# Sind Sie sicher?
# IT-Sicherheit: Wie geh ich's an?

**Interaktives Expertengespräch mit Mag. Verena Becker**

Donnerstag, 20. Oktober 2016
14.00 – 14:45 Uhr

Die Teilnehmerinnen und Teilnehmer des Interaktiven Expertengesprächs hatten die Möglichkeit über Chat live Fragen zu stellen. Wir haben die Fragen für Sie gesammelt und unsere Expertin hat sie mit Unterstützung von Harald Wenisch, IT-Security Experts Group, beantwortet.

**Die Expertin**

Mag. Verena Becker, BSc (WU) hat Rechtswissenschaften und Betriebswirtschaftslehre studiert. Sie ist in der Bundessparte Information und Consulting der WKÖ für das Projekt „it-safe.at" verantwortlich.

**1. Ich sichere meine Buchhaltung in der Cloud. Ist das eine gute Lösung?**

Die Datensicherung in der Cloud hat Vor- und Nachteile.

Bei der Online-Sicherung werden Daten über das Internet zu einem Cloud-Speicher-Anbieter übertragen und können dort im Notfall abgerufen werden.
Daten sind außer Haus gespeichert und damit räumlich getrennt von den Originaldaten
Die Daten können online von überall her abgerufen werden.

Es ist jedoch wichtig, sich den Anbiete genau anzuschauen und u.a. folgende Fragen zu stellen:
Wo genau sind die Daten? Aus rechtlicher Sicht ist es sinnvoll einen Anbieter mit einem Rechenzentrum in Österreich oder innerhalb der EU zu wählen.
Welchen Schutz bietet der Cloudanbieter (Datenschutz, IT-Sicherheit, Verschlüsselung)?
Besondere Vorsicht ist bei personenbezogenen Daten geboten.
Wie erfolgt die Datenübermittlung bei schützenswerten Daten? (Verschlüsselung)
Vertrag: Kosten, Vertragsdauer, Möglichkeit der Kündigung, wem gehören die Daten…

Die Verantwortung für die Daten tragen Sie als Unternehmer!

**2. Kann ich mich gegen IT-Sicherheitsvorfälle versichern?**

Cyberversicherungen sind in den USA weit verbreitet, in Europa aber relativ neu.
IT-Security-Versicherungen decken eigene Schäden und Drittschäden (Cyberhaftpflicht) und sind als Absicherung bei Datenverlust, Datendiebstahl und Hacking zunehmend interessant.
Cyberversicherungen sind aber keinesfalls ein Ersatz für ein Sicherheitskonzept, sondern eine Ergänzung. Die Versicherungen schauen sich im Vorfeld z.B. mittels eines Fragebogens ganz genau an, welche Sicherheitsvorkehrungen im Unternehmen getroffen werden.
Falls es schon Sicherheitsvorfälle im Unternehmen gab, sind Ausschlüsse möglich, Selbstbehalte sind durchaus üblich.

**3. Wie hoch sind die Lösegeldforderungen bei Erpressertrojanern?**

Die Lösegeldforderung bei Erpessertrojaner erfolgt meist in Bitcoin.
Die bekanntgewordenen Forderungen beginnen bei ca. bei 0,5 Bitcoin bis zu 3 Bitcoin.
Teils erhöhen sich die Forderungen, wenn zugewartet wird bzw. je interessanter das Ziel ist.
Ein Bitcoin entspricht derzeit rund EUR 600, wobei der Bitcoin-Kurs stark schwankt.
Die Zahlung für die Entschlüsselung erfolgt über das anonyme Tor-Netzwerk und ist kaum nachverfolgbar.

**4. Wir sind eine kleine Tischlerei und haben eine eigene Firmenwebsite, auf der eigentlich nur unsere Adresse, Öffnungszeiten und Fotos drauf sind. Muss ich mir trotzdem Sorgen machen, dass die Seite gehackt werden könnte?**

Leider ja.
Als Betreiber sind Sie für Ihre Website verantwortlich.
Gerade bei kleineren Internetportalen werden Sicherheitsaspekte oft gar nicht berücksichtigt, wodurch Hacker hier leichtes Spiel haben. Es können z.B. Virenprogramm installiert oder Website verunstaltet („hacked by…“) werden. Websites können zum Spamversand oder für Angriffe auf andere Websites missbraucht werden, mit der Folge, dass die Website auf einer Backlist landet oder Google vor der Website warnt.
Als Mindestvorkehrungen sollten Sie daher Webapplikationen auf dem aktuellen Stand halten, Backups der Daten, Datenbanken und Systemdateien Ihrer Webanwendung machen und sichere Passwörter verwenden.
Wenn Ihre Website gehackt wird, schließen Sie die Sicherheitslücken umgehend.

**5. Brauche ich für mein Android-Handy eine Firewall?**

Grundsätzlich stellen Smartphone-Hersteller regelmäßig Sicherheits-Updates zur Verfügung. Gerade im mobilen Bereich ist aber Malware ein Riesenproblem: Es können z.B. teure SMS versendet, Nutzerdaten ausspioniert, Twitter- oder Facebook-Konten gekapert werden. Die Installation einer zusätzlichen Sicherheits-App ist sicher empfehlenswert, oft bieten die Apps auch diverse Zusatzfunktionen wie Diebstahlschutz an.

**6. Ich arbeite allein, habe nur ein Notebook und ein Smartphone. Was sind die wichtigsten Punkte, die ich beachten muss?**

Daten sichern
Passwortsicherheit beachten
Firewall und Virenschutz installieren und regelmäßig aktualisieren
Regelmäßig Sicherheits-Updates durchführen

**7. Bin ich gesetzlich verpflichtet etwas für meine IT-Sicherheit zu tun?**

Derzeit gibt es **keine allgemeine gesetzliche Vorschrift** zur Einhaltung von IT-Sicherheitsmaßnahmen.
Auszugsweise sind folgende Vorgaben zu beachten:
**Die bestehende EU-Richtlinie zur Netz- und Informationssicherheit muss** in Österreich bis 2018 durch ein Cybersicherheitsgesetz umgesetzt werden. Diese betrifft aber vorwiegend kritische Infrastrukturen wie Energieversorger oder Banken und die Betreiber wesentlicher Dienste.
Alle Unternehmen müssen aber nach UGB mit der Sorgfalt eines ordentlichen Kaufmannes handeln. Informationssicherheit ist eine Managementverantwortung. Dies kann im

Kapitalgesellschaftsrecht aus der Verantwortlichkeit eines ordentlichen Geschäftsleiters abgeleitet werden, die auch die Verantwortung für Risiken umfasst.
**Das Datenschutzgesetz** regelt den Umgang mit personenbezogenen Daten (z.B. Name, Geburtsdatum, Adresse, Geschlecht, Einkommen). Im Sinne der Datensicherheit müssen organisatorische und technische Maßnahmen getroffen werden, um personenbezogene Daten zu schützen und sicherzustellen, dass keine Unbefugten an die Daten gelangen.
Bei der Archivierung von Daten sind gesetzliche Aufbewahrungsfristen zu beachten, z.B. müssen gemäß Bundesabgabenordnung Bücher, Aufzeichnungen und Belege 7 Jahre aufbewahrt werden.
**Grundsätzlich können bei Sicherheitsvorfällen auch Schadenersatzansprüche entstehen**, z.B. wenn Kreditkarten von Kunden gestohlen werden oder Pönalen, wenn Aufträge im B2B-Bereich nicht fristgerecht fertiggestellt werden können.

**8. Was passiert, wenn meine elektronischen Aufzeichnungen für das Finanzamt durch einen Defekt gelöscht wurden?**

Es handelt sich um einen Verstoß gegen die Aufbewahrungspflicht. Dieser kann zur Schätzung der Besteuerungsgrundlagen durch die Finanzbehörde führen.

**9. Ich betreibe ein kleines Gasthaus und will für meine Gäste ein WLAN einrichten lassen. Was muss ich dabei beachten?**

Trennen Sie Gäste-Wlan und Firmen-Netzwerk unbedingt strikt voneinander, sodass für Gäste ausschließlich die Verbindung zum Internet möglich ist.
Es ist empfehlenswert, den Zugang für das Gäste-WLAN durch ein Passwort zu schützen. Dadurch haben sie bessere Kontrolle und es wird verhindert, dass es als kostenloser Internetzugang missbraucht wird.
Sichern Sie den WLAN-Anschluss hinreichend vor dem Zugriff von Unbefugten durch eine handelsübliche Verschlüsselung (WPA1, 2).
Das Gäste-Wlan sollte erst nach dem Akzeptieren einer Benutzerordnung (Verbot des widerrechtlichen Down- und Uploaden von urheberrechtlich geschützten Dateien, Empfehlung von Schutzmaßnahmen wie Virenschutz/Firewall etc.) aktiviert werden können. Dies dient ihrer eigenen rechtlichen Absicherung. Ansonsten könnten z.B. Abmahnbriefe wegen Urheberrechtsverletzungen drohen.

**10. Wie lange muss ich meine Daten sichern?**

Eine Datensicherung ersetzt nicht unbedingt eine Archivierung Ihrer Daten und umgekehrt.

Wie lange die Daten aufbewahrt werden sollten, ist genauso wie im normalen Büro mit Papierunterlagen unterschiedlich.

Hier einige Praxisbeispiele dazu:
Beispiel EDV-Buchhaltung: Daten über das betriebliche Rechnungswesen müssen sieben Jahre aufbewahrt werden, ebenso elektronische Aufzeichnungen in Zusammenhang mit der Registrierkassenpflicht (z.B. Datenerfassungsprotokoll, Startbeleg, Monatsbeleg usw.)

Unterlagen von anhängigen Abgaben- oder Gerichtsverfahren müssen trotz Fristablauf weiter aufbewahrt werden.

Beispiel personenbezogene Daten:

Wenn der rechtmäßige Zweck für die Datenverarbeitung wegfällt, müssen die Daten gelöscht werden. Wenn z.B. ein Kunde sein Online-Konto bei einem Webshop schließt, sind Benutzername und Passwort zu löschen, die zugehörigen Daten für das betriebliche Rechnungswesen sind aber 7 Jahre aufzubewahren.

Verträge oder Unterlagen über Versicherungen sollten „lebenslang" aufbewahrt werden.

## 11. Was sind Bitcoins genau und wo werden diese gehandelt?

Bitcoin ist eine weltweit verwendbare und durch Verschlüsselungstechniken von Computern errechnete Währung. Dabei wird anders als im normalen Bankverkehr keine zentrale Abwicklungsstelle verwendet. Bitcoins kann man z.B. an Internet-„Börsen", bei Internet-„Wechselstuben", bei Trafiken oder Automaten kaufen und verkaufen.
Bitcoin dienen sowohl als Zahlungsmittel, als auch als Spekulationsobjekt.

Bitcoin-Kontoinhaber haben einen öffentlichen Schlüssel (ähnlich einer Kontonummer) und einen privaten, vom System berechneten Schlüssel (ähnlich einer TAN). Bei einer Transaktion wird die Zusammengehörigkeit dieser Zahlenschlüssel im Netz geprüft. Wenn alles in Ordnung ist, erfolgt die Übertragung der Bitcoins von einer elektronischen Geldbörse in die andere.

Da die Internetwährung teils auch aufgrund von Hackerangriffen sehr volatil ist, ist beim Handel besondere Vorsicht geboten.

## 12. Welche wesentlichen Neuerungen kommen durch die EU-Datenschutz-Grundverordnung auf Unternehmen zu?

Auszug: KC-Merkblatt EU-Datenschutz-Grundverordnung, WKO

- Es wird keine Meldepflicht bei der Datenschutzbehörde (Datenverarbeitungsregister) mehr geben.

- Statt dessen stärkere Verantwortung für Verantwortliche (derzeit „Auftraggeber") und Auftragsverarbeiter (derzeit „Dienstleister") und weitreichende Neuregelung der Pflichten bei der Datenverarbeitung:◦Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („privacy by design/privacy by default"): Es sind geeignete technische und organisatorische Maßnahmen und Verfahren (z.B. Pseudonymisierung) zu treffen, damit die Verarbeitung den Anforderungen der Verordnung genügt und die Rechte der betroffenen Personen geschützt werden. Datenschutzrechtliche Voreinstellungen sollen sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

- Verantwortliche und Auftragsverarbeiter müssen ein „Verzeichnis von Verarbeitungstätigkeiten" führen: Der Inhalt ist ähnlich den derzeitigen DVR-Meldungen und hat insbesondere die eigenen Kontaktdaten, die Zwecke der Verarbeitung, eine Beschreibung der Datenkategorien und der Kategorien von betroffenen Personen, die Empfängerkategorien, gegebenenfalls Übermittlungen von Daten in Drittländer, wenn möglich die vorgesehenen Löschungsfristen und eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen zu enthalten.

- Diese „Dokumentationspflicht“ trifft Unternehmen mit weniger als 250 Mitarbeitern dann nicht, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien bzw. die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten einschließt.

- Meldungen von Verletzungen des Schutzes personenbezogener Daten sind sowohl den nationalen Aufsichtsbehörden (ohne unangemessene Verzögerung – möglichst binnen höchstens 72 Stunden nach dem Entdecken; außer die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten) als auch der betroffenen Person (ohne unangemessene Verzögerung, wenn die Wahrscheinlichkeit besteht, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt) mitzuteilen.

- Pflicht zur Datenschutz-Folgenabschätzung bei Verarbeitungsvorgängen, die (insbesondere bei Verwendung neuer Technologien) aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.

- Vorherige Konsultation der Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der für die Verarbeitung Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

- (Verpflichtender) Datenschutzbeauftragter: Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für Unternehmen (Verantwortliche und Auftragsverarbeiter), wenn ◦die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht.

- (Neue) Informationspflichten und Betroffenenrechte Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden

- Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu erledigen (diese Frist kann um höchstens weitere 2 Monate verlängert werden)

    - Auskunftsrecht (u.a. auch über geplante Speicherdauer)
    - Recht auf Berichtigung
    - Recht auf Löschung und auf „Vergessen werden“
    - Recht auf Einschränkung der Verarbeitung
    - Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
    - Recht auf Datenübertragbarkeit
    - Widerspruchsrecht
    - Regelungen betreffend automatisierte Generierung von Einzelentscheidungen einschließlich profiling

- Befugnisse und Aufgaben der Aufsichtsbehörden werden erweitert, insbesondere auch Verhängung von „Geldbußen“

- Hohe Strafen Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

## 13. Wie oft soll man eine Datenrücksicherung testen

Eine auf das Unternehmen abgestimmte Datensicherungsstrategie ist einer der wichtigsten Punkte in Bezug auf IT-Sicherheit.
Dabei muss auch regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, dh insbesondere, ob gesicherte Daten problemlos zurückgespielt werden können.

Abhängig davon, wie kritisch die Daten für das Unternehmen sind, empfehlen wir, diese Tests mindestens einmal jährlich durchzuführen.

## 14. Ist die Firewall im Modem vom Provider bereits integriert?

Es kommt auf das jeweilige Modem an. Eine lokale Firewall ist jedenfalls vorzuziehen und sollte aktuell gehalten werden.

## 15. Welche einfach zu administrierenden Verschlüsselungsmechanismen für Endgeräte sind empfehlenswert?

Man kann soferne Windows eingesetzt wird gleich vom Betriebssystem den Bitlocker verwenden oder auf VeraCrypt zurückgreifen bzw. unter Mac den FileVault 2, dieser ist unter OS X Lion und neuer verfügbar. Bei Linux Betriebssystem kann auch direkt LUKS eingesetzt werden.

## 16. Wie wirken sich Social Media wie WhatsApp auf die Sicherheit aus ?

In Sicherheitsprognosen zählen Social Media regelmäßig zu den Top-Risken im Sicherheitsbereich. Die Gefahren sind Social-Engineering-Attacken, manipulierte Links, ungewollter Datenabfluss und Datenabschöpfung durch Internetkriminelle. Das soll nicht heißen, dass Social Media generell nicht genutzt werden sollen, aber es sind hier besondere Vorsicht und verantwortungsbewusster Umgang notwendig.

Stand: November 2016



**Persönliche Beratung in Ihrer WKO-Landeskammer**
Burgenland, Tel. Nr.: 05 90907-3310,
Kärnten, Tel. Nr.: 05 90904-741,
Niederösterreich Tel. Nr.: 02742 851-16500,
Oberösterreich, Tel. Nr.: 05 90909-3540,
Salzburg, Tel. Nr.: (0662) 8888-441,
Steiermark, Tel. Nr.: 0316 601-357,
Tirol, Tel. Nr.: 05 90905-1372,
Vorarlberg, Tel. Nr.: 05522 305-385,
Wien, Tel. Nr.: 01 476 77-5355

**WIFI Unternehmerservice**
Das WIFI Unternehmerservice der Wirtschaftskammer Österreich hat die Unternehmerin und den Unternehmer im Fokus. Mit Interaktiven Expertengesprächen (Webinare) geht das WIFI Unternehmerservice einen neuen Weg, mit dem Ziel die Unternehmerkompetenzen zu erweitern.

Für weitere Fragen wenden Sie sich bitte an unternehmerservice@wko.at