Technische Universität Braunschweig

Gauß-IT-Zentrum

Die 4x4 verbreitesten IT-Sicherheits-Irrtümer

Dr. Christian Böttger, 20.10.2016

Fallen Sie auf Mythen herein?

- IT-Sicherheit kann man nicht in der Packung kaufen – man muss etwas dafür tun.

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die häufigsten Irrtümer zusammen gestellt – die Basis auch für uns.
- Sicherheitstipps nachzulesen unter
  - https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec

- 4 Bereiche – und jeweils 4 Irrtümer

- Wer schon alles wusste – Hut ab, gut informiert!

Bereich 1: Surfen im Internet

Ist alles so schön bunt hier! (Nina Hagen, 1978)

Irrtum 1: meine Firewall schützt mich vor allem!

Schön wäre es ja, aber: leider nein!

Punkt 1: die **Konfiguration der Firewall**

Wenn Sie jede Anfrage eines Programms für Zugriff auf das Internet freigeben – dann haben Sie bald viele Löcher. Und: kennen Sie sich wirklich so gut aus?

Punkt 2: **Firewalls blocken nur ganz direkte Angriffe (IP-Ebene)**

Es gibt natürlich *auch Angriffe über legitime Kanäle* – ihr Browser und Ihr Mailprogramm müssen ins Internet können, da hilft Ihnen auch die Firewall nichts.

Und damit sind Sie „bösen“ Mails und Webseiten ausgeliefert.
Das können Sie nicht mit einer Firewall blocken – außer, Sie nehmen die Schere. Dann brauchen Sie allerdings auch kein Internet mehr.

Irrtum 2: mein Virenschutz ist aktuell – das reicht aus!

Ganz so einfach ist das Leben leider nicht!

Natürlich ist ein **aktuell gehaltenes Virenschutzprogramm(*)** wichtig für die Sicherheit.
Dazu muss auch die Virensignaturdatenbank **täglich** aktualisiert werden. Aber ein Virenprogramm kann nur nach bekannten Schädlingen suchen, **jagt** also die **Angreifer**.

Die **Aktualisierung der „normalen“ Softwarepakete** dagegen **beseitigt** die möglichen **Angriffsflächen**, da die Hersteller in ihren Updates und Patches ja ihnen bekannte Lücken schließen, ggf. auch bevor Schädlinge „auf dem Markt“ sind.

Das ist wie beim Autofahren: nur weil Sie sich anschnallen, fahren Sie ja nicht unvorsichtig – oder anders herum. Beide Maßnahmen sind nötig.

Angehörige der TU: https://doku.rz.tu-bs.de/doku.php?id=software:sophos

Irrtum 3: ein komplexes Passwort für alles ist genug!

Passwörter sind nicht der Highlander!

Natürlich sollte ein Paßwort „sicher“, also schwer zu „knacken“ sein – Paßwort-Richtlinien an der TU Braunschweig: https://rzotrs.rz.tu-bs.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=795

Aber auch ein „starkes“ Paßwort kann verloren gehen, ausgespäht werden oder eben doch „geknackt“ werden. Und wenn man dann nur eins hat, dann sind gleich alle Dienste und Webseiten für den Angreifer offen.

Also: **für jeden Zweck ein eigenes Passwort**!

Passwortsicherheit: siehe Vortrag von Sebastian Homann

Irrtum 4: ich bin vorsichtig beim Surfen – mir passiert nichts!

Leider können Sie nicht alles erkennen!

Natürlich minimiert **überlegtes Surfverhalten** das Cyber-Risiko drastisch – aber leider können **auch vertrauenswürdige Seiten** ab und an **selbst infiziert** sein oder **gehackt** worden sein – beispielsweise über **Werbebanner**, **unsichtbare (Statistik-)Zähler** und ähnliches.

Und mit Techniken wie **Cross-Site-Scripting** und **Drive-by-Infection** brauchen Sie gar nicht mehr auf einen verdächtigen Link zu klicken – sie merken gar nicht, dass Ihr Rechner infiziert wurde. Und Sie können es auch gar nicht bemerken, egal wie vorsichtig Sie sind!

Und mal Hand auf‘s Herz: wer war noch nie **unaufmerksam** oder **zu neugierig**?

Es hilft nichts – Sie müssen sich aktiv schützen, mit Firewalls, Virenschutz, guten Passwörtern, Sicherheitsupdates – und natürlich mit Vorsicht.

Bereich 2: E-Mail (Un-)Sicherheit

Spam, Spam, Spam, lovely Spam (Monty Python, 1970)

Irrtum 1: Anhang bleibt zu – Gefahr gebannt!

Das trifft nur für reine Text-Mails zu!

Heute soll aber ja alles schön bunt und farbig sein, zumindest **hübsch formatiert**, und es sollen ja auch **Bilder** (z.B. das Firmenlogo) mitgeschickt werden.

Das geht nur mit **HTML-Mails** – und das bedeutet,
dass Sie **eigentlich keine Mail öffnen, sondern sich eine Webseite ansehen**, auch wenn es im Mailprogramm geschieht – da ist nämlich ein kleiner Browser eingebaut.
Also gelten auch alle Gefahren des Surfens im Internet: im HTML-Quellcode können alle möglichen Schadprogramme und gefährliche Links eingebettet sein.

Das einzige was dagegen hilft, ist die **Anzeige der Mail auf „Nur-Text-Modus**“ einzustellen und **nur bei vertrauenswürdigen Absendern** dann im Einzelfall in die **HTML-Ansicht** zu wechseln.

Irrtum 2: Immer schön den Link zum Austragen (Verteiler) nutzen!

Tun Sie das bloß nicht!

Ganz im Gegenteil: *Spam-Mails sollten sie umgehend, und am besten ohne sie überhaupt zu öffnen, löschen* – oder Ihrem Provider über den dafür bereit gestellten Knopf/Ordner als Spam melden.

Natürlich werden Sie *nicht* aus dem Verteiler gelöscht werden, wenn Sie den Link zum Löschen aus dem Verteiler anklicken:

ganz im Gegenteil, durch den Klick weiß der Spammer, dass diese E-Mail Adresse gültig ist und das Spam-Aufkommen wird noch weiter ansteigen.

Irrtum 3: die Absenderangabe einer Mail ist zuverlässig!

Nein! Sowohl der *angezeigte Absendername* als auch die *angebliche Absenderadresse* lassen sich sehr leicht fälschen.

Spammer und Phisher tun das auch!

Fahren Sie mit der Maus über den angezeigten Absendernamen – Ihr Mailprogramm sollte Ihnen dann die **technische Absenderadresse** anzeigen.

Wenn diese nicht mit dem Namen übereinstimmt, ist Vorsicht geboten.

Genauer geht es mit der Anzeige der Details: die „Received:“-Zeilen verraten den Trickser.

Vergleichen Sie auch den Betreff mit dem angeblichen Absender: passt das inhaltlich zusammen?

Deshalb im Zweifel: ungeöffnet löschen!

- und ggf nachfragen – **Ruf doch mal an!**

Irrtum 4: auf Phishing-Mails falle ich doch nicht rein!

Hochmut kommt vor dem Fall!

Phisher und Spammer werden immer besser in Gestaltung und Inhalt Ihrer Mails.

Ziel von Phishing-Mails ist es, Ihnen **Zugangsdaten und Passwörter** zu Online-Banking oder Shops oder auch Kreditkartendaten zu entlocken. Dafür werden Sie auf **gefälschte Webseiten** gelockt, die den echten Seiten täuschend echt sehen – bis auf die in solchen Fällen **immer falsche Webseitenadresse** (URL). Auch die **Mails sind täuschend echt** aufgemacht und fordern Sie z.B. zu einer Sicherheitsüberprüfung auf oder informieren Sie über eine angebliche Sperrung Ihres Kontos.

Folgen Sie auf keinen Fall den Links in solchen Mails!

Im Zweifel rufen Sie Ihre Bankseite/Seite des Shops direkt auf durch manuelle Eingabe des Ihnen bekannten Links und prüfen Sie, ob da etwas zu tun ist.

Training:
https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/nophish/

Bereich 3: Mobile Geräte

Das Böse ist immer und überall! (EAV, 1985)

Irrtum 1: In der Cloud sind meine Daten sicher – macht nix, wenn das Handy weg ist!

Das ist nur die eine Seite der Medaille.

Seriöse Anbieter sorgen zwar für die (**technische) „Sicherheit**“ Ihrer Daten – allerdings nutzen einige sie trotzdem für eigene Zwecke, beispielsweise Werbung.

Außerdem unterliegen ausländische Anbieter de facto nicht dem deutschen Recht. In den USA beispielsweise sind nur die die Daten von US-Bürgern wirklich gesetzlich geschützt, und auch das nach ganz anderen Grundsätzen als in der EU.

Als *Angehöriger der TU Braunschweig nutzen Sie bitte den vom GITZ bