ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

AKTUELLES ZUR IT-SECURITY

Karl Machan, CRM
Graz, 30.09.2022

INHALTSVERZEICHNIS

Entwicklung Cyberkriminalität

FMA

Cyberrisiko, IT-Risiko, IT-Sicherheitsrisiko

- 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“

Entwicklung Cyberkriminalität

CHRONIK

Hackerangriff auf Therme Waltersdorf

In der Steiermark haben erneut Computerhacker zugeschlagen. Nachdem vergangene Woche die Stadt Feldbach Ziel einer Attacke geworden war, wurde nun die Therme Bad Waltersdorf zum Opfer.

13. September 2022, 12.36 Uhr (Update: 13. September 2022, 19.39 Uhr)

Teilen

Wie in Feldbach - mehr dazu in **Hackerangriff legt Feldbacher EDV lahm** (6.9.2022) - schlugen die Hacker auch in der Therme Bad Waltersdorf an einem Wochenende zu: Seit vergangenem Sonntag geht nichts mehr, die eigenen Mitarbeiter sind aus dem System ausgesperrt.

Quelle: https://steiermark.orf.at/stories/3173396/

Entwicklung Cyberkriminalität

APA OTS

KPMG

KPMG Studie: 3 von 4 Unternehmen in Österreich von Cyberattacken betroffen

72 Prozent aller Unternehmen in Österreich waren in den letzten 12 Monaten Opfer einer Cyberattacke.

Wien (OTS)- Cyberkriminalität ist in Österreich am Vormarsch: Die Anzahl der betroffenen Unternehmen ist im Vergleich zum Vorjahr stark angestiegen – von 49 Prozent auf 72 Prozent. Jedes zweite Unternehmen litt als Folge unter einer Unterbrechung der Geschäftsprozesse. Große Verschwiegenheit prägt dabei das Bild: Nur rund ein Drittel (31 Prozent) aller Cyberangriffe werden gemeldet. Zu diesem Ergebnis kommt die aktuelle KPMG Studie „Cyber Security in Österreich", an der knapp 240 Cybersicherheitsexperten österreichischer Unternehmen teilnahmen. Die KPMG Studie präsentiert und analysiert bereits zum zweiten Mal in Folge die wichtigsten Fakten und Trends zum Thema in Österreich.

Quelle: https://www.ots.at/presseaussendung/OTS_20170913_OTS0070/kpmg-studie-3-von-4-unternehmen-in-oesterreich-von-cyberattacken-betroffen-video

Entwicklung Cyberkriminalität

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

DIE ZAHLEN IM DETAIL:

Bei den Delikten wird unterschieden zwischen:

- Cybercrime im engeren Sinne
- Cybercrime im weiteren Sinne

Cybercrime im engeren Sinne (IKT als Angriffsziel):

Diese umfassen kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) begangen werden.

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Cybercrime im engeren Sinne:

Delikt	Beschreibung	Anzahl 2021
§ 107c StGB	Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems	395
§ 118a StGB	Widerrechtlicher Zugriff auf ein Computersystem	952
§ 119 StGB	Verletzung des Telekommunikationsgeheimnisses	14
§ 119a StGB	Missbräuchliches Abfangen von Daten	58
§ 126a StGB	Datenbeschädigung	354
§ 126b StGB	Störung der Funktionsfähigkeit eines Computersystems	95
§ 126c StGB	Missbrauch von Computerprogrammen oder Zugangsdaten	540
§ 148a StGB	Betrügerischer Datenverarbeitungsmissbrauch	12 701
§ 225a StGB	Datenfälschung	375

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Cybercrime im weiteren Sinne (IKT als Tatmittel):

Hierbei handelt es sich um Straftaten, bei denen die Informations- und Kommunikationstechnik als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird.

Beispiele:

- Betrugsdelikte
- Drogenhandel im Darknet
- Online-Kindesmissbrauch
- Cybergrooming (gezielte Manipulation Minderjähriger)
- Cybermobbing

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Cybercrime im weiteren Sinne (IKT als Tatmittel):

- Die Anzahl der Delikte betrug hierbei im Jahr 2021 bei 30.695, wobei der größte Anteil mit 22.440 bei Internetbetrugsfällen lag.

Ergänzung:

- Die Zahlen des Lageberichts Cybercrime sind mit Vorsicht zu genießen, da die Dunkelziffern in diesem Bereich als besonders hoch eingeschätzt werden. Viele Betroffene scheuen eine Anzeige, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könnte.
- Prinzipiell ist natürlich anzuführen, dass die alarmierende Entwicklung im Bereich Cybercrime auch teilweise aufgrund der anhaltenden Covid-19-Pandemie zurückzuführen sind.

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Aktuelle Trends im Bereich Cyberkriminalität:

- Fraud Calls und Call-Bots: Hierbei bedienen sich die Täter bestimmter Computerprogramme um potenzielle Opfer anzurufen. Die Nummer auf dem Display wird mit technischen Mitteln, dem sogen. „Call-ID-Spoofing“ verfälscht. Die Opfer werden aufgefordert Tastenkombinationen zu drücken, damit werden mögliche englischsprachige Opfer bereits vorselektiert. Danach melden sich beispielsweise Täter, die sich als (Interpol-) Polizistinnen oder -Polizisten oder Parlamentsangehörige ausgeben.
- 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

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Aktuelle Trends im Bereich Cyberkriminalität:

FluBot:

- Technisch hoch entwickelte Schadenssoftware auf Smartphones mit Android-Betriebssystem. Diese konzentrieren sich auf Banking-Apps bzw. Mobile Wallets (Kryptowährungen) um Zugangsdaten auszuspähen.
- Verbreitung über SMS
  - bspw. vermeintliche Paketsendung, die erst durch ein vorgetäuschtes Update des Betriebssystems beziehungsweise die Installation des Flashplayers anzusehen sind.
  - SMS mit Inhalten zu Videos, die erst durch ein vorgetäuschtes Update des Betriebssystems beziehungsweise die Installation des Flashplayers anzusehen sind.
- Overlay-Angriff: eine nicht erkennbare Applikationsschicht legt sich über eine originale Anwendung (Phishing-Seite, die der Banking-App zum Verwechseln ähnlich sieht)
- Keylogger: sämtliche Eingaben (z.B. Zugangsdaten) werden abgefangen und an einen Server übermittelt.

Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

Aktuelle Trends im Bereich Cyberkriminalität:

FluBot:

- FluBot richtet sich selbst als Standard-SMS-Anwendung ein und kann unbemerkt SMS senden und empfangen
- durch die Bank versendete TAN SMS werden abgefangen und an einen Server übermittelt
- Während der Installation müssen durch den Benutzer diverse Berechtigungen bzw. Zugriffsrechte vergeben werden
- Zugriff auf Kontaktliste
- Infiziertes Smartphone fungiert auch als direkter Verteiler der Links zur Schadsoftware

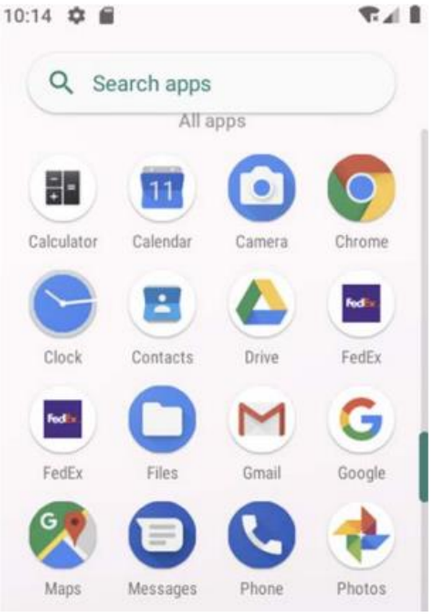
Quelle: Bundeskriminalamt Cybercrime Report 2021

