IOS
INSTITUT ÖSTERREICHISCHER
STEUERBERATER

Informationsveranstaltung
Donnerstag, 23.02.2017

„Cybercrime und Datenschutz – Haftungsfallen für Wirtschaftstreuhänder“

Referent:
RA Mag. Martin Führer, LL.M.

Cybercrime und Datenschutz

Haftungsfallen für Wirtschaftstreuhänder

Informationsveranstaltung
Akademie der Wirtschaftstreuhänder, 23.02.2017

Mag. Martin Führer, LL.M.
Rechtsanwalt
Lektor FH St. Pölten
Zertifizierter Datenschutzbeauftragter

to do …

- **Teil I – Gefährdungspotenziale**
- **Teil II – Maßnahmen für Datenschutz und Datensicherheit**
- **Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung**

to do …

- **Teil I – Gefährdungspotenziale**
  - **CyberCrime / IT-Strafrecht**
  - **Zivilrechtliche Haftungsfallen**
  - **Verwaltungsrecht**
- Teil II – Maßnahmen für Datenschutz und Datensicherheit
- Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung

IT-Strafrecht

- **CyberCrime / IT-Strafrecht**
- Keine einheitliche Definition von Computer- und Internetstrafrecht bzw. Cyber Crime.

- Europäische Cybercrime-Convention
  - Umgesetzt seit dem Strafrechtsänderungsgesetz
  - Mehrere neue Straftatbestände

IT-Strafrecht

u|l|s|r

| Zahlen und Fakten

- | Keine neue Erkenntnis: Rasanter Anstieg der Anzeigen

	2005	2014	2015	Prozent (zu 2014)
CyberCrime-Anzeigen	1.800	9.000	10.010	+ 11,6 %
Aufklärungsrate		*40,8%*	*41,5%*	*+ 0,7*
Hacking		677	387	- 42,8 %
Betrügerischer Datenmissbrauch		404	647	**+ 60,1 %**
Ransomware (nur 126a berücksichtigt)		140	144	**+ 2,9%**
Störung Funktionsfähigkeit (DDoS)		140	164	**+ 17,8%**

Quelle: Cybercrime Österreich Jahresbericht 2015, Bundeskriminalamt

IT-Strafrecht

u|l|s|r

| Zahlen und Fakten

- | Art der Schäden
  - | Reputationsverluste
  - | Betriebsunterbrechungen
  - | Verlust von Kundendaten
- | Durchschnittlicher Schaden: EUR 400.000,00 / Unternehmen

IT-Strafrecht

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**

- IT-Dienstleister und Buchungssoftware
- Ausspionieren von Kundendaten
- Erpressung mittels Ransomware
- Blockieren von Bestelladresse und Server
- Fake president fraud

IT-Strafrecht

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- IT-Dienstleister und Buchungssoftware
  - Achtung bei der Auswahl des IT-Dienstleistungsunternehmens
  - Manipulation der Buchungssoftware
  - Abzweigen eines geringen Betrages auf eigenes Konto

  - → **§ 148a StGB** (Betrügerischer Datenverarbeitungsmissbrauch)
    - „Betrug an der Maschine"
    - bis zu sechs Monaten (360 TS); gewerbsmäßig oder > 5.000: 3 Jahre; > 300.000: 1 bis 10 Jahre
    - Phishing-Paragraph

IT-Strafrecht

u|l|s|r

| **Zahlen und Fakten**

  | Keine neue Erkenntnis: Rasanter Anstieg der Anzeigen

	2005	2014	2015	Prozent (zu 2014)
CyberCrime-Anzeigen	1.800	9.000	10.010	+ 11,6 %
Aufklärungsrate		*40,8%*	*41,5%*	*+ 0,7*
Hacking		677	387	- 42,8 %
Betrügerischer Datenmissbrauch		404	647	**+ 60,1 %**
Ransomware (nur 126a berücksichtigt)		140	144	**+ 2,9%**
Störung Funktionsfähigkeit (DDoS)		140	164	**+ 17,8%**

Quelle: Cybercrime Österreich Jahresbericht 2015, Bundeskriminalamt

IT-Strafrecht

u|l|s|r

| **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**

| IT-Dienstleister und Buchungssoftware
| Ausspionieren von Kundendaten
| Erpressung mittels Ransomware
| Blockieren von Bestelladresse und Server
| Fake president fraud

