regelmäßige Tests inkl. Protokollierung
    - Kontrolle und Anpassung der Dokumentation bei jeder Änderung der IT-Infrastruktur

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Änderungsrisiko**
  - Das Risiko, das sich aus der mangelnden Fähigkeit ergibt, IT-Systemänderungen (Hardware als auch Softwareänderungen) zeitgerecht und kontrolliert zu steuern
  - Trennung von Entwicklungs-, Test-, und Produktivumgebung
  - Genaue und detaillierte Planung der IT-Systemänderungen
  - Planung zur Wiederherstellung des ursprünglichen Zustands bei missglückter Systemänderung
  - Berücksichtigung der IT-Sicherheit bei Einsatz neuer Software, Systeme, Geräte, etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Datenintegritätsrisiko**
  - Das Risiko, dass die von IT-Systemen gespeicherten und verarbeiteten Daten unvollständig, ungenau oder inkonsistent sind
  - beispielsweise aufgrund mangelhafter oder fehlender IT-Kontrollen der Daten
  - Mögliche Maßnahmen:
    - regelmäßige Kontrollen der korrekten Funktionsweise der eingesetzten Systeme
    - Einhaltung des 4-Augen-Prinzips
    - Regelmäßige Überprüfung durch interne Revision
    - Maßnahmen zur Verhinderung von unautorisierter Veränderung von Daten (Berechtigungen, Kontrolle von log-Files, etc.)
    - Etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Outsourcingrisiko**
  - Das Risiko, dass die Beauftragung eines Dritten mit der Bereitstellung von IT-Systemen oder der Erbringung damit zusammenhängender Dienstleistungen das Unternehmen nachteilig beeinflusst
  - Mögliche Maßnahmen:
    - Entsprechender Auslagerungsvertrag mit dem IT-Dienstleister z.B. Notfallplanung, Reaktionszeiten, Service Level Agreement, Zugriffsberechtigungen, etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Mögliche IT-Risiken:**

- **Outsourcingrisiko**
  - Mögliche Maßnahmen:
    - Notfallplanung bei Ausfall des Dienstleisters
    - Detaillierte und ausführliche Dokumentationen des IT-Systems im eigenen Unternehmen, sodass ein anderer Dienstleister die Betreuung ehestmöglich übernehmen kann
    - Einhaltung von Sicherheitsstandards durch Drittanbieter
    - Etc.
  - Bei Einsatz von **Cloudsystemen** sind ebenfalls sämtliche zuvor genannten **IT-Risiken** zu berücksichtigen
  - Etc.

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

**Weiterführende Informationen:**

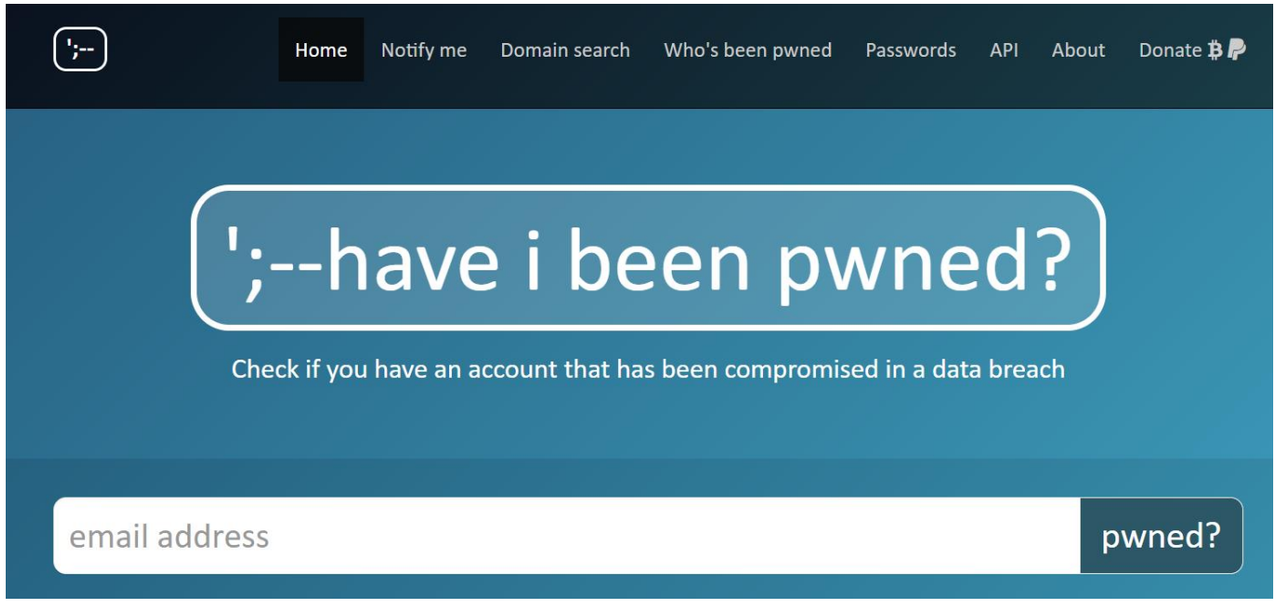
- **ISO-27000-Reihe** beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems in Unternehmen
- **BSI-Grundschutz:** ist eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die zur Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IT-Umgebungen dienen.
- **Control Objectives for Information and related Technology (COBIT):** ermöglicht die Steuerung und Kontrolle des IT-Betriebs durch das Management. COBIT entstand aus einer Sammlung von mehreren IT-Standards, Rahmenwerken, Richtlinien und Best Practices
- **IT Infrastructure Library (ITIL):** ist ein etablierter Qualitätsstandard, in dem sich vordefinierte Prozesse, Funktionen und Rollen für IT-Infrastrukturen von Unternehmen finden (Sammlung von Best Practices für Service Management).

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- **Weiterführende Informationen:**
  - **Leitfaden IT-Sicherheit** in WPF und WPDLU
    - Seit August 2018
    - Rechtsgrundlagen
    - Unterstützung zur Behandlung der IT-Risiken
  - **EBA-Guideline** - Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)

# CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- **Weiterführende Informationen:**
  - **https://haveibeenpwned.com/**
  - Datenbank, in der seit 2013 Informationen zu gehackten Konten und Passwörtern gesammelt wurden



FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz