www computertraining4you.eu
Schnell und einfach ft am PC

Online Zusammenarbeit Kapitel 1 Lektion 2
Vor- und Nachteile

- × Vorteile
- × Nachteile
- × Einige Tipps zum Surfen im Internet

✓ Neben den Vorteilen der Online Zusammenarbeit (gemeinsame Nutzung von Dateien und Kalendern, geringe Reisekosten, einfache Kommunikation und Teamarbeit, globaler Zugriff) machen Sie sich in dieser Lektion auch Gedanken über die vorhandenen Nachteile.

Aufgabe

Recherchen: http://www.wieistmeineip.de
http://anonymouse.org

Ob Smart Homes mit IP-Adressen für Ihre Haushaltsgeräte oder ferngesteuerte Autos für Sie vor- oder nachteilig sind, müssen Sie selber entscheiden.

Wenn Sie bei Stromausfall nicht in Ihr Haus können, wird es unlustig. Spätestens, wenn Banken und Versicherungen neben Ihren Postings auf Facebook auch auf den Inhalt Ihres Kühlschranks zugreifen möchten, Ihr Auto während der Fahrt gehackt oder Ihre Identität missbraucht wird, beginnt die Vernetzung gefährlich zu werden.

1. Vorteile

In der vergangenen Lektion wurde besprochen, wie IKT die Online Zusammenarbeit fördert. Durch die gemeinsame Nutzung von Dateien und Kalendern und gemeinsame Bearbeitung online wird vor allem wertvolle Zeit gespart. Dazu kommt die einfache Verwaltung, sowohl was das Hochladen, Erstellen und Freigeben von Dateien betrifft, als auch die Verwaltung – es gibt nun lediglich eine einzelne Datei anstatt zahlreicher veränderter Dateien.

Das Outsourcing der IT verringert vor allem für kleinere Firmen die Kosten, weil keine eigene IT-Abteilung vorhanden ist. Bei defekter Hardware werden weder Fehler gesucht, noch neue Geräte angeschafft. Außerdem sind die Daten (bei einer aktiven Internetverbindung) schnell verfügbar.

Sprechen wir von Online-Konferenzen, so können relativ schnell Meetings mit Personen aus aller Welt vereinbart werden. Weder schlagen Reise- und Hotelkosten zu Buche, noch fallen diese Personen am jeweiligen Arbeitsplatz durch Geschäftsreisen aus. Die Auswirkungen auf Teamarbeit und globale Kommunikation sind umwälzend.

2. Nachteile

Neben all den Vorteilen, machen Sie sich bewusst, dass die Online Zusammenarbeit auch Gefahren mit sich bringt:

Zugangskontrolle
In einem firmeninternen Netzwerk verwalten Administrierende, sogenannte Administratoren und Administratorinnen die Zugriffsrechte. Darum geben Sie nach dem Hochfahren des Rechners Ihren Benutzernamen und das geheime Passwort ein. Auch online müssen die Daten sicher sein. Um den unberechtigten Zugriff auf die Daten hier zu verhindern, wählen Sie sichere Kennwörter und laden Sie die Daten nur über gesicherte Verbindungen (also https) hoch. Gehen Sie dazu sorgfältig mit der Freigabe Ihrer Daten in der Cloud um.

Datensicherheit und Identitätsdiebstahl
Bevor Sie einen Anbieter von Cloud-Diensten wählen recherchieren Sie und holen Informationen ein. Neben sicherer Datenübertragung, Speicherplatz und der

Synchronisation der Daten ist vor allem der Datenschutz ein wesentliches Kriterium. Wenn Daten umgeleitet, ausspioniert oder zerstört werden, kann das den Diebstahl der Identität kosten oder dem Unternehmen hohe Verluste einbringen, im Extremfall sogar in den Ruin führen.

Identitätsdiebstahl ist nicht nur bei der Online Zusammenarbeit eine Gefahr. Auch in Firmennetzwerken oder beim privaten Surfen versuchen Hacker beispielsweise durch Social Engineering, sich Zugang zu Informationen oder zum System zu verschaffen. Dazu kann man unter anderem jemandem ganz simpel über die Schulter gucken, wenn Passwörter eingegeben werden oder sich als vertrauliche Person ausgeben und frech nach Zugangsdaten fragen.

Daten abgleichen
Synchronisieren Sie die Daten, denn so sind die Versionen online und lokal am Rechner sicher am selben Stand. Wenn Sie Dokumente für andere Personen freigeben, dann achten Sie darauf, dass diese über gleiche oder kompatible Programmversionen verfügen.

Malware
Vor Viren, Würmern, Trojanern, Phishing E-Mails oder Spyware sind Sie auch bei der Online Zusammenarbeit nicht gefeit. Sobald Ihr Rechner an das Internet angeschlossen ist, nutzen Sie Dienste eines anderen Rechners. Doch dabei kann es durchaus passieren, dass andere Nutzende Ihren Rechner ausfindig machen, die Zugangshürden überwinden und Schaden anrichten. Mit diversen Schadensprogrammen, so genannter *Malware*, werden beispielsweise Programme zum Ausspionieren installiert.

- Ein *Virus* nistet sich in einem Programm ein. Wird eine infizierte Datei geöffnet, wird der Virus aktiv und kann sich am Rechner oder in einem Netzwerk verbreiten.
- *Makroviren* sind in ein Dokument eingebettet. Normalerweise eine tolle Möglichkeit, wiederkehrende Arbeitsabläufe zu erleichtern, kann ein Makro aber auch so programmiert werden, dass es sich in andere Dateien einnistet – um hier schädliche und / oder unerwünschte Aktionen auszuführen
- *Würmer* funktionieren wie sehr einfache Viren, sie verbreiten sich aber selbständig (beispielsweise über die Kontakte in Outlook).
- *Trojaner* werden in den Computer eingeschleust. Sie tarnen sich als nützliche Software, führen im Hintergrund aber schädliche Aktionen durch, zB können Hacker so Passwörter herausfinden.
- *Backdoor-Programme* steuern fremde Computer, meist mit dem Ziel, massenhaft Spam-Mails zu versenden.
- *Keylogger* zeichnen die Tastatureingaben auf. So werden Kennwörter herausgefunden und zB gleich über das Internet an den Empfänger gesendet-
- Durch *Spyware* wird das Online-Verhalten ohne das Wissen oder Einverständnis von Webnutzenden ausspioniert.
- Sogenannte *Dos-Attacken* (Denial of Service) versenden beispielsweise viele E-Mails oder Anfragen an einen Server. Wenn dieser überlastet ist, fällt er aus und ist nicht mehr erreichbar.
- Mit *Phishing*-Mails geben sich Betrüger als eine Ihnen bekannte und seriöse Firma aus. Sie versuchen so an Zugangsdaten zum Telebanking, E-Mail-Konto oder ähnlich wichtigen Accounts zu gelangen.

Dienst- und Serviceunterbrechungen
Zuletzt brauchen Sie neben einer aktiven Internetverbindung und schneller Datenübertragung auch einen zuverlässigen Provider.

3. Einige Tipps zum Surfen im Internet

Zur eigenen Sicherheit und zur Sicherheit Ihrer Daten berücksichtigen Sie einige Tipps beim Surfen und der Arbeit online:

- Installieren Sie ein Antivirenprogramm.
- Führen Sie in öffentlichen WLANs keine sensiblen Transaktionen durch (zB Telebanking).
- Geben Sie persönliche Daten nur über https ein.
- Geben Sie Ihre Kennwörter und PIN-Codes nicht bekannt.
- Öffnen Sie keine E-Mail-Anhänge von unbekannten Personen, schon gar keine *.exe Files oder *.zip Archive.
- Kommen Sie der Aufforderung, einem Link zu folgen und Zugangsdaten einzugeben, niemals nach! Es handelt sich dabei um Phishing.
- Wer im Internet surft, hinterlässt unweigerlich eine Datenspur: Webseiten erfahren etwa die IP-Adresse[1], die Aufschluss über Ihren ungefähren Wohnort gibt. Schutz bietet zB *Anonymouse*[2]. Tippen Sie bei diesem Dienst die Adresse einer Webseite ein und besuchen Sie diese anonym.
- Sichere Passwörter sind ein Muss, um Online-Konten bestmöglich zu schützen.
- Außerdem achten Sie bitte darauf, dass Sie für jedes Konto ein eigenes Passwort verwenden. Sollte eines dieser Kennwörter geknackt werden, dann kann der Hacker damit wenigstens nicht auch noch auf andere Konten zugreifen.

Übung

1. Wenn Sie sich einmal nicht sicher sind, ob hinter einer Datei ein Virus steckt, dann prüfen Sie sie per Online-Scanner.
   - Empfehlenswert sind *VirusTotal*[3] und *Jotti*[4].
   - Laden Sie eine Datei hoch und prüfen Sie hier die Seiten gleich mit mehreren Virenscannern.
   - Nach abgeschlossener Prüfung erfahren Sie, welche Antiviren-Software Alarm geschlagen hat.

---

[1] *Öffnen Sie den Browser und geben Sie mal www.wieistmeineip.de (auch .ch oder .at) ein – so einfach wird die IP-Adresse Ihres Rechners gefunden und angezeigt.*
[2] *Den Dienst finden Sie unter http://anonymouse.org/anonwww_de.html*
[3] *https://www.virustotal.com/*
[4] *http://virusscan.jotti.org/de*

2. Was Ihre Kennwörter taugen, finden Sie mithilfe des Microsoft *Password Checkers*[5] heraus.
   - Geben Sie hier eines Ihrer Passwörter ein, erhalten Sie eine Sicherheits-Bewertung.
   - Unsichere Geheimwörter sollten Sie ersetzen. Online *Password-Generatoren*[6] unterstützen Sie dabei und erstellen sichere Kennwörter auf Knopfdruck.

Testen Sie Ihr Wissen

1. Nennen Sie Vorteile oder Online Zusammenarbeit.
2. Nennen Sie Nachteile der Online Zusammenarbeit.

Notizen

Weiter geht es mit dem Recht auf geistiges Eigentum.

[5] *https://getpass.info/de/*

[6] *Nutzen Sie aus der Vielzahl von Angeboten zB www.gaijin.at/olspwgen.php, www.passwort-generator.com/ oder http://passwortgenerator.org/*