ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

FMA-PRAXISDIALOG 2019

IT-SICHERHEIT FÜR WERTPAPIERUNTERNEHMEN

FMA-LEITFADEN

Karl Machan, CRM
Wien, 05.06.2019

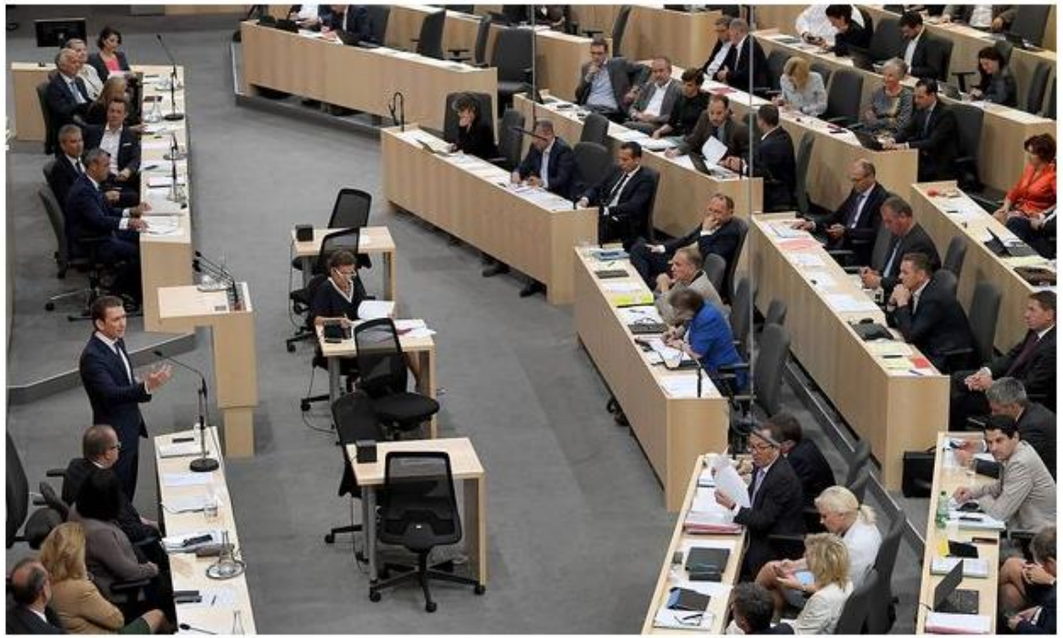
CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- 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.

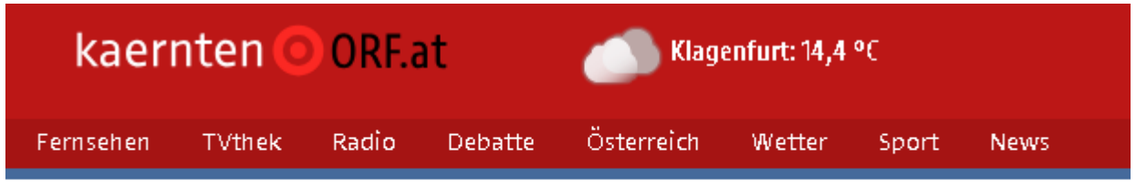


In dem gestohlenen Datensatz sollen sich knapp 7800 E-Mail-Adressen und dazugehörige Passwörter von Mitarbeitern der öffentlichen Hand befinden. – APA/ROLAND SCHLAGER

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

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

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

WERTPAPIERAUFSICHTSGESETZ 2018:

Auslagerungen:

- **§ 34.** Ein Rechtsträger hat sicherzustellen, dass beim Rückgriff auf Dritte (**Dienstleister**) zur Wahrnehmung **betrieblicher Aufgaben**, die für die **kontinuierliche** und **zufrieden stellende Erbringung von Dienstleistungen für Kunden** und **zur Ausübung von Anlagetätigkeiten** wesentlich sind, unter Beachtung der Art. 30 bis 32 der delegierten Verordnung (EU) 2017/565 **angemessene Vorkehrungen** getroffen werden, um unnötige zusätzliche **Geschäftsrisiken** zu vermeiden. ….
- **Siehe auch delegierte Verordnung (EU) 2017/565 Art. 30 (1) u. Art. 31 (2)**
- Etc.

CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

- **Leitfaden IT-Sicherheit** in WPF und WPDLU
  - Seit August 2018
  - Rechtsgrundlagen
  - Unterstützung zur Behandlung der IT-Risiken

CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

Mögliche IT-Risiken in Wertpapierunternehmen:

- **Verfügbarkeits- und Kontinuitätsrisiko**
  - Verfügt das Unternehmen bei Ausfall von IT-Komponenten über eine adäquate **Notfallplanung**?
  - **Backup/Restore** Konzept (Dokumentation, regelmäßige Tests, etc.)
  - Etc.

- **IT-Sicherheitsrisiko**
  - Schutz vor Cyber- bzw. anderen IT-Attacken (**Firewall**, **Netzwerksicherheit**, **Notebooks**, **Remote-Zugang**, **Verschlüsselung** etc.)
  - **Benutzerberechtigungsvergaben**, **Passwortrichtlinien**, etc.
  - Umgang mit **Administrationsrechten**

CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

IT-Risiken in Wertpapierunternehmen :

- **Änderungsrisiko**
  - Unterliegen die eingesetzten Systeme einem entsprechenden Sicherheitspatchmanagement (Zuständigkeit, Regelmäßigkeit, Kontrollen, etc.)
  - Berücksichtigung der IT-Sicherheit bei Einsatz neuer Software, Systeme, Geräte, etc.
- **Datenintegritätsrisiko**
  - Welche Maßnahmen wurden gesetzt, dass die in den verwendeten Daten, korrekt sind (z.B. regelmäßige Kontrollen, etc.)?
  - Welche Maßnahmen verhindern die unautorisierte Veränderung von Daten (z.B. Überprüfung von Logfiles, etc.)?
  - Etc.

CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

IT-Risiken in Wertpapierunternehmen :

- **Outsourcingrisiko**
  - Berücksichtigung des IT-Risikos im Auslagerungsvertrag (z.B. Notfallplanung, Reaktionszeiten, Service Level Agreement, Zugriffsberechtigungen, etc.)
  - Notfallplanung bei Ausfall des Dienstleisters (z.B. ausreichende Dokumentationen über IT-System im eigenen Unternehmen, sodass ein anderer Dienstleister die Betreuung ehestmöglich übernehmen kann)
  - Einhaltung von Sicherheitsstandards durch Drittanbieter
  - Bei Einsatz von **Cloudsystemen** sind sämtliche zuvor genannten **IT-Risiken** zu berücksichtigen
  - Etc.

CYBERRISIKO, IT-RISIKO, IT-SICHERHEITSRISIKO

Standards :

- **Österreichisches Informationssicherheitshandbuch** beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheits-managementsystems in Unternehmen und der öffentlichen Verwaltung.
- **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).

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz