Dieser Vortrag versucht auf die häufigsten und für den privaten Anwender gefährlichsten Problemen im Umgang mit dem Computer, Internet und E-Mail-Verkehr aufmerksam zu machen und Lösungsvorschläge anzubieten.

Der Vortrag bezieht sich auf Desktopcomputer und Laptops.

Obwohl die hier angesprochenen Gefahren auch im Umgang mit Smartphones und Tablets bestehen und auch mit den hier genannten Maßnahmen verhindert werden können, sind gerade die Probleme mit der Hardware und der Software (Apps) noch vielfältiger und verlangen eine etwas detailliertere Betrachtungsweise

In diesem Vortrag werden die Themen

- Hardware incl. Betriebssysteme, Software
- Internet
- E-Mail
- Wie kann ich mich schützen

angesprochen.

Vorweg

100% Sicherheit gibt es nicht.
Weder durch Verschlüsselung, was verschlüsselt wurde, kann wieder entschlüsselt werden. Es ist nur eine Frage der Zeit und des Aufwandes.
Noch durch Einsatz von Antivirenprogrammen und anderen Sicherheitsprogrammen.

Kostenlos gibt es nicht, wenn es kein Geld kosten, dann eure Daten.

Das größte Problem ist der User, also ihr. Und zwar durch Unwissenheit, Neugier, Hektik und Leichtsinn.

Hardware incl. Betriebssysteme, Software (ohne zusätzlichen Schutz)

Hier muss man Hardwaremäßig unterscheiden zwischen Apple-Systemen und Windows/Linux-Systemen.

<u>Apple:</u>
Hardware und Betriebssystem werden in einem Haus entwickelt. Es gibt wenige Rechnermodelle. Außerdem gibt es diese Rechner in nur wenigen unterschiedlichen Konfigurationen. Zudem ist es dem Nutzer nicht möglich den Rechner aufzurüsten, also zusätzliche oder geänderte Hardware wie Grafikkarten einzubauen.
Dadurch kann man sagen das die Anfälligkeit des Gesamtsystem relativ gering ist.

<u>Windows/Linux:</u>
Beide Betriebssysteme werden auf Rechnern eingesetzt, die von anderen Firmen hergestellt werden. Dies ergibt eine sehr große Anzahl von Gerätetypen mit fast unübersichtlichen Konfigurationsmöglichkeiten. Das verlangt vom Betriebssystem sehr viele Konfigurationen zumindest mit Standardeinstellungen abzudecken.
Hinzu kommt, das bei diesen Rechnertypen der Benutzer Erweiterungen vornehmen kann, die nicht mit den Standardtreiber abzudecken sind. Die entsprechenden Treiber müssen dann von den Hardwareherstellern gesondert geladen und installiert werden.

Diese Kombination aus Möglichkeiten erhöht das Risiko, dass irgendwo im System und im Zusammenspiel der ganzen Komponenten Lücken entstehen, durch die der Rechner angreifbar wird.
Bei den beiden Betriebssystemen gibt es aber ein Unterschied. Während bei Windows ein Team von Entwicklern bei Microsoft sitzt und am System arbeitet , ist Linux ein offenes System ist, an dem viele Fachleute, Spezialisten und erfahrene Amateure auf der ganzen Welt mitarbeiten, das System testen und helfen es zu verbessern.

<u>Resümee</u>
Wenn man nur von der Hardware und dem Betriebssystem ausgeht ist Windows das gefährdetste von allen Dreien.
Linux und Apple sind relativ sicher, wobei Experten sich nicht ganz einig sind. manche sehe Linux als das sicherste System, manche Apple. Es gibt sogar Aussagen, dass für Privatanwender die Linux oder Apple benutzen kein extra Schutz nötig ist. Das ist meiner Meinung nach unrichtig und sollte nicht beachtet werden.

Internet

Problem

1. durch “Tracking“ Aufzeichnung/Verfolgung der eigenen Web-Adresse durch Suchmaschinen oder die Anbieter von Diensten um möglichst viel über das Verhalten der Nutzer zu erfahren.
2. Gefälschte Adressen, die in den Suchmaschinen auftauchen (z.B. Anazon.de statt Amazon.de) um an persönliche Daten, Passwörter etc zu kommen. Siehe auch Pishing.

Maßnahmen

1. Sichere Browser benutzen, z. B. Mozilla Firefox. Einstellungen kontrollieren ob Tracking Filter eingeschaltet sind (können bei vielen Browsern als so genanntes Add On heruntergeladen werden). Browser so einstellen, dass Cookies und Verlauf beim schließen automatisch gelöscht werden.
2. Sichere Suchmaschinen verwenden. Google zeichnet alles auf, wer dann noch Google Mail und andere Anwendungen von Google benutzt kann sicher sein, dass seine Daten gut verknüpft für personalisierte Werbung und mehr verwendet wird. Sicher sind zum Beispiel “Startpage.com“ oder “DuckDuckgo.com“
3. Immer die gewünschte Adresse kontrollieren, ob alles richtig ist. Nie auf Verknüpfung in E-Mail klicken, sondern Adresse per Hand in den Browser eingeben oder aus den eigenen gespeicherten Lesezeichen.

E-Mail

Über die E-Mail kann für den Nutzer der meiste Schaden entstehen. Hier eine Liste der häufigsten Gefahren (Überbegriff ist meist Viren)

- SPAM unerwünschte Werbung, kann aber auch viele der nachfolgend genannten Schadsoftware enthalten.
- PISHING Versuch durch gefälschte Aufmachung einer Mail an persönliche Daten und Passwörter zu kommen. Wie “ wir müssen Ihre Daten überprüfen, klicken sie bitte auf den Link“. Siehe Beispiel
- RANSOMWARE kleines Programm im Anhang der Mail, verschlüsselt die Festplatte. Der Code zur Entschlüsselung wird erst nach Zahlung eines Geldbetrages zugesandt, angeblich.
- MALWARE kleine Programme die unterschiedliche Gefahren darstellen, zum Beispiel können sie Eingaben am Computer überwachen und so persönliche Daten abfangen. Sie können bestimmte Funktionen lahmlegen etc.
- ROOTKITS (auch Bootkits) sind eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem System installiert wird, um zukünftige Logins des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.

Wieso soll PayPal eine GMX E-Mail Adresse verwenden

Walter Urban

Von: Support <mailversand-2130@gmx.de>
Gesendet: Freitag, 3. Mai 2019 16:57
An: post@w-urban.de
Betreff: Wichtige Mitteilung Referenzcode: 335173

Sehr geehrter Herr Walter Urban,

damit wir weiterhin konform mit den Gesetzen bleiben, welche durch das Parlament der Europäischen Union ins Leben gerufen wurden, arbeiten wir stets an unserem System des Kundendatenschutzes und der Betrugsbekämpfung.
Um weiterhin die Industriestandards an Nutzersicherheit einhalten zu können, werden wir unser ganzes System zeitnah generalüberholen. Bevor wir dies durchführen, müssen wir sicherstellen, dass die Daten, welche sich bereits in unseren Datenbanken befinden, der Wahrheit entsprechen.
Bitte folgen Sie der untenstehenden Schaltfläche in Ihr Kundeportal, in welchem Sie Ihre Eingaben auf ihre Richtigkeit überprüfen können. Falls Sie diesen Vorgang nicht durchführen, müssen wir Ihr Konto vorsorglich deaktivieren.

Konto bestätigen

Mit freundlichen Grüßen,
Ihr PayPal Kundendienst

An diese E-mail-Adresse können keine Antworten gesendet werden, da sie nur zum Versand von Nachrichten eingerichtet ist.

s

Mit dieser Servicemitteilung informieren wir Sie über wichtige Änderungen bezüglich Ihres Paypal Kundenkontos.
Copyright © 1998-2019 Paypal.com. Alle Rechte vorbehalten.

1

Walter Urban

Von: Support <mailversand-2130@gmx.de>
Gesendet: Freitag, 3. Mai 2019 16:57
An: post@w-urban.de
Betreff: Wichtige Mitteilung Referenzcode: 335173

Koernigeren, zuecktest Nervensaegerei.Abtrieb, takelnde umformend offizielleren.
logo<https://cdn.merchantmaverick.com/wp-content/uploads/2013/03/Paypal-Logo-2015-300x86.png>

Sehr geehrter Herr Walter Urban,

Chlorophyll, talgigen, meistertet, U-Booten.

damit wir weiterhin konform mit den Gesetzen bleiben, welche durch das Parlament der Europäischen Union ins Leben gerufen wurden, arbeiten wir stets an unserem System des Kundendatenschutzes und der Betrugsbekämpfung.

Um weiterhin die Industriestandards an Nutzersicherheit einhalten zu können, werden wir unser ganzes System zeitnah generalüberholen. Bevor wir dies durchführen, müssen wir sicherstellen, dass die Daten, welche sich bereits in unseren Datenbanken befinden, der Wahrheit entsprechen.

Bitte folgen Sie der untenstehenden Schaltfläche in Ihr Kundeportal, in welchem Sie Ihre Eingaben auf ihre Richtigkeit überprüfen können. Falls Sie diesen Vorgang nicht durchführen, müssen wir Ihr Konto vorsorglich deaktivieren.

Herausfindende weggeschlossen, gehobeneren. Konto bestätigen <http://bit.ly/2ValimN>

Mit freundlichen Grüßen,

Ihr PayPal Kundendienst

An diese E-mail-Adresse können keine Antworten gesendet werden, da sie nur zum Versand von Nachrichten eingerichtet ist.

s
Notwendiger Rassendiskriminierung.Analogem, Aufhebungsbeschluss.Ehering Segelschulschiff, Nobelkneipen Regionalisierungen, Tonbandprotokolle.

Mit dieser Servicemitteilung informieren wir Sie über wichtige Änderungen bezüglich Ihres Paypal Kundenkontos.
Copyright © 1998-2019 Paypal.com. Alle Rechte vorbehalten.

Steuerpflichtigem rasiert Sowie, Verhalten,.
Fangen charakteristische, beschattet.
Lieferpapiere bekundest.

Kurz-URL oder Shortlink: Zweifelhaft bis gefährlich, da die eigentliche Webadresse verborgen wird, also nicht bekannt ist. Normal müsste hier ein Link zu PayPal stehen, also http://www.paypal.com/de.

Länderkennung ly = Top Level[1] Domain Libyen, sehr zweifelhaft

Ihre Mithilfe ist erforderlich

Amazon.de <04wf47382nd8ndc@marketplace.amazon.de>

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Gesendet: Sa 04.05.2019 11:45

An: post

amazon

Sie haben eine Nachricht erhalten.

Nachricht:

Guten Tag,

da wir für. Sie tägli.ch die Sic.herheitsst.andards er.weitern

un.d dran arb.eiten Ihne.n einen si.cheren

Ein.kauf mit Amazon zu e.rmöglichen., haben wi.r auch nun.

wieder fü.r Sie ein .neues Upda.te entwick.elt..

Mit dem ne.uen Update. sind Sie .gegen Angr.iffe dritt.er

Persone.n besser g.esichert u.nd geben d.en Betrüge.rn

somit w.eniger Mög.lichkeiten. Ihre Date.n zu erlan.gen..

Um das neu.e Update b.ei Ihnen w.irksam zu .machen müs.sen

Sie Ih.re Daten m.it unseren. neuen Sic.herheitssy.stem verkn.üpfen.

Log.gen Sie si.ch dazu Bi.tte in Ihr.em Konto u.nter folge.ndem Link .ein.

Weiter zu Amazon.de

Wir freuen uns auf Ihren nächsten Besuch bei Amazon.de!

Amazon.de

Beste Grüße

Walter Urban

Von: Amazon.de <04wf47382nd8ndc@marketplace.amazon.de>
Gesendet: Samstag, 4. Mai 2019 11:45
An: post
Betreff: Ihre Mithilfe ist erforderlich

<http://g-ecx.images-amazon.com/images/G/01/tmtdefaulttemplate/img/logo-selling_coach.png>
Sie haben eine Nachricht erhalten.

Nachricht:

<https://mailing.dhl.de/assets/bm/binary/7/9/4/1/794169b1eedae786054dff04ad6d7fed_115499.jpg?mobile=1>
Guten Tag,

da wir fürLpp Sie tägliSb2ch die SiczXoherheitsstBRtandards er1wLweitern

unnA8d dran arbZXReiten Ihne1Uwn einen siZJXcheren

EinYqLkauf mit Ajcbmazon zu eJ5mrmöglichenMEj, haben wiafar auch nunDgH

wieder füpEir Sie ein xDfneues UpdapFate entwickWETelt.TCk

Mit dem neFWwuen UpdateQFB sind Sie csggegen AngrwCviffe drittHgMer

PersonepFrn besser gHd4esichert uXCKnd geben d7zoen Betrüge1s1rn

somit wl7Xeniger MögSXDlichkeitenua5 Ihre DateKHIn zu erlangoYgen.3OD

Um das neuuvQe Update bzttei Ihnen wjA2irksam zu IBvmachen müsJXDsen

Sie IhHQBre Daten mklLit unserenq6s neuen Sic9nRherheitssy7qFstem verknLVbüpfen.

LogCvEgen Sie si6Pfch dazu Bi9yRtte in IhrEhPem Konto uhZFnter folgeSk0ndem Link EK6ein.

Weiter zu Amazon.de <http://u.tlht.us/5n>

Wir freuen uns auf Ihren nächsten Besuch bei Amazon.de!
Amazon.de

<https://mailing.dhl.de/assets/bm/binary/2/8/c/c/28ccd9d58a664edef05f544c0a1f9df0_30129.jpg?mobile=1>

<https://mailing.dhl.de/op/4/383XFPRE-2DENCMYO-160CU69.gif> <https://sellercentral-europe.amazon.com/nms/img/fe379f79-25c0-3470-80fc-73a4d846b18c?sk=yuUNz7x0X5Sb0IYEyPTTNbr_Pmf70_bDKaTT1U5j_e9eLQT_x0R-Oi9VfKR7bPsbteXgkbmft5XpwggUciJfbw&n=1>

Amazon Services Europe S.à r.l.
5 Rue Plaetis
L-2338 Luxembourg
Handelsregisternummer Luxemburg: B-93815
Gesellschaftskapital 12.500 EUR
Gewerbelizenznummer: 100416
USt.-Identifikationsnummer Luxemburg: LU 19647148

Wichtiger Hinweis: Wenn Sie dieser E-Mail antworten, wird Amazon.de Ihre E-Mail-Adresse mit einer von Amazon bereitgestellten Adresse ersetzen, um Ihre Identität zu schützen, und die Nachricht in Ihrem Namen weiterleiten. Um einen möglichen Betrug zu verhindern, setzt Amazon.de Filtertechniken ein. Nachrichten, die diesen Filter nicht passieren, werden nicht weitergeleitet. Amazon.de behält Kopien aller über diesen Service gesendeten und empfangenen E-Mails, einschließlich der Nachricht, die Sie hier eingeben. Amazon.de wird diese Kopien insbesondere zur Klärung von eingereichten A-bis-z-Garantie-Anträgen heranziehen. Indem Sie diesen Dienst nutzen, erklären Sie sich mit diesem Vorgehen einverstanden.

Wir möchten, dass Sie stets mit Vertrauen einkaufen, wenn Sie Produkte auf Amazon.de erwerben. Hier finden Sie nähere Informationen über sichere Online-Einkäufe (http://www.amazon.de/gp/help/customer/display.html?nodeId=13023711) und unsere Garantie für den sicheren Einkauf (http://www.amazon.de/gp/help/customer/display.html?nodeId=886414).
[commMgrTok:A061468111SCC6DEG5CN5]

Wie voriges Beispiel Short Link, diesmal USA mit wahrscheinlicher Weiterleitung.

Alle anderen Links scheinen in Ordnung zu sein, falls der Empfänger sie versehentlich anklickt, was eigentlich nicht vom Sender geplant ist. Ihr sollt auf “weiter zu Amazon klicken“

Taktisch sehr clever!

Wie kann ich mich schützen

Neben den bereits im Teil Internet / Browser genannten Maßnahmen ist folgendes zwingend.

1. Ein gutes Antiviren / Internetschutzprogramm. Diese gibt es auch als kostenlose Downloadversionen. Kostenpflichtige Versionen geben zum Teil einen zusätzlichen Schutz z.B. beim Onlinebanking, Echtzeitschutz, Rootkits usw. Informationen über Leistungen und Qualität der Programme kann man unter folgenden Adressen erfahren:
   - www.heise.de (Computerzeitung c`t)
   - www.bsi-fuer-buerger.de (Bundesamt für Sicherheit in der Informationstechnik, viele Informationen)
   - www.test.de (Stiftung Warentest)

   Nach meinen Information bietet auch der in Win10 enthaltene Defender mittlerweile einen guten bis sehr guten Schutz.

2. Betriebssystem und Programme immer aktuell halten, dass heißt Updates immer installieren.

3. Regelmäßige Sicherheitskopien der eigenen Dateien auf einer externen Festplatte .

4. Eventuell einmal ein komplettes Backup des gesamten Systems oder eine Rettungsdisk für Windows.
   Pkt. 3 und 4 helfen wenn der Rechner gekapert und verschlüsselt wurde um das System neu aufzusetzen und Datenverlust zu vermeiden.
5. Nie aus einer E-Mail heraus einen Link anklicken, auch wenn er vertrauenswürdig aussieht. Immer in den Browser gehen und die Adresse selbst eingeben, oder aus den eigenen Lesezeichen.
6. Spam oder Mails von Unbekannten nie öffnen, sondern löschen oder in den Spamordner verschieben.
7. Banken oder seriöse Unternehmen werden nie nach irgendwelchen Daten fragen. Wenn ihr Zweifel habt, geht in den Browser ruft die Seite auf und prüft eure Daten. Meist gibt es dort einen Hinweis ob Daten unklar sind oder fehlen. Gefälschte Internet Auftritte von Banken etc. sind mittlerweile sehr gut gemacht, nicht wie im Beispiel weiter vorne. Also Vorsicht.
8. Wenn der Rechner langsamer wird, lasst die Antivirensoftware das gesamte System prüfen. Es könnte ein Hinweis auf ein Rootkit oder Bootkit sein. Beliebt sind zur Zeit Cryptomining (fremde Rechner werden zusammengeschlossen um die fremde Rechnerleistung zur Erzeugung von Cryptowährung zu benutzen). Oder das so erzeugt Rechnernetz zum versenden von Spam Mails zu mißbrauchen.

Zum Schluss noch ein Wort zur Social Media

Ihr könnt sicher sein, dass bei Benutzung von Facebook und Co alle eure Daten gesammelt, verknüpft, aufbereitet und auch verkauft werden.
Das ist das erklärte Geschäftsmodel von z.B. Facebook. Trotz Beteuerungen von Marc Zuckerberg, dass man sich bemüht Datensicherheit und für den Nutzer Klarheit über die benutzten Daten zu schaffen, hat sich nichts geändert. Es ist eher schlechter geworden.
Leider ist auch WhatsApp davon betroffen, welche seit einigen Jahren zu Facebook gehören. Die Nachrichten sind zwar weiter verschlüsselt, die persönlichen Daten werden aber an Facebook weitergereicht.

Andere Social Media Plattformen dürften ähnlich durchlässig sein, da das Geschäftsmodel nicht anders funktionieren kann, kostenlos, aber irgendwo muss das Geld ja herkommen. Also Werbung und vielleicht auch der Verkauf von Daten.

Also Vorsicht, nur die Daten eingeben die minimal nötig sind um teilnehmen zu können und alles was möglich ist sperren. Dann nach und nach die Features öffnen die man wirklich braucht.

DAS WICHTIGSTE

NICHTS IST SO WICHTIG, EILIG ODER DRÄNGEND, DASS IHR INNERHALB VON MINUTEN DARAUF REAGIEREN MÜSST.

WENN ES WIRKLICH WICHTIG WAR MELDET SICH DER ABSENDER NOCHMAL.

WENN ES EIN SUPERTOLLES ANGEBOT IST (VON WEM AUCH IMMER) GEHT ÜBER DEN BROWSER, ES GIBT DAS ANGEBOT IN EINER ODER ZWEI STUNDEN IMMER NOCH, WENN NICHT WAR ES WAHRSCHEINLICH EIN LOCKMITTEL.

ALSO

INFORMIERT EUCH, LASST EUCH ZEIT UND DENKT NACH!!!!!

DANN SOLLTE NICHT SCHIEFGEHEN (HOFFENTLICH) UND NUN VIEL SPASS