10 Schritte zu mehr IT-Sicherheit

Jürgen Kunert

InformationsTechnologie Effizient Einsetzen, Hamburg

Einleitung

Im 21. Jahrhundert ist eine funktionierende und sichere IT-Infrastruktur die Grund-Voraussetzung für die Leistungsfähigkeit und Überlebensfähigkeit jedes Unternehmens.

„Sie sind abhängig von einer funktionierenden IT."

Risiken

- menschliches Verhalten
- das Aushebeln der technischen Mechanismen durch Schadsoftware
- Hardware-Ausfall
- Verlust von
  - Arbeitsfähigkeit
  - von vertraulichen Informationen (Preise, Produktionsgeheimnisse, ..)
  - Kommunikationsmöglichkeiten
- Erpressbarkeit
- …

Schutzziele

- **Integrität:** betrifft die Daten selbst
  Sind die Daten wirklich originalgetreu (z.B. seit Ihrer Erzeugung unverändert?)
- **Verfügbarkeit:** betrifft Zugang zu den Daten
  Sind die Daten (für Befugte!) abrufbar, wenn man sie benötigt?
  a) in dem Moment oder b) überhaupt noch
- **Vertraulichkeit:** betrifft Zugang zu den Daten
  Kann keine unbefugte dritte Person die Daten lesen?
- **Authentizität:** betrifft beteiligte Personen
  Ist die/der Autorin/Leserin der Daten wirklich die behauptete Person?

Abwägung

- Spannungsverhältnis zwischen Aufwand und Sicherheit
- Spannungsverhältnis zwischen den Schutzzielen
  - Wie viel Integrität, Verfügbarkeit, Vertraulichkeit, … brauche ich?

- Absolute Sicherheit gibt es nicht!

1. Sensibilisierung / Training der Benutzer

- Nachdenken vor den Agieren! – Gesunder Menschenverstand
- Nicht einfach auf Links klicken
- eMail-Adresse kontrollieren
- Anlagen im Zweifel nicht öffnen
- Beispiel: Bewerbungs-Trojaner
- Social Engineering!

- Mangelndes KnowHow: führt ggf. zu unbeabsichtigtem Löschen von Daten, Senden von sensiblen Daten an Unberechtigte, fälschliches Verändern von Daten, zu fehlerhafter Konfiguration von Systemen

2. Backup

- Daten, die nicht (**regelmäßig**) gesichert werden, können Sie auch nicht wiederherstellen!
- Backups, die nicht mindestens in einem Test erfolgreich **wiederhergestellt** wurden, verdienen den Namen „Backup“ nicht.
- Backup-Lösungen und –Daten, für die niemand in der Firma direkt **verantwortlich** ist, sind definitiv schlechte bis unbrauchbare Sicherungen.
- Sicherungen, die in Sie im **gleichen Raum/Gebäude** lagern, in dem sich auch Ihre restliche IT befindet, werden einen ernsten Zwischenfall wie Feuer, Überschwemmung und so weiter, sicher nicht überstehen.

2. Backup - Risikobetrachtung

- Risikobetrachtung:
  - Was sind erfolgskritische Daten und Systeme?
  - Was bedeutet der Datenverlust für das Unternehmen? Kosten, Reputation, Kundenverlust, Ende, …?
  - Wie viele Tage kann ihr Unternehmen bei einem Ausfall überleben?
  - SPOF (Single Point Of Failure)

- **Katastrophenplan**
  - Was passiert, wenn Daten und/oder Systeme nicht verfügbar sind?
  - Wenn ihr PC nicht verfügbar ist, was machen Sie dann?
  - Versicherung?

2. Backup – Fragen

- Was für Daten und Geräte haben Sie?
- Wer hat die Verantwortung?
- Was wird gesichert, wenn Dateien in Bearbeitung sind?
- Datenmenge, auch für die Rücksicherung wichtig
- Wachstum der Daten?
- Sicherungs-Rhythmus?
- Vollsicherung vs. nur Sicherung von Änderungen
- Aufbewahrungsfristen beachten
- Hardware und Betriebssystem? Server, virtuelle Maschinen, Client-PCs, Mobilgeräte?
- Lizenzen
- Installationsmedien
- Band, Festplatte, CD/DVD, Cloud, Laptop?
- Ort für dieAufbewahrung der Backups
- Datenschutz?

- Wirtschaftlichkeit?
- Versicherung abschließen?

3. Updates

- Betriebssystem (Windows Update, iOS, Android, …)
- Anwendungen (Office Update, Domino Update, …)
- Browser
- Browser Add-Ons (Adobe Flash)
- Smartphone-Apps
- Wenn möglich automatisieren

- Windows XP, Windows Server 2003?

4. Passworte

- sichere Passworte verwenden - nicht „password“
- Für jede Stelle ein einzigartiges Passwort verwenden
- Wenn jemand Zugriff auf ihr Mail-Konto hat, dann kann er auch Passworte wiederherstellen
- Einmal-Konten verwenden
- Passwort-Manager verwenden

5. Rechtevergabe

- nicht mit Administrator-Rechten arbeiten
- nicht zu viel Rechte
- nicht zu wenig Rechte

- Wer hat Zugriff auf welche Systeme/Funktionen?
- Ist geregelt, wer was darf, können muss?
- nicht benötigte Software deinstallieren/deaktivieren
- Wer kennt das Administrator-Passwort?
- Wer kennt das Passwort eines Kollegen? Urlaubsvertretung?
- Was passiert, wenn der einzige Mitarbeiter, der das Passwort kennt, nicht mehr da ist?

6. Firewall

○ … ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.

○ Hardware-Firewall am Internet-Zugang
○ Software-Firewall auf dem PC/Laptop
○ **Mindestens eine davon**
○ professionell eingerichtet … und gewartet

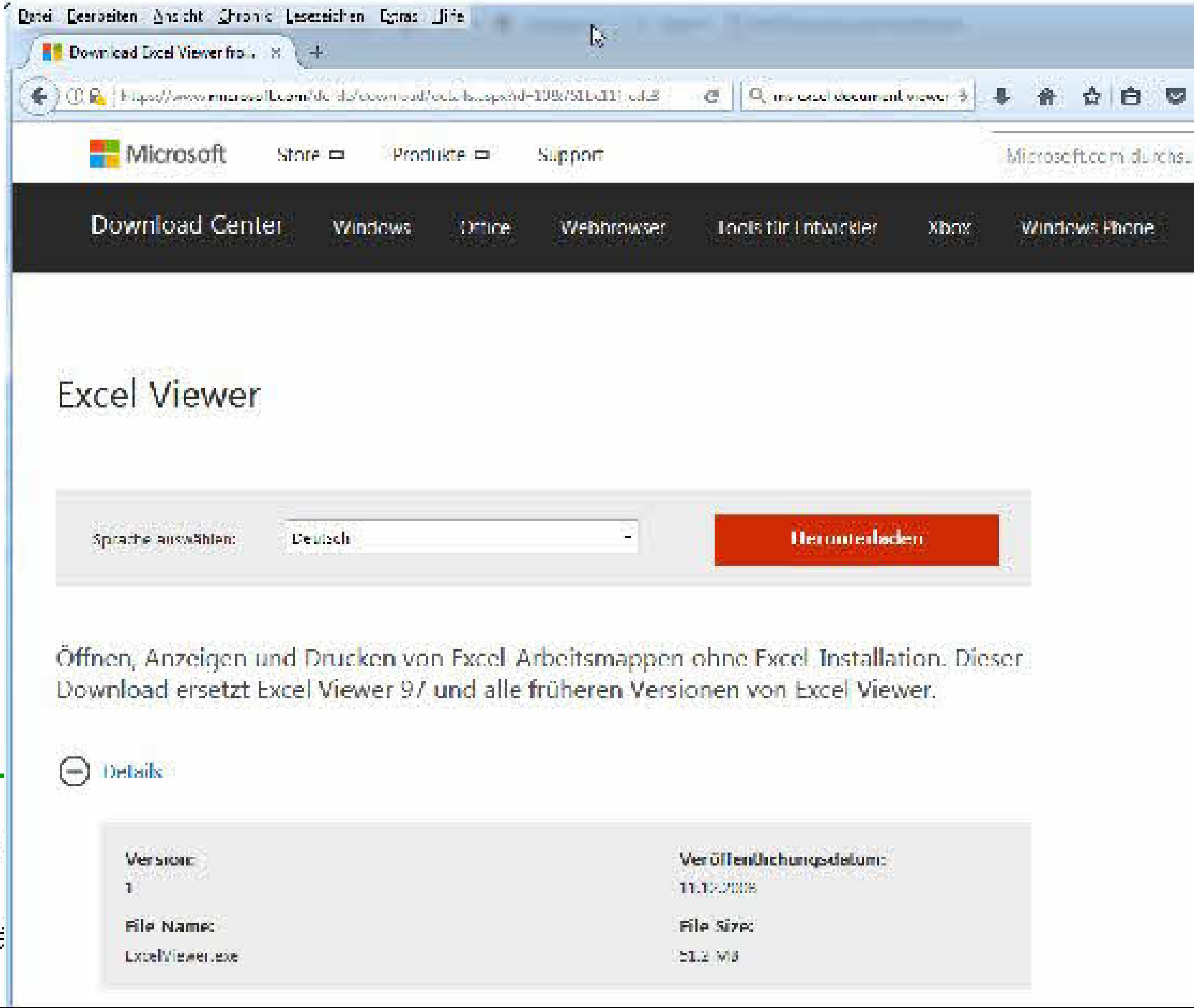
7. Schutz vor Malware

- Empfehlung: externer Virenscanner für eMail (beim Provider)
- Ein lokaler Virenscanner mit aktuellen Patterns
- zwei Virenscanner kämpfen gegeneinander und stören den Anwender und sich gegenseitig

- Wenn Sie unsicher sind, ob sich Schadsoftware auf ihrem Rechner befindet:
  http://housecall.trendmicro.com/de/
  https://www.eset.com/us/home/online-scanner/

8. Sicherheits-Einstellungen in Programmen

- Sicherheitseinstellungen in Programmen
  - Anzeige statt Ausführen von MS Office-Dokumenten
  - Browser-Sicherheitseinstellungen
  - Email-Programm (Javascript deaktivieren)



Excel Viewer

Sprache auswählen: Deutsch

Öffnen, Anzeigen und Drucken von Excel Arbeitsmappen ohne Excel Installation. Dieser Download ersetzt Excel Viewer 97 und alle früheren Versionen von Excel Viewer.

Version:
1

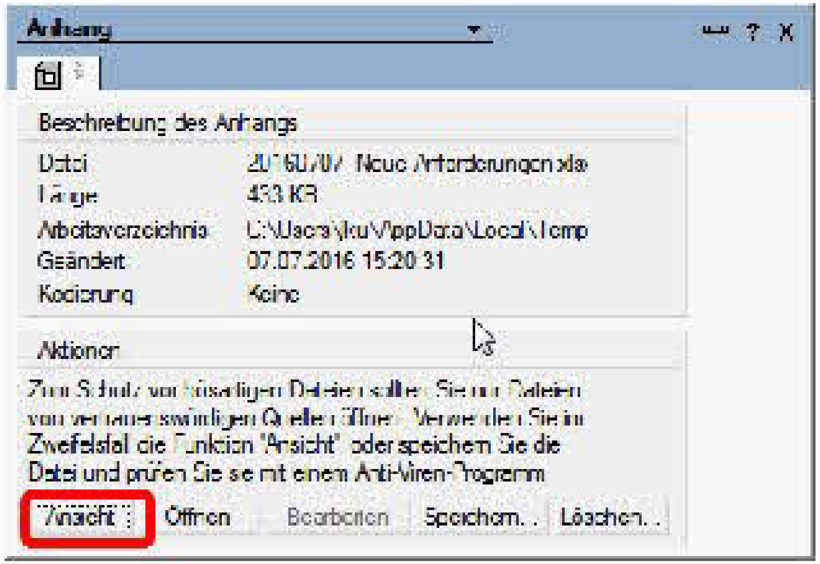
Veröffentlichungsdatum:
11.12.2008

File Name:
ExcelViewer.exe

File Size:
51.2 MB

8. Sicherheits-Einstellungen in Programmen

- Sicherheitseinstellungen in Programmen
  - Anzeige statt Ausführen von MS Office-Dokumenten
  - Browser-Sicherheitseinstellungen
  - Email-Programm (Javascript deaktivieren)



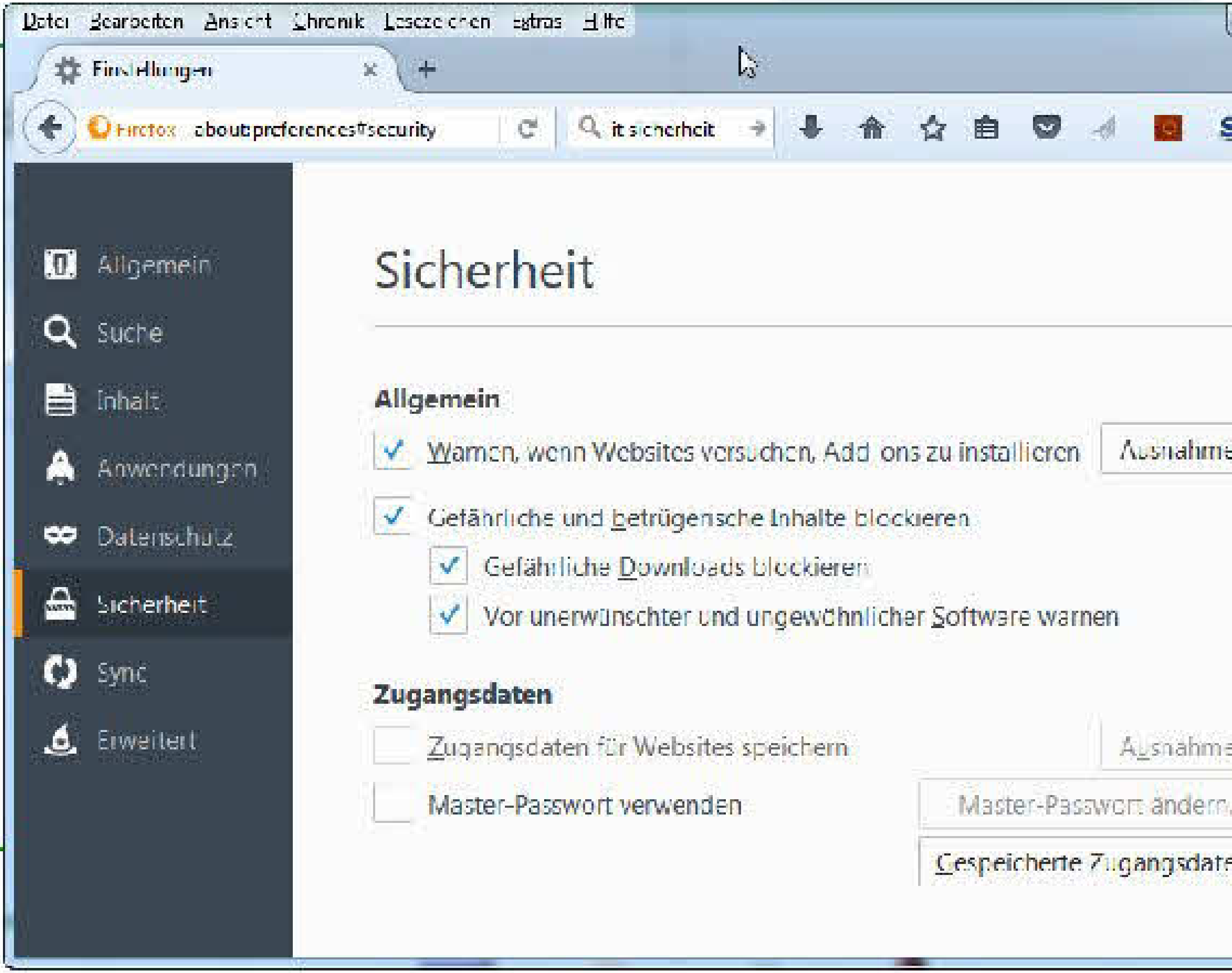
Beschreibung des Anhangs

Datei: 20160707 Neue Anforderungen.xls
Länge: 433 KB
Arbeitsverzeichnis: C:\Users\jku\AppData\Local\Temp
Geändert: 07.07.2016 15:20:31
Kodierung: Keine

Zum Schutz vor bösartigen Dateien sollten Sie nur Dateien von vertrauenswürdigen Quellen öffnen. Verwenden Sie im Zweifelsfall die Funktion 'Ansicht' oder speichern Sie die Datei und prüfen Sie sie mit einem Anti-Viren-Programm

8. Sicherheits-Einstellungen in Programmen

- Sicherheitseinstellungen in Programmen
  - Anzeige statt Ausführen von MS Office-Dokumenten
  - Browser-Sicherheitseinstellungen
  - Email-Programm (Javascript deaktivieren)



Sicherheit

Allgemein

☑ Warnen, wenn Websites versuchen, Add-ons zu installieren

☑ Gefährliche und betrügerische Inhalte blockieren

☑ Gefährliche Downloads blockieren

☑ Vor unerwünschter und ungewöhnlicher Software warnen

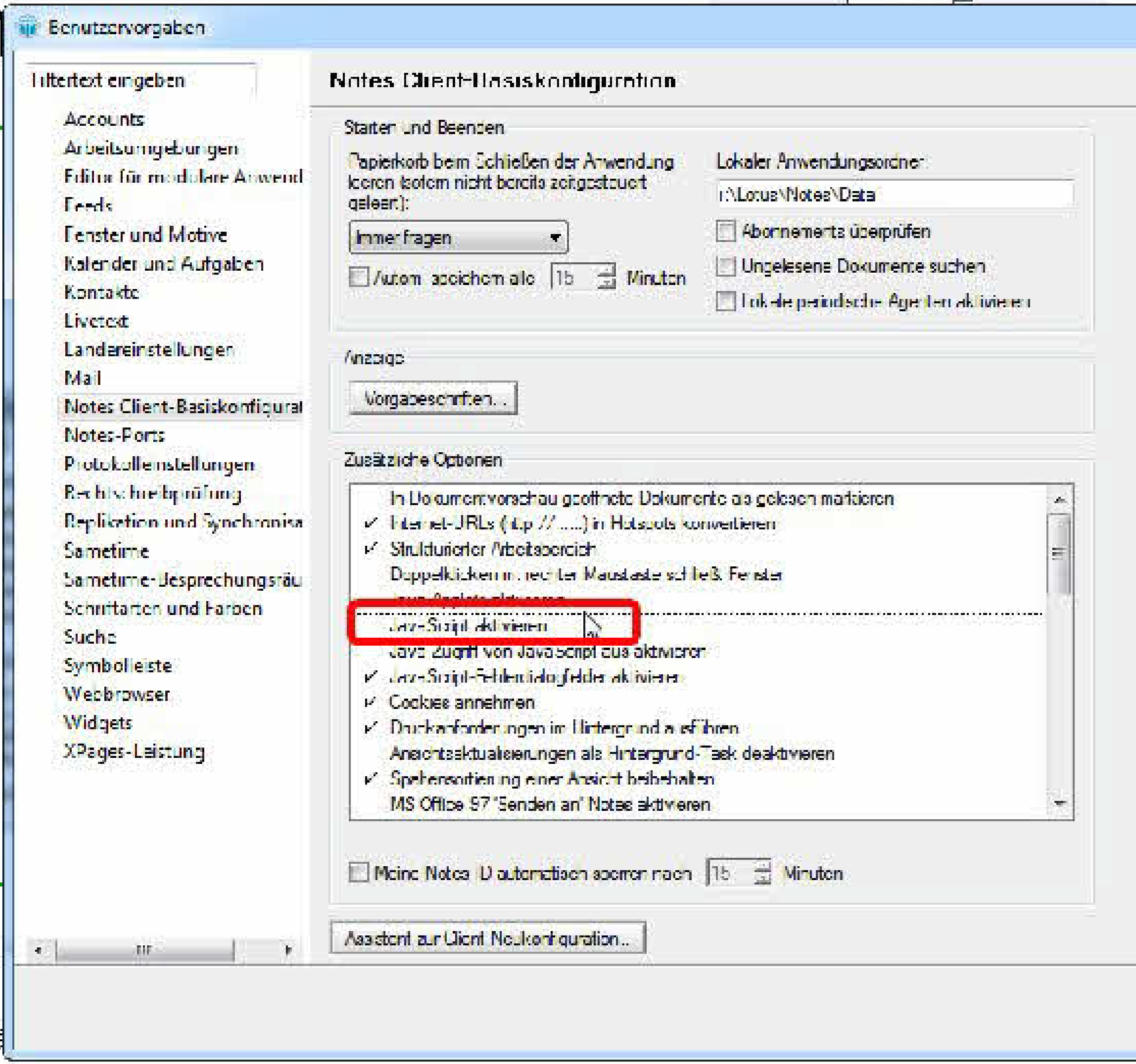
Zugangsdaten

☐ Zugangsdaten für Websites speichern

☐ Master-Passwort verwenden

8. Sicherheits-Einstellungen in Programmen

- Sicherheitseinstellungen in Programmen
  - Anzeige statt Ausführen von MS Office-Dokumenten
  - Browser-Sicherheitseinstellungen
  - Email-Programm (Javascript deaktivieren)



Notes Client-Basiskonfiguration

Starten und Beenden

Papierkorb beim Schließen der Anwendung leeren (sofern nicht bereits zeitgesteuert geleert): Immer fragen

☐ Autom. speichern alle 15 Minuten

Lokaler Anwendungsordner: :\Lotus\Notes\Data

☐ Abonnements überprüfen

☐ Ungelesene Dokumente suchen

☐ Lokale periodische Agenten aktivieren

Anzeige

Zusätzliche Optionen

- In Dokumentvorschau geöffnete Dokumente als gelesen markieren
- ✓ Internet-URLs (http://.....) in Hotspots konvertieren
- ✓ Strukturierter Arbeitsbereich
- Doppelklicken mit rechter Maustaste schließt Fenster
- Java-Applets aktivieren
- Java-Script aktivieren
- Java-Zugriff von JavaScript aus aktivieren
- ✓ Java-Script-Fehlerdialogfelder aktivieren
- ✓ Cookies annehmen
- ✓ Druckanforderungen im Hintergrund ausführen
- Ansichtsaktualisierungen als Hintergrund-Task deaktivieren
- ✓ Spaltensortierung einer Ansicht beibehalten
- MS Office 97 "Senden an" Notes aktivieren

☐ Meine Notes-ID automatisch sperren nach 15 Minuten

9. Verschlüsselung

- Transportverschlüsselung
- Inhaltsverschlüsselung

- Verlorenes Smartphone, verlorener Laptop
- Metadaten – mit wem kommunizieren Sie
- Browser: https
- eMail
- Kommunikation zwischen ihrem Server und ihrem Smartphone/Laptop, wenn Sie unterwegs sind

