Bildungsakademie Mittweida e.V.

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Computerkurs

Computersicherheit II

21.02.2017

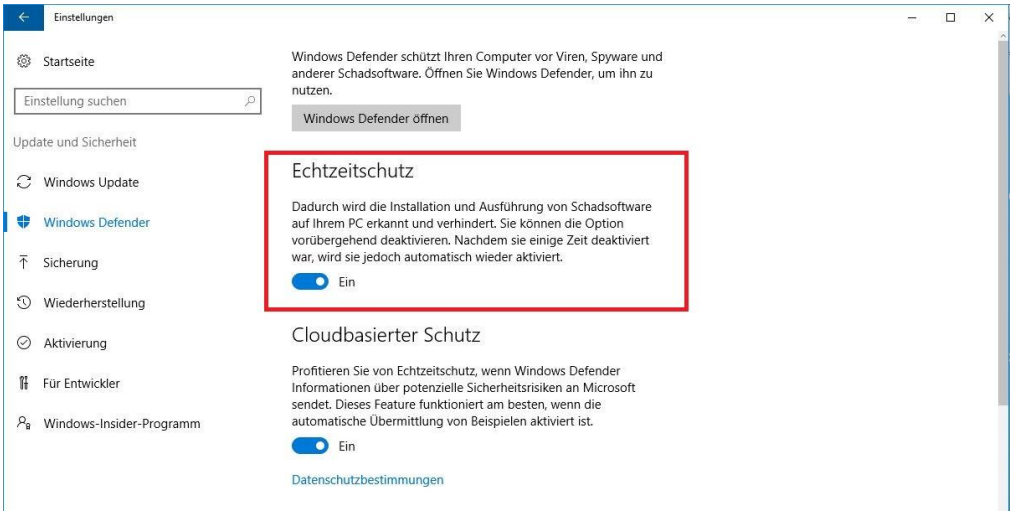
Inhalt:

- Windows Defender Aktivieren
- Kaspersky Virus Removal Tool und Kaspersky Rescue Disk 10
- Phishing E-Mails erkennen
- Daten verschlüsseln

Windows Defender Aktivieren:

Unter Windows 10:

1. Wählen Sie die Schaltfläche Start und dann Einstellungen > Update und Sicherheit aus.
2. Wählen Sie Windows Defender aus und aktivieren oder deaktivieren Sie den Echtzeitschutz.



Unter Windows Vista und Windows 7:

- Sofern kein anderer Virenschutz vorhanden, sollte der Windows Defender unter Windows 7 bereits aktiviert sein.
- Um den Defender zu einem vollwertigen Virenschutz aufzuwerten, muss aber noch Microsoft Security Essentials installiert werden
- Die Downloadlinks lauten wie folgt:
    - Für 64Bit Systeme:
        - https://download.microsoft.com/download/0/2/C/02C8AB73-0774-4975-826F-9E8A0FD7F65D/DEDE/amd64/MSEInstall.exe
    - Für 32Bit Systeme:
        - https://download.microsoft.com/download/0/2/C/02C8AB73-0774-4975-826F-9E8A0FD7F65D/DEDE/x86/MSEInstall.exe

Autor: Daniel Meerwald

Kaspersky Virus Removal Tool:

- Das Kaspersky Virus Removal Tool (KVRT) ist ein ziemlich mächtiges Tool um gezielt Schadware von ihrem System zu durchsuchen auf dem Standard eines der führenden Unternehmen in Sachen Virenschutz.
    - Vorteil: Das Tool ist kostenfrei und immer top Aktuell
    - Nachteil: Das Tool ist nur ein Tool und kein Antivirensystem. Es muss von Ihnen gestartet werden und durchsucht darauf hin den von Ihnen definierten Speicher nach Schadsoftware.
- Einsatzgebiete:
    - Kleinere Suchläufe auf Verdacht, Durchsuchen von fremden USB-Sticks, Checken einzelner Dateien denen Sie nicht vertrauen

Kaspersky Rescue Disk 10:

- Kaspersky Rescue Disk 10 (KRD10) ist ein sogenanntes **Live-System** das ihren gesamten Computer nach Schadsoftware durchsucht und dabei Windows nicht startet. Das gibt dem Virus deutlich weniger Chancen, dem „Desinfizieren“ zu entgehen. Die erfolgsrate von KRD10 ist deutlich höher als von jedem Virensystem das auf Windows arbeitet.
    - Vorteil: Höchste Säuberungsrate
    - Nachteil: Relativ langsam, Benötigt Neustart des Systems
- Einsatzgebiete:
    - Zum kompletten Desinfizieren eines Systems nach Virenbefall, ins besondere wenn der Virenscanner den Virus wiederholt nicht vollständig entfernen konnte

Für die Schritt für Schritt Anleitungen für Kaspersky’s Rescue Disk 10 und das Virus Removal Tool, schauen Sie bitte in die Folien vom 21.02.2017 Computersicherheit II ab Seite 7, da es sehr viele Bilder sind eignet sich dies nicht für die Printversion der Zusammenfassung.

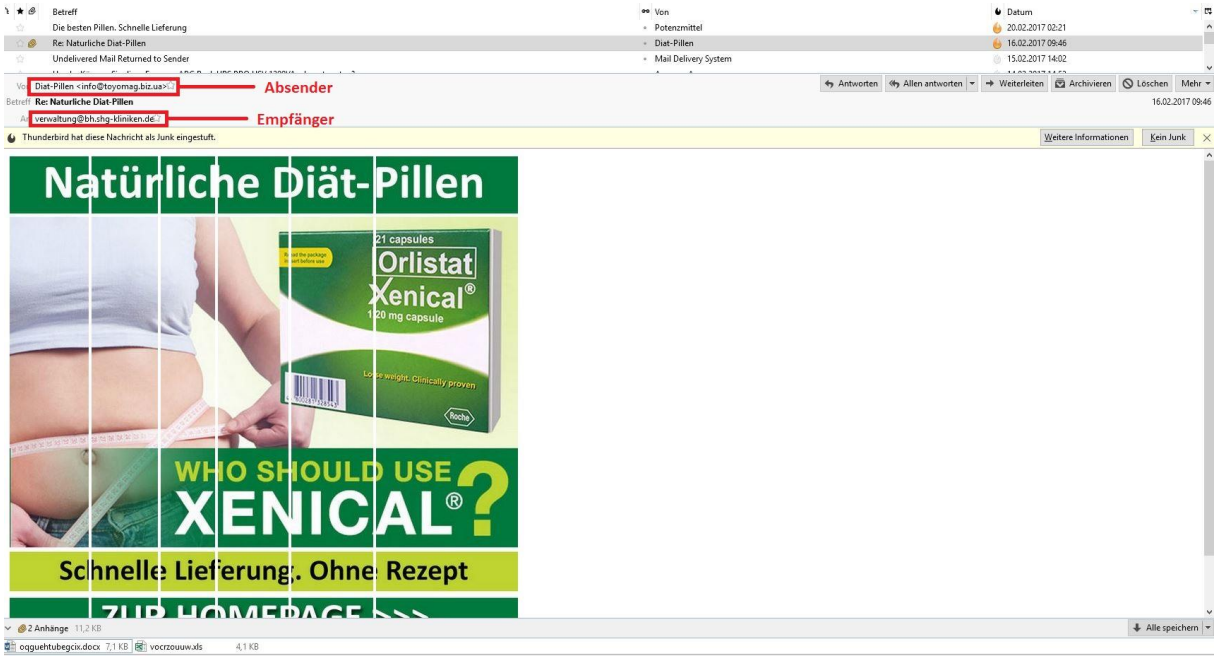
Phishing E-Mails erkennen:

- **Wikipedia definiert:** Unter dem Begriff **Phishing** (Neologismus von *fishing*, engl. für ‚Angeln‘) versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.
- Die Angebote in Phishing-Emails sind also nie wirkliche Angebote. Es soll an Ihre Daten gekommen werden und am besten auch noch Geld von Ihnen gezahlt werden, aber die Waren würde nie ankommen.

- Hier wird damit gelockt, das man Viagra Rezeptfrei kaufen kann. Dies ist natürlich nicht möglich, weshalb viele die Chance wittern hier doch ohne ein Rezept an besagtes mittel zu kommen und gehen damit dem Angreifer in die Falle. Alle Angebote die nicht „normal“ sind oder sich in Grauzonen befinden oder zu gut klingen um wahr zu sein sind meist Phishing Emails

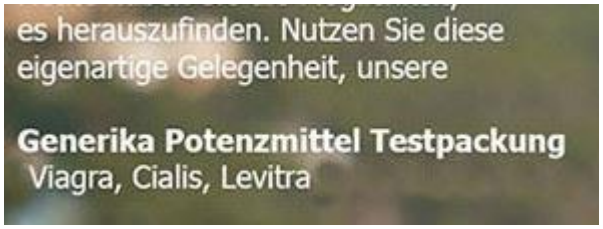
Autor: Daniel Meerwald

- In unserem Nächsten Beispiel achten wir einmal auf Absender und Empfänger.



- Unser Email Programm versucht auf einfache Weise über Schlüsselwörter oder Ähnliches für uns diese Betrügerischen Mails zu sortieren. In diesem Fall hat es Recht und die Mail als „Junk“ (dt. Müll) eingestuft. Ab und an werden aber auch vertrauenswürdige Mails als „Junk“ eingestuft.
- Wie wir sehen können ist der Absender eine Kryptische Email Adresse, die wir nicht zuordnen können. Interessanter Weise ist der eigentliche Empfänger ebenfalls eine Seltsame E-Mail nämlich: verwaltung@bh.shg-kliniken.de
- Beides deutet auf einen Betrugsversuch hin. Die Mail wurde offenbar auf Masse produziert und an verwaltung@bh.shg-kliniken.de geschickt. Diese haben die Mail dann zu uns weitergeleitet. Betrugsemails können aber genauso gut an Sie direkt adressiert sein.
- Am besten überprüfen Sie also ob die Absende-Email seltsam ist. **Phishing Mails haben meist Kryptische oder seltsam klingende Absender. ^**
- Des Weiteren ist der Inhalt solcher Mails meist dubios, Sie sollen ja mit einem Angebot gelockt werden, das Sie nirgendwo anders bekommen können.
- Ein weiterer Hinweis sind Anhänge mit Kryptischen Namen oder angehängte Dokumente ohne sinnvollen Verweis aus der Email auf den Anhang.

- Zuletzt sind solche Mails meist von nicht-Muttersprachlern verfasst und schlecht übersetzt oder enthalten viele Rechtschreibfehler.



Autor: Daniel Meerwald

Dateien Verschlüsseln:

- Das verschlüsseln von Dateien kann viele Gründe haben. Nicht nur Kriminelle verschlüsseln Ihre Dateien weil sie Illegale Inhalte enthalten.
- Jedem steht das Recht zu seine Dateien zu verschlüsseln und so vor dem unbefugten Zugriff anderer zu schützen. So wie das Türschloss in Ihrem Haus.
- Verschlüsseln kann viele Gründe haben:
    - Verwahren von Wichtigen Dokumenten wie: Urkunden, Verträge, Zugangsdaten
    - Schützen von Persönlichen Daten wie: Urlaubsbilder, Geistiges Eigentum
    - Schutz ihrer Arbeit wie: Das Buch an dem grade geschrieben wird, unfertige Kunst, etc.
- Beim Verschlüsseln von Daten werden diese mit einem Schlüsselwort, dem Passwort, vermischt umso eine unkenntliche Datei zu erhalten, welche sich nur mit besagtem Passwort wieder so lesen lässt, wie sie ursprünglich war. Für das Erstellen eines Sicheren Passwortes, verweise ich auf PC-Kurs 3 vom 14.02.2017 mit dem Titel Computersicherheit.
- Viele Systeme bieten mehr oder minder gute/sichere Möglichkeiten um schnell und einfach ihre Daten vor dem flüchtigen Zugriff anderer zu schützen.
- Für geübte Eindringlinge sind diese Methoden doch meistens kein Hindernis und es ist bekannt, dass Behörden wie der BND oder das FBI sich Hintertüren in vielen solcher Programme erkaufen.
- Deshalb stelle ich ihnen hier ein Programm vor das getestet wurde und „Quelloffen“ ist. Damit ist garantiert, das die Verschlüsselung selbst keine Lücken enthält und das Programm in keiner Weise eine Hintertür eingebaut hat.

Dateien Verschlüsseln mit Truecrypt:

- Truecrypt ist ein Tool, das uns eine Art verschlüsselten Ordner erstellen lässt, in dem wir nach Eingabe des Passwortes, wie bei einem USB-Stick, darauf zugreifen können und Dateien hinzufügen, entfernen oder verändern können.
- Dabei muss die Größe dieses „virtuellen Sticks“ vorher festgelegt werden und ist hinterher nicht mehr zu verändern.
- Truecrypt lässt uns darüber hinaus auch echt, physische Laufwerke, wie einen USB-Stick, vollständig verschlüsseln.
- Zum Benutzen der Dateien muss immer eine Version von Truecrypt gestartet werden um besagte Verschlüsselungen zu öffnen.
- Truecrypt kommt in Fest installierbaren Versionen und mit einer Portablen Version, die nicht installiert werden muss.
- Nachdem das FBI wiederholt die entwickler von Truecrypt unter druck gesetzt hat, haben diese die Weiterentwicklung beendet, da ihr Programm auf dem heutigen stand der Technik nicht zu knacken ist. Deshalb müssen wir uns einer anderen Downloadseite bedienen.
- Link:
    - https://www.heise.de/download/product/truecrypt-25104

Für eine detaillierte Schritt für Schritt Anleitung bitte in die Folien vom 21.02.2017 Computersicherheit II schauen. Ab Seite 24. Da es sehr viele Bilder sind, passt es nicht zur Printversion.