IT-Strafrecht

u|l|s|r

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- Ausspionieren von Kundendaten
  - Auftrag, bestimmte Kundendaten vom Konkurrenzunternehmen auszuspähen
  - Wirtschaftsspionage stark angestiegen
  - → § 118a StGB **(Widerrechtlicher Zugriff auf ein Computersystem)**
  - „Hacking"
    - früher nicht strafbar; Vorbereitungsdelikt
  - Heute:
    - Wenn Sicherheitsvorkehrungen zwecks Datenspionage oder Datenverwendung und eigener Vorteil bzw. Nachteil für einen anderen
    - tatsächlicher Schaden nicht notwendig; beabsichtigte Schadenszufugung reicht
    - → bis 6 Monate (360 TS); Ermächtigungsdelikt

IT-Strafrecht

u|l|s|r

- **Zahlen und Fakten**
  - Keine neue Erkenntnis: Rasanter Anstieg der Anzeigen

	2005	2014	2015	Prozent (zu 2014)
CyberCrime-Anzeigen	1.800	9.000	10.010	+ 11,6 %
Aufklärungsrate		*40,8%*	*41,5%*	*+ 0,7*
Hacking		677	387	- 42,8 %
Betrügerischer Datenmissbrauch		404	647	**+ 60,1 %**
Ransomware (nur 126a berücksichtigt)		140	144	**+ 2,9%**
Störung Funktionsfähigkeit (DDoS)		140	164	**+ 17,8%**

Quelle: Cybercrime Österreich Jahresbericht 2015, Bundeskriminalamt

IT-Strafrecht

u|l|s|r

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**

- IT-Dienstleister und Buchungssoftware
- Ausspionieren von Kundendaten
- Erpressung mittels Ransomware
- Blockieren von Bestelladresse und Server
- Fake president fraud

IT-Strafrecht

u|l|s|r

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- Erpressung mittels Ransomware *(von engl. Ransom = „Lösegeld")*
  - Eingang der Schadsoftware durch E-Mail-Anhänge
  - Dateien (Kundendaten und Zugangsdate) verschlüsselt
  - Geforderte Lösegeldzahlung von EUR 1.200,00 in Bitcoins
  - Gezahlt → Schlüssel erhalten
    - früher auch noch zurückgehalten; mangels Akzeptanz nun „Zusammenarbeit" mit den Erpressern
  - → **§ § 126a** (Datenbeschädigung)
  - Alle Handlungen, die die Daten unbrauchbar machen (löschen, unterdrücken, etc.)
    - bis 6 Monate (360 TS);
    - mehrere Computersysteme unter Verwendung eines Computerprogrammes: 3 Jahre
    - > EUR 300.000: 6 Monate – 5 Jahre

IT-Strafrecht

u|l|s|r

| **Zahlen und Fakten**

  | Keine neue Erkenntnis: Rasanter Anstieg der Anzeigen

	2005	2014	2015	Prozent (zu 2014)
CyberCrime-Anzeigen	1.800	9.000	10.010	+ 11,6 %
Aufklärungsrate		*40,8%*	*41,5%*	*+ 0,7*
Hacking		677	387	- 42,8 %
Betrügerischer Datenmissbrauch		404	647	**+ 60,1 %**
Ransomware (nur 126a berücksichtigt)		140	144	**+ 2,9%**
Störung Funktionsfähigkeit (DDoS)		140	164	**+ 17,8%**

Quelle: Cybercrime Österreich Jahresbericht 2015, Bundeskriminalamt

IT-Strafrecht

u|l|s|r

| **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**

| IT-Dienstleister und Buchungssoftware
| Ausspionieren von Kundendaten
| Erpressung mittels Ransomware
| Blockieren von Bestelladresse und Server
| Fake president fraud

IT-Strafrecht

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- Blockieren von Bestelladresse und Server
  - Spammails an die Bestell-Mailadresse
  - Keine Bestellungen annehmbar
  - Denkbar auch: Kontakt-Adresse bei Dienstleistern (→ ggfalls Kundenverlust)
  - → **§ 126a** (Datenschädigung)

IT-Strafrecht

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- Blockieren von Bestelladresse und Server
  - Webseite nicht abrufbar
  - Laufend Anfragen (klassische DDoS-Attacke)
  - → **§ 126b StGB** (Störung der Funktionsfähigkeit eines Computersystems)
    - bis 6 Monate (360 TS)
    - bei längerer Zeit Funktionsunfähigkeit: bis 2 Jahre
    - mehrere Computersysteme unter Verwendung eines Computerprogrammes: 3 Jahre
    - > EUR 300.000: 6 Monate – 5 Jahre

IT-Strafrecht

u|l|s|r

| **Zahlen und Fakten**

  | Keine neue Erkenntnis: Rasanter Anstieg der Anzeigen

	2005	2014	2015	Prozent (zu 2014)
CyberCrime-Anzeigen	1.800	9.000	10.010	+ 11,6 %
Aufklärungsrate		*40,8%*	*41,5%*	*+ 0,7*
Hacking		677	387	- 42,8 %
Betrügerischer Datenmissbrauch		404	647	**+ 60,1 %**
Ransomware ~~(nur 126a berücksichtigt)~~		140	144	**+ 2,9%**
Störung Funktionsfähigkeit (DDoS)		140	164	**+ 17,8%**

Quelle: Cybercrime Österreich Jahresbericht 2015, Bundeskriminalamt

IT-Strafrecht

u|l|s|r

| **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**

| IT-Dienstleister und Buchungssoftware
| Ausspionieren von Kundendaten
| Erpressung mittels Ransomware
| Blockieren von Bestelladresse und Server
| Fake president fraud

IT-Strafrecht

- **Ein Blick hinter die Zahlen: Beispiele aus der Praxis**
- Fake president fraud (CEO-Fraud)
  - E-Mail von einem Vorgesetzten
    - mit dringendem Zahlungsaufforderung
    - Bezugnahme auf bestimmte Angelegenheit
    - auch an RA-Kanzleien (Bsp.: dr-martina-haag@gmx.de – Angezeigt als „Martina Haag")
  - Korrespondenz nur per direktem Antwort-Mail
  - Oft auch telefonisch
    - Kontakt-Information leicht herauszufinden
    - Kenntnis der Praxis

IT-Strafrecht

- **Probleme**
  - Aufklärungsquote
  - Selbst Verurteilung führt nicht zwingend zur Schadenswiedergutmachung

to do …

- **Teil I – Gefährdungspotenziale**
  - **CyberCrime / IT-Strafrecht**
  - **Zivilrechtliche Haftungsfallen**
  - **Verwaltungsrecht**
- Teil II – Maßnahmen für Datenschutz und Datensicherheit
- Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung

Datensicherheit

- **Zivilrechtliche Haftungsfallen**
- Abseits des Strafrechtes: Nicht von der Statistik umfasst
  - Zivilrecht
  - Verwaltungsrecht (Datenschutz)
- Datenverlust, Datenbeschädigung, etc. kann auch ohne strafrechtlich relevante Handlung eines Dritten eintreten
  - → zivilrechtliche Folgen
    - Schadenersatz
    - Unterlassungsanspruch

Datensicherheit

- **Zivilrechtliche Haftungsfallen – Beispiel**
  - Mitarbeiter öffnet E-Mail mit Schadsoftware
  - Sicherheitsvorkehrungen / Passwörter geknackt
  - → Erhalt sämtliche Kundendaten
    - Exkurs: Steuerdaten beträchtliches Geheimhaltungsinteresse; hohes Erpressungsrisiko
  - Gegenständliche mit Bankverbindung, Kundendaten Einkäufe getätigt
  - **→ Haftung des Unternehmens!?**
    - Kein Antivirus / Spamfilter
    - Keine interne Vorgaben zum Umgang mit E-Mails mit bestimmten Anhängen
    - Gibt es dafür überhaupt eine Verpflichtung?

Datensicherheit

- **Zivilrechtliche Haftungsfallen – Beispiel**
- Jeder Auftraggeber hat Datensicherheitsmaßnahmen zu ergreifen (§ 14 DSG; *Exkurs: auch Dienstleister*)
  - Welche?
    - Schutz vor zufälliger oder unrechtmäßiger Zerstörung
    - Schutz vor Verlust
    - Gewähr der ordnungsgemäßen Verwendung
    - Nur Befugten zugänglich

Datensicherheit

- **Zivilrechtliche Haftungsfallen – Beispiel**
- **→ Verletzung der Datensicherheitsmaßnahmen**
  - Rechtswidrigkeit
    - Verletzung des Vertrages mit dem Kunden?
    - Verletzung eines Schutzgesetzes?
  - Schuldhaft
    - Außerachtlassung der Sorgfaltspflicht
    - IT-Sicherheit dem Stand der Technik zu gewähren ist Teil der Sorgfalt eines ordentlichen UN

- Konsequenzen / Sanktionen
  - Schadenersatz
    - zB für Wiederherstellung der Daten, unterlassene Benachrichtigung an Kunden, etc.
    - **Änderung DS-GVO**: auch immaterieller Schaden

Datengeheimnis

- **Datengeheimnis** (§ 15 DSG)
  - Auftraggeber, Dienstleister und deren Mitarbeiter haben Daten geheim zu halten
    - wenn aufgrund der berufsmäßigen Beschäftigung anvertraut
    - wenn kein rechtlich zulässiger Grund für eine Übermittlung
  - Kreis weiter als § 9 VStG
  - → Verpflichtungserklärungen einholen (DV)

Betroffenenrechte

- **Reaktion auf Kundenanfragen**
- Betroffenenrechte
  - Recht auf Auskunft
  - Recht auf Richtigstellung / Löschung
- Verfahren vor Datenschutzbehörde
  - Verstoß gegen die Auskunftspflicht
- Verfahren vor den Landesgerichten
  - Verstoß gegen Richtigstellung / Löschung / Geheimhaltung *(im privaten Bereich)*

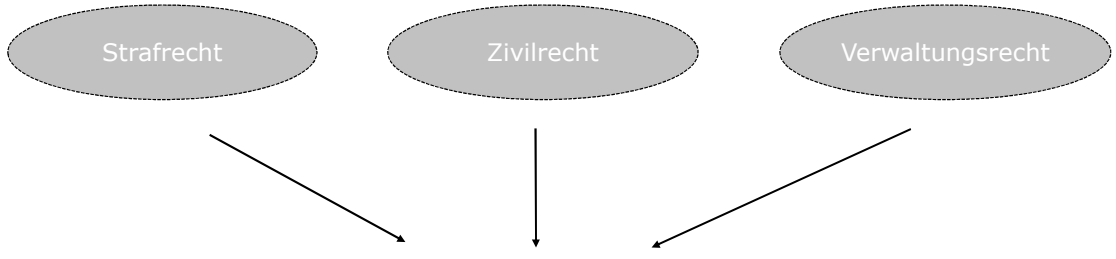
to do …

- **Teil I – Gefährdungspotenziale**
  - **CyberCrime / IT-Strafrecht**
  - **Zivilrechtliche Haftungsfallen**
  - **Verwaltungsrecht**
- Teil II – Maßnahmen für Datenschutz und Datensicherheit
- Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung

Datensicherheit

- Auch denkbar: **Verwaltungsübertretung**
  - Verstöße gegen Datensicherheitsmaßnahmen und Datengeheimnis
    - bis zu 10.000,00
    - Änderung DS-GVO: bis zu 10,000.000,00 und Behördenzuständigkeit
  - Verstoß gegen Auskunfts-, Richtigstellungs- und Löschungspflicht
    - bis zu 10.000,00 (wenn vorsätzlich)
    - 500,00 (wenn fahrlässig)
    - Änderung DS-GVO: bis zu 10,000.000,00 und Behördenzuständigkeit

- **Folgen für die betroffenen Unternehmen**



Haftung

Unternehmen und/oder persönlich?

Wer haftet?

- Verantwortlicher
  - IT-Sicherheit obliegt der Unternehmensführung
  - Delegierung an einzelne Mitarbeiter / Datenschutzbeauftragte möglich
- Juristische Personen: Geschäftsführerhaftung?
  - Datenschutz = Bestandteil der unternehmerischen Sorgfaltspflichten
  - Haftung gegenüber der Gesellschaft
    - Schadenersatz, Geldbußen
  - Gegenüber Dritten bei Schutzgesetzverletzung
    - DSG, DS-GVO
    - Nicht selbst tätig: Auswahl- und Überwachungsverschulden
- Geldbußen nach VbVG denkbar
  - Straftat durch Unterlassung bestimmter Sorgfaltspflichten begangen

to do …

- Teil I – Gefährdungspotenziale
- **Teil II – Maßnahmen für Datenschutz und Datensicherheit**
- Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung

Datensicherheit

- Wirtschaftstreuhänder / Steuerberater verarbeiten Kundendaten
  - → Auftraggeber iSd DSG
  - Exkurs: Dienstleister bei reiner Lohnverrechnung

- *wie bereits besprochen …*
- Jeder Auftraggeber hat Datensicherheitsmaßnahmen zu ergreifen (§ 14 DSG; *Exkurs: auch Dienstleister*)
  - Wogegen?
    - Maßnahmen zur **Schadensminimierung** bei Eintritt von Schadensfällen
    - unabhängig des Grundes – höhere Gewalt, organisatorisches/technische Mängel, menschliches Fehlverhalten, etc.
    - Maßnahmen zur **Rekonstruktion** von Programmen und Daten
    - Maßnahmen zur **Verringerung des Manipulationsrisikos**

Datensicherheit

- **Datensicherheitsmaßnahmen**
  - Wie?
    - dem Stand der Technik entsprechend (dynamisch beurteilen)
    - wirtschaftlich vertretbar

- **Datensicherheitsmaßnahmen konkret** *(auszugsweise)*
  - Risikoanalyse
    - → Einschätzung der angemessenen Vorkehrungen
  - Technische Maßnahmen
    - Firewall, Virenschutz, Verschlüsselung von Daten und Endgeräten, Updatemanagement, etc.
  - Personelle Maßnahmen
    - Belehrung und Sensibilisierung der Mitarbeiter
    - Häufigste „Fehlerquelle

Datensicherheit

- **Datensicherheitsmaßnahmen konkret** *(auszugsweise)*
  - Organisatorische Maßnahmen
    - Festlegung der Aufgabenverteilung
    - Strikte Zweckwidmung der Daten nur für Auftragsabwicklung
    - Beschränkung der Zugriffsrechte
    - Kennwortrichtlinien, **Richtlinien E-Mail-Nutzung**
    - Vorgaben BYOD *(bring your own device)*
    - **Geeignete Backupstrategie**
    - Mehr-Augen-Prinzip (zB fake president fraud)
    - Überprüfung der Einhaltung der Vorgaben
    - Dokumentationspflicht und Pflicht zur Protokollierung (von Änderungen, Abfragen, Übermittlungen)
  - Festlegung von Reaktionsszenarien zu Betroffenenrechte

Datensicherheit

- **Datensicherheitsmaßnahmen konkret**
  - Bei Ausgliederung an einen IT-Dienstleister
    - Überzeugung von dessen Zuverlässigkeit (erhöhte Sorgfaltspflicht bei der Auswahl)
    - Saubere Dienstleistungsverträge
    - Haftungsfreizeichnungen, Schad- und Klagloshaltungen, etc.
- **Schaden eingetreten**
  - Informationspflicht an den Kunden (data breach notification)
  - **Änderung DS-GVO**: Hinkünftig auch an die Behörde

to do …

| Teil I – Gefährdungspotenziale
| Teil II – Maßnahmen für Datenschutz und Datensicherheit
| **Teil III – Ausgewählte Neuerungen der Datenschutz-Grundverordnung**

DS-GVO

| **Neuerungen**

1. Einwilligung des Betroffenen
2. Data breach Notification
3. Verzeichnis bei Beauftragung von Auftragsverarbeitern
4. Verzeichnis der Verarbeitungen
5. Recht auf Vergessen (werden)
6. Strafen

(auszugsweise)

Was wird neu?

- **Einwilligung des Betroffenen**
  - = einer der Rechtfertigungsgründe
- Anforderungen wie bisher
  - freiwillig
  - in Kenntnis der Sachlage
  - Widerrufsmöglichkeit
- Zusätzlich: eindeutig bestätigende Handlung
  - also zB.: schriftliche/mündliche Erklärung, Anklicken eines Kästchens
  - nicht (mehr) zulässig: Stillschweigen, Untätigkeit, vorausgewählte Kästchen, AGB
- → Einwilligungen bereits jetzt umstellen
  - Mitarbeiter, Kunden, Bürger
  - Bleiben zulässig, wenn inhaltlich/formell den Anforderungen der DSGVO entsprechen

Was wird neu?

- **Data Breach Notification**
- Zweierlei Meldepflichten:
  - Information an den Betroffenen
    - um Schaden des Betroffenen abzuwehren; zB bei Hacking einer Bankverbindung
  - neu: Information an die zuständige Aufsichtsbehörde
    - um Überprüfen der AG-Pflichten durchführen zu können
    - Höchstwahrscheinlich an die DSB
    - Was ist in welchem Umfang passiert?
    - Welche und wie viele Daten sind betroffen?
    - Welche Maßnahmen zur Schadensabwehr wurden ergriffen? → Behörde Recht, Maßnahmen aufzutragen

Was wird neu?

- **Data Breach Notification**
- Wer muss anzeigen?
  - immer der VV
  - ist ein AV vorhanden, hat der VV im Vertrag bzw. in den AGB festzuhalten, dass der DL unverzüglich nach Bekanntwerden den AG von Datenlecks zu informieren hat.
  - DS-GVO: Es haften beide, der Betroffene kann sich dann aussuchen, an wen er sich wendet
    - → Schad- und Klagloshaltung im AV-Vertrag
- Wann?
  - Binnen 72 Stunden

Was wird neu?

- **Beauftragung von Auftragsverarbeitern**
- Verzeichnis führen
- Vollständige AV-Vertragskette
- Sinnvoller Inhalt einer Auftragsdatenverarbeitungs-Vereinbarung, u.a.:
  - Einhaltung DSG, Sicherheitskonzept, Vertragszweck
  - keine Werbung an die Betroffenen schicken
  - keine Übermittlungen in ein Drittland vorzunehmen
    - weil der AG für den Bescheid der DSB verantwortlich ist
  - keine Sub-AV einsetzen (oder solche zu nennen),
  - Daten nach Verarbeitung löschen
  - Information Data Breach Notification
  - Protokollierung von Datenübermittlungen
  - Prozess für austretende Mitarbeiter (damit die keinen Zugriff mehr haben)
  - Ausschluss von Haftungsbeschränkungen (zB aus Hauptverträgen) für Datenschutzverstöße

Was wird neu?

- **Verzeichnis der Datenverwendungen**
  - Führung eines Verzeichnis der DV (trifft nun auch Auftragsverarbeiter direkt)
    - „ersetzt" Meldepflicht
    - Tipp: Anhalten an Standard- und Musterverordnung
    - Inhalt: Name des VV, Zweck, Datenkategorien, Übermittlungen, Fristen für Löschung
    - Ideal: Interner Aktenvermerk vorab, ob/welche Risiken erwartet und wie sie verhindert werden können
    - Form: Schriftlich oder elektronisch ausdruckbar (zB Word, Excel, Datenbank)
  - Eine Verarbeitung – ein Eintrag
    - Grobe Einteilung der Verarbeitungen besser als zu aufgesplittet
    - *„Personaldatenverwaltung"* oder *„Lohnbuchhaltung"*, *„Urlaubsverwaltung"*, *„Zeiterfassung"* eigene Verarbeitungen?
  - Ausnahme:
    - Nicht bei < 250 Mitarbeiter und wenn weitere Voraussetzungen (zB DV „nicht nur gelegentlich") vorliegen

Was wird neu?

- **Recht auf Vergessen (werden)**
  - Bereits jetzt gegeben (Zweckbindungsgrundsatz)
  - Jeder Betroffene kann ohne Grund, ohne Formzwang Antrag stellen
  - Zu löschen sind:
    - Nicht mehr notwendige Daten (Zweckbindungsgrundsatz)
    - Widerruf der Zustimmung
  - Nicht zu löschen bei:
    - Erfüllung einer rechtlichen Verpflichtung
    - Erfüllung einer im öffentlichen Interesse liegenden Aufgabe
  - → Löschungsprozedere festlegen

Was wird neu?

- **Strafen**
  - Strafbefugnis bei der DSB
  - Wohl erforderlich: neue Unternehmensverantwortlichkeit (Strafe direkt an Unternehmen)
  - Höhe
    - Geldbußen bis zu 10 Mio Euro oder bis zu 2 % seines weltweiten Jahresumsatzes (zB Sicherungsmaßnahmen)
    - Geldbußen bis zu 20 Mio Euro oder bis zu 4 % seines weltweiten Jahresumsatzes je nachdem, was höher ist
    - Höchststrafe muss auch eintreten können, d.h. die Umsetzung kann hier nicht geringere Strafen oder Mechanismen festlegen, die dafür sorgen, dass die Strafe nicht so hoch wird

kontakt

RA Mag. Martin Führer, LL.M.
Rechtsanwalt
Lektor FH St. Pölten
Zertifizierter Datenschutzbeauftragter

urbanek | lind | schmied | reisch
RECHTSANWÄLTE OG

3100 St. Pölten, Domgasse 2

tel | 02742 **|** 351 550 119

mail | fuehrer@ulsr.at
fb | www.facebook.com/ulsr.rechtsanwaelte
hp | www.ulsr.at

IOS
INSTITUT ÖSTERREICHISCHER
STEUERBERATER

Informationsveranstaltung
Donnerstag, 23.02.2017

„Cyber Versicherung – Schutz gegen digitale Angreifer“

Referentin:
Mag. Kerstin Keltner
(Koban Südvers GmbH)

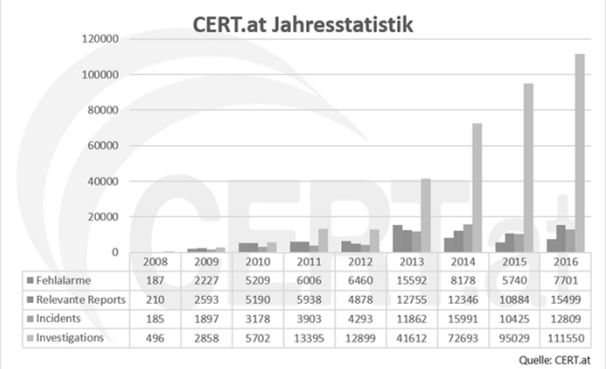
Cyber Versicherung

Schutz gegen digitale Angreifer

Wien, 23.02.2017

WBN
Worldwide Broker Network

Cyber Crime Aktuell



	2008	2009	2010	2011	2012	2013	2014	2015	2016
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550

Quelle: CERT.at

- **KPMG Studie: 49% der österreichischen Unternehmen wurden bereits Opfer einer Cyber-Attacke**
- **Anfang 2016: bis zu 25.000 Erpresser Trojaner pro Tag in Österreich**

WBN

Cyber Versicherung - Deckungsumfang

Haftpflichtschäden	Eigenschäden
Cyber Haftpflichtschäden	Cyber Krisenmanagement
	Cyber Erpressung
	Cyber Betriebsunterbrechung
	Cyber Kreditkartenschaden

Eigenschäden

Cyber Krisenmanagement

- **24h-Hotline eines IT-Sicherheitsexperten**
  - HiSolutions, MSG, Corporate Trust, KPMG
- **Kosten für IT-Forensik**
  - Kosten zur Wiederherstellung von Daten und Systemen
  - Ursachenermittlung und Ermittlung des Schadenumfangs
- **Data Breach Notification Costs**
  - Identifikation der betroffenen Personen
  - Honorare externer Rechtsanwälte zur Prüfung und Erfüllung der geltenden Melde- und Anzeigepflichten
- **Public-Relations-Maßnahmen**
  - Unterstützung bei der krisenfallbezogenen Öffentlichkeitsarbeit

Eigenschäden

- **Cyber Erpressung**
  - Kosten zur Schadenabwehr und -minderung
  - Lösegeldzahlungen
  - Belohnungsgelder
- **Cyber Betriebsunterbrechung**
  - Fortlaufende Kosten
  - Entgangener Betriebsgewinn
  - Mehrkosten
- **Cyber Kreditkartenschaden**
  - Bereitstellung von Kreditschutz- und Kreditüberwachungsdienstleistungen für betroffene Personen
  - PCI (Payment Card Industry) Vertragsstrafen

Haftpflichtschäden

Cyber Haftpflichtschäden – Freistellung und Abwehr von Haftungsansprüchen (reine Vermögensschäden inkl. immaterielle Schäden)

- **Datenschutzverletzungen oder IT-Sicherheitsverletzungen**
  - Personenbezogene Daten sowie Betriebs-/Geschäftsgeheimnisse
  - Vertragliche Geheimhaltungspflichten
- **Rechtsschutz für Straf- und Verwaltungsstrafverfahren**
  - Rechtsfreundliche Vertretung gegenüber der Datenschutzbehörde
  - Beauftragung eines externen Rechtsanwaltes/Strafverteidigers
- **Bußgelder**
  - Versicherungsmöglichkeit umstritten

Wir vermögen mehr …

Vielen Dank für Ihre Aufmerksamkeit!

Mag. Kerstin Keltner
KOBAN SÜDVERS GmbH
Kopfgasse 7, A-1130 Wien
Tel.: +43 (0) 1 877 70 00 -70
Fax.: +43 (0) 1 877 70 00 - 66
E-Mail: kerstin.keltner@kobangroup.at

IOS
INSTITUT ÖSTERREICHISCHER
STEUERBERATER

Informationsveranstaltung
Donnerstag, 23.02.2017

„Vertrauensschaden Versicherung – Schützt sie auch bei Cyberbetrugsschäden?“

Referent:
Dr. Georg Aichinger
(Koban Südvers GmbH)

I. Einführung in die Vertrauensschadenversicherung

Die VSV greift idR bei vorsätzlich unerlaubten Handlungen, wie zB

- Raub, Diebstahl, Unterschlagung, „klassischem" Betrug, zT Untreue
- Geheimnisverrat
- Computerbetrug (Eingriffe in das EDV System, Software Manipulationen)

…die bei der versicherten Kanzlei zu Vermögensschäden führen und

nach den gesetzlichen Bestimmungen zu Schadenersatz verpflichten.

I. Einführung in die Vertrauensschadenversicherung

Der Versicherer trägt

- Kosten, die bei der Rechtsverfolgung oder für die Schadenermittlung entstehen und
- ersetzt Vermögensschäden, die dem vn Unternehmen von Vertrauenspersonen (Mitarbeitern und Dritten) zugefügt werden. Die VSV bietet so einen schnellen Liquiditätsersatz.

MARKT: In Österreich bieten rund 10 Versicherer gute Lösungen für Steuerberatungskanzleien an.

KOSTEN: Eine Absicherung ist zu relativ moderaten Prämien möglich.

II. Versicherungsschutz bei *Fake President* Fällen

= zunächst Fall für die „Vertrauensschaden Versicherung“

Weshalb besteht aber oftmals kein Versicherungsschutz?

Viele Steuerberatungskanzleien haben

- keine VSV abgeschlossen.
- zwar eine VSV aber
  - mit viel zu geringer Versicherungssumme und/oder nur einem „Sublimit“ für *solche* Fälle.
  - eine ältere Polizze, die die Mitversicherung *solcher* Betrugsfälle gar nicht vorsieht, wegen
    - des Fehlens einer Erwähnung in der primären Risikoumschreibung
    - des Vorliegens eines dezidierten Ausschlusses von Cyberbetrugsschäden
    - des Risikoausschlusses der „*grob fahrlässigen Herbeiführung eines Versicherungsfalls*“
    - einer vereinbarten nachteilhaften Subsidiaritätsklausel („*anderweitige Versicherungen*“).

III. Schlussfolgerungen

1. Eine VSV kann nach Cyber Betrug Versicherungsschutz bieten, jedoch nur bei
   a. optimaler Ausgestaltung und hoher Versicherungssumme
   b. klar geregelter und auf die anderen Polizzen abgestimmter Subsidiaritätsklausel

2. Eine VSV ersetzt aber keine gute Cyber Versicherung, weil sie nur eine bewusste Lücke in der Cyber Versicherung füllt, diese aber nicht kopiert. keine Doppelversicherung

Vielen Dank für Ihre Aufmerksamkeit.

Kontakt:

Dr. Georg Aichinger
Geschäftsführer

Koban solDORA GmbH
Kopfgasse 7, 1130 Wien
Tel: +43 1 877 70 00 30
Mobil: +43 664 255 32 37

georg.aichinger@kobangroup.at
www.kobansoldora.at