10. Externe Geräte

- Stecken Sie nicht einfach irgendwelche CDs, USB-Sticks oder Festplatten in ihren Rechner, wenn Sie nicht wissen, wo diese herkommen

- Sichern Sie ihr WLAN, so dass sich nicht „jeder“ dort einwählen kann

Zusammenfassung: 10 Schritte

1. Machen Sie es einfach
2. Sensibilisierung – Seien Sie wachsam
3. Erstellen Sie einen Katastrophenplan
4. Kümmern Sie sich um Updates
5. Verwenden Sie sichere Passworte
6. Klären Sie Verantwortlichkeiten und Rechte
7. Benutzen Sie eine Firewall
8. Benutzen Sie Anti-Malware-Programme
9. Konfigurieren Sie ihre Anwendungen sicher
10. Verschlüsseln Sie
11. Seien Sie vorsichtig mit externen Geräten

Zur Vertiefung: Links 1

- Online-Sicherheitscheck:
  https://www.itsicherheit-online.com/news/online-sicherheitscheck
- Der Heise Verlag Security Consulter:
  https://www.heise.de/security/dienste/Der-heise-Security-Consulter-2126442.html
  https://www.heise.de/security/dienste/Netzwerkcheck-2114.html
- Online-Virenscanner:
  http://housecall.trendmicro.com/de/
  https://www.eset.com/us/home/online-scanner/
- Tipps für ein sicheres Passwort:
  http://www.computerwoche.de/a/die-besten-tricks-fuer-ein-sicheres-passwort,3329874?tap=b28622df41dd36065e45ac10cd10d28a&utm_source=Nachrichten%20mittags&utm_medium=email&utm_campaign=newsletter&r=7666341201779818&lid=641011&pm_ln=70

Zur Vertiefung: Links 2

- Backup-Ratgeber:
  http://www.computerwoche.de/a/der-grosse-backup-ratgeber,2491258
- Bundesamt für Sicherheit in der IT (BSI) - Entwicklung eines Datensicherungskonzepts:
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06033.html?nn=6604926
- Cyber-Security für kleine und mittlere Unternehmen:
  https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf
- Beispielangebot für ein Backup-Konzept:
  https://forum.selfhtml.org/self/2012/jul/17/datensicherungskonzept-fuer-kmu/1552951
- Das Privacy-Handbuch:
  https://www.privacy-handbuch.de/print.htm
- Was man mit ihren Daten machen kann:
  https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Ist ihre IT sicher (genug)?

Vielen Dank für Ihre Aufmerksamkeit

Was ist wichtig?

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

Quelle: https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

Beispiel-Angebot

Erstellung eines Datensicherungskonzepts

Phase 1: Ist-Zustand erfassen, ca. 1 Beratertag
- Aufnahme des Ist-Zustands relevanter Hard-/Software und Daten
- IT-Fachmann für 1 Tag beim Kunden

=> Ergebnis: Überblick über die vorhandene Datenstruktur, die derzeit gesichert wird

Phase 2: individuelles Datensicherungskonzept erstellen, ca. 3 Beratertage
- Daten klassifizieren
- Datenvolumen ermitteln
- Zeitpunkt und Intervall für Datensicherung bestimmen
- Dauer für Rekonstruktion ermitteln
- Medien für Datensicherung auswählen
- Aufbewahrungsorte der Medien auswählen
- Aufbewahrungsfristen definieren
- Verantwortlichkeit für die Datensicherung bestimmen
- Verantwortlichkeit für die Prüfung der Datensicherung festlegen

=> Ergebnis: Kunde kann eine effektive Datensicherung konfigurieren und durchführen

Phase 3: jährliche Soll-Ist-Überprüfung, ca. 1 Beratertag
- überprüfen des in Phase 2 erstellten Datensicherungskonzepts
- festlegen erforderlicher Änderungen und Maßnahmen

⇒Ergebnis: Kunde kann seine Datensicherung an aktuelle Anforderungen anpassen/