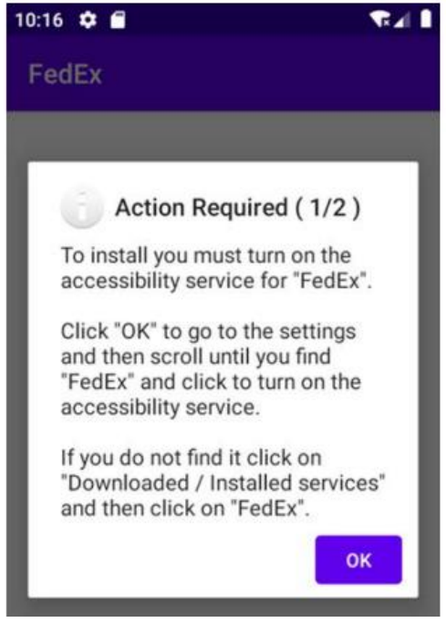
Entwicklung Cyberkriminalität

<u>Aktuelle Trends im Bereich Cyberkriminalität:</u>

<u>FluBot:</u>

Beispiel FedEX:





Quelle: Bundeskriminalamt Cybercrime Report 2021

Entwicklung Cyberkriminalität

FMA

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**

Entwicklung Cyberkriminalität

Cyberrisiko, IT-Risiko, IT-Sicherheitsrisiko

- Das größte **IT-Risiko** findet sich **zwischen Tastatur und Stuhl**
- **Awareness:** Sorgen Sie in Ihrem Unternehmen für sich und für Ihre Mitarbeiter für ein **IT-Sicherheits-Bewusstsein**!
- Eines der größten Risiken in Ihrem Unternehmen ist das **Reputationsrisiko**! Die wichtigste Basis für Ihre **Geschäftstätigkeit** ist das **Vertrauen der Kunden!** Sollten heikle **Kundendaten gehackt** werden, kann dies Ihr **Unternehmen ruinieren!**

Entwicklung Cyberkriminalität

Bespiel Awareness:

Das beliebteste Passwort Österreichs ist...

...auch im Jahr 2021 „123456“.

Es ist der Albtraum aller Sicherheitsexperten: das aktuelle Ranking der beliebtesten Passwörter. Der Anbieter eines Passwortmanagers hat die aktuelle Aufstellung veröffentlicht. An der Spitze - weltweit wie auch in Österreich - steht die einfache Zahlenkombination „123456“. Auf dem zweiten Platz folgt „123456789“. Platz 3 geht an „12345“.

Zum kompletten Ranking

Die Topplatzierungen unterscheiden sich in den verschiedenen Ländern kaum. In Indien gehört der Platz an der Spitze des Rankings dem einfachen „password“. Je weiter man sich im Ranking von den Top 10 entfernt, umso häufiger finden sich landesspezifische Begriff und vor allem Namen in der Liste.

„Ö3-Wecker“ mit Robert Kratky, 18. November 2021 (WJLED)

Entwicklung Cyberkriminalität

AUSZUG AUS DEN BELIEBTESTEN PASSWÖRTER IN ÖSTERREICH (TOP 200):

- qwerty
- Passwort
- Flocke123
- Beliebtester Vorname: daniel (gefolgt von michael)
- Beliebteste Stadt: salzburg
- Süßes darf nicht fehlen: puderzucker
- Beliebtestes Auto: mercedes
- Heimatverbundenheit: austria
- Nicht jugendfrei: ***** (finden sich auch in den Top 150)

Quelle: https://nordpass.com/de/most-common-passwords-list/

Entwicklung Cyberkriminalität

AUSZUG AUS DEN BELIEBTESTEN PASSWÖRTER WELTWEIT:

- Autos: Ferrari, Porsche
- Männer verwenden häufiger Schimpfwörter als Passwörter als Frauen
- Auch der Delfin ist sehr beliebt
- Beliebteste Team: Liverpool
- Metallica (88.543 mal verwendet)

Quelle: https://nordpass.com/de/most-common-passwords-list/

Digital Operational Resilience Act (DORA)

ZIEL:

- Schaffung eines einheitlichen Rechtsrahmens für die digitale operationelle Widerstandsfähigkeit von Finanzdienstleistungen
- Teil des Pakets zur Digitalisierung des Finanzsektors, eines Maßnahmenpakets, das darauf abzielt, das Innovations- und Wettbewerbspotenzial des digitalen Finanzwesens weiter zu erschließen und zu fördern und gleichzeitig mögliche Risiken zu mindern.

INKRAFTTRETEN:

- 2022/2023
- Übergangsfristen: 2 Jahre nach Inkrafttreten

Digital Operational Resilience Act (DORA)

VON DORA UMFASSTE UNTERNEHMEN:

- Kreditinstitute
- Zahlungsinstitute
- Kontoinformationsdienstleister
- E-Geld-Institute
- **Wertpapierfirmen**
- Anbieter von Krypto-Dienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Token und Emittenten signifikanter an Vermögenswerten geknüpfter Token
- Zentraverwahrer
- zentrale Gegenparteien
- Handelsplätze
- Transaktionsregister
- Verwalter alternativen Investmentfonds
- Verwaltungsgesellschaften
- Datenbereitstelungsdienstleister
- Versicherungs- und Rückversicherungsunternehmen
- Versicherungsvermittler und Rückversicherungsvermittler
- Einrichtungen zur betrieblichen Altersversorgung
- Ratingagenturen
- Administratoren von kritischen Benchmarks
- **Crowdfunding-Dienstleister**
- Verbriefungsregister
- IKT-Dienstleister

Digital Operational Resilience Act (DORA)

INHALT:

Wesentliche Kapitel:

- **IKT-RISIKOMANAGEMENT**
- **IKT-BEZOGENE VORFÄLLE - BEWÄLTIGUNG, KLASSIFIZIERUNG UND BERICHTERSTATTUNG**
- **PRÜFUNG DER DIGITALEN BETRIEBSSTABILITÄT**
- **STEUERUNG DES RISIKOS DURCH IKT-DRITTANBIETER**

Digital Operational Resilience Act (DORA)

IT-Risikomanagement (Art. 5 bis 16):

Erleichterungen für den größten Teil der österreichischen Wertpapierunternehmen -

Art. 16 – Vereinfachter IKT-Risikomanagementrahmen:

- Einrichtung eines **soliden** und **dokumentierten IKT-Risikomanagementrahmen** für ein schnelles, effizientes und umfassendes **Management aller IKT-Risiken** (inkl **Schutz der relevanten physischen Komponenten und Infrastrukturen**)
- Die **Sicherheit** und das **Funktionieren aller IKT-Systeme** sind kontinuierlich zu **überwachen**
- **Einsatz solider, widerstandsfähiger und aktueller IKT Systeme, Protokolle und Instrumente**, die geeignet sind, die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** zu gewährleisten

Digital Operational Resilience Act (DORA)

IT-Risikomanagement (Art. 5 bis 16):

Erleichterungen für den größten Teil der österreichischen Wertpapierunternehmen -

Art. 16 – Vereinfachter IKT-Risikomanagementrahmen:

- **Vorsorge treffen,** um **IKT-Risikoquellen** und **Anomalien** im **Netz** und in den **Informationssystemen unverzüglich zu identifizieren** und **aufzudecken**, sodass **IKT-bezogene Vorfälle** rasch behandelt werden können
- Ermittlung der wichtigsten **Abhängigkeiten** von **IKT-Drittanbietern**
- Gewährleistung der Kontinuität **kritischer** und **wichtiger Funktionen** durch **Geschäftskontinuitätspläne** und **Reaktions-** und **Wiederherstellungsmaßnahmen**, die zumindest **Back-up-** und **Wiederherstellungsmaßnahmen** umfassen
- **Regelmäßiges Testen** der genannten **Pläne** und **Maßnahmen**

Digital Operational Resilience Act (DORA)

IT-Risikomanagement (Art. 5 bis 16):

Erleichterungen für den größten Teil der österreichischen Wertpapierunternehmen -

Art. 16 – Vereinfachter IKT-Risikomanagementrahmen:

- **Regelmäßige Überprüfung** (sowie beim Auftreten größerer **IKT-bezogener Vorfälle**) des **Risikomanagementrahmen**. **Ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens ist der zuständigen Behörde auf deren Verlangen vorzulegen.**
- **Vorsorge treffen,** um **IKT-Risikoquellen** und **Anomalien** im **Netz** und in den **Informationssystemen unverzüglich zu identifizieren** und **aufzudecken**, sodass **IKT-bezogene Vorfälle** rasch behandelt werden können
- Ermittlung der wichtigsten **Abhängigkeiten** von **IKT-Drittanbietern**

Meldung schwerwiegender IT-bezogener Vorfälle (Art. 17 bis Art. 23)

- Einrichtung eines **Verfahren** für das **Management** von **IKT-Vorfällen**, um **IKT-Vorfälle** zu **erkennen**, zu **verwalten** und zu **melden** können.
- Zuweisung von **Rollen** und **Verantwortlichkeiten** im Falle von IT-bezogenen Vorfällen
- Für das Management von IKT-Vorfällen ist folgendes vorzusehen:
  - **Verfahren** zur **Ermittlung**, **Verfolgung**, **Protokollierung**, **Kategorisierung** und **Klassifizierung** von **IKT-bezogenen Vorfälle**
  - Zuweisung von **Rollen** und **Verantwortlichkeiten** definier, die im Falle von IT-bezogenen Vorfällen aktiviert werden müssen
- **Einrichtung** von **Verfahren** zur **Reaktion auf Vorfälle**, um die **Auswirkungen** zu **mindern** und **sicherzustellen**, dass die **IT-Dienste** rechtzeitig **betriebsbereit** und **sicher** sind.

Meldung schwerwiegender IT-bezogener Vorfälle (Art. 17 bis Art. 23)

- **Einstufung** von **IKT-bezogenen Vorfällen** und **Cyber-Bedrohungen** nach folgenden Kriterien ua:
  - **Anzahl** der betroffenen **Kunden** (ggf. Betrag od. Anzahl der betroffenen Transaktionen)
  - **Auswirkung auf Reputation**
  - **Dauer** der **IKT-bedingten Störung** (**Ausfallzeit der Dienste**)
  - durch die **IKT-bedingte Störung** verursachten **Datenverluste**, wie z. B. Verlust der Vertraulichkeit, Integrität oder Verfügbarkeitsverlust

Meldung schwerwiegender IT-bezogener Vorfälle (Art. 17 bis Art. 23)

- Wenn ein **schwerwiegender IT-Vorfall Auswirkungen** auf **die finanziellen Interessen** von **Kunden** hat, **müssen** diese **unverzüglich** über den schwerwiegenden IT-bezogenen Vorfall **informiert werden**

- **Meldung** von **schwerwiegenden Vorfällen** in Form eines Berichts an die **FMA**:
  - **Erstmeldung**
  - **Zwischenbericht**, sobald sich der **Status** des **ursprünglichen Vorfalls** oder der **Umgang** mit dem **schwerwiegenden IKT-Vorfall** geändert hat
  - **Abschlussbericht**

Digital Operational Resilience Act (DORA)

Prüfung der digitalen Betriebsstabilität (Digital Operational Resilience Testing; Art. 24 bis Art. 27)

- Unternehmen haben ein **solides** und **umfassendes Programm** zur **Überprüfung** der **digitalen operationellen Belastbarkeit** einzurichten, um IT-bezogene Vorfälle zu bewerten, Schwachstellen, Mängel oder Lücken in der Ausfallsicherheit des digitalen Betriebs festzustellen zu können
- Programm zur **Prüfung der digitalen Betriebsstabilität** als Bestandteil des **IT-Risikomanagements**
- Tests durch **unabhängige Parteien** (intern/extern)
- Verfahren zur **Priorisierung**, **Klassifizierung** und **Behebung** von erkannten Problemen
- Programm zur Prüfung der Ausfallsicherheit umfasst **Schwachstellenbewertungen** und **-scans**, **Open Source-Analysen**, **Prüfung der Netzwerksicherheit**, **Penetrationstests**, **Quellcode-Überprüfungen**, etc.

Digital Operational Resilience Act (DORA)

Steuerung des Risikos durch IKT-Drittanbieter (Art. 28 bis Art. 44)

- **Drittanbieter-Risiko** (Outsourcing-Risiko) ist integraler **Bestandteil** des **IKT-Risikomanagements**
- **Wertpapierfirmen**, die vertragliche **Vereinbarungen** mit **IKT-Drittanbieter** getroffen haben, bleiben **jederzeit voll verantwortlich** für die **Einhaltung** und für die **Erfüllung** aller **Verpflichtungen** aus den geltenden **Rechtsvorschriften**
- **Festlegung** und **Überprüfung** einer **Strategie** für **IKT-Drittrisiken**
- Umfasst eine **Strategie** für die Nutzung von **IKT-Diensten** für **kritische** oder **wichtige Funktionen**
- **Register** aller vertraglichen Vereinbarungen zu **IT-Diensten von Drittanbietern**
- **Mindestens einmal jährlich Meldung an FMA** über die **Zahl** der **neuen Vereinbarungen** mit **IKT-Drittanbietern**
- **Rechtzeitige Meldung** von **geplanten vertraglichen Vereinbarungen** für **kritische** oder **wichtige Funktionen** mit Drittanbieter an die **Aufsicht**

Steuerung des Risikos durch IKT-Drittanbieter (Art. 28 bis Art. 44)

- Vor einer **vertraglichen Vereinbarung müssen** Wertpapierfirmen folgendes **berücksichtigen:**
  - **Prüfung**, ob es sich um eine **IKT-Dienstleistung** in **Bezug** auf eine **kritische** oder **wichtige Funktion** handelt
  - **Prüfung**, ob die **aufsichtsrechtlichen Bedingungen** erfüllt sind
  - **Ermittlung** und **Bewertung aller relevanten Risiken**
  - **Due Diligence-Prüfungen** für potenzielle IT-Drittanbieter durchführen, um die **Geeignetheit** des IT-Drittanbieter sicherzustellen
  - Wertpapierfirmen dürfen nur vertragliche Vereinbarungen mit IKT-Drittdienstleistern eingehen, die angemessene **Informationssicherheitsstandards** einhalten

Steuerung des Risikos durch IKT-Drittanbieter (Art. 28 bis Art. 44)

- Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IT-Drittanbietern und Finanzunternehmen
  - Vereinbarung bei **kritischen** oder **wichtigen Funktionen**, dass die **aktuellsten** und **höchsten Informationssicherheitsstandards angewendet** werden
  - Zugangs-, Prüf- und Einschaurechte
  - Regelungen zur Vertragsbeendigung, Ausstiegsszenarien
  - Etc.

- Unternehmen stellen sicher bei Beendigung der vertraglichen Vereinbarung:
  - Keine Unterbrechung ihrer Geschäftstätigkeit
  - Einhaltung der aufsichtsrechtlichen Anforderungen
  - Keine Beeinträchtigung der Kontinuität und Qualität der Dienstleistungen für die Kunden

Steuerung des Risikos durch IKT-Drittanbieter (Art. 28 bis Art. 44)

- **Wesentliche Vertragsbestimmungen**:
  - Klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen
  - Ob eine Untervergabe erfolgen darf
  - Standorte
  - Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit, Vertraulichkeit und Schutz von Daten
  - Bestimmungen über die Gewährleistung des Zugangs, der Wiederherstellung und der Rückgabe in einem leicht zugänglichen Format von personenbezogener und nicht personenbezogener Daten
  - Leistungsbeschreibungen
  - Kündigungsrechte und entsprechende Mindestkündigungsfristen für die Beendigung des Vertrags

Steuerung des Risikos durch IKT-Drittanbieter (Art. 28 bis Art. 44)

- **Wesentliche Vertragsbestimmungen bei kritischen oder wichtigen Funktionen** :
  - Mitteilungsfristen und Berichtspflichten des IKT-Drittdienstleisters
  - Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen
  - die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und -Audits durch die zuständigen Behörden

Exkurs: Mögliche IT-Risiken in Wertpapierunternehmen:

- **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**
    - **Benutzerberechtigungs-vergaben (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.

Exkurs: Mögliche IT-Risiken in Wertpapierunternehmen:

- **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

Exkurs: Mögliche IT-Risiken in Wertpapierunternehmen:

- **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

Exkurs: IT-Risiken in Wertpapierunternehmen :

- **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.

Exkurs: IT-Risiken in Wertpapierunternehmen :

- **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.

Exkurs: IT-Risiken in Wertpapierunternehmen :

- **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.
    - 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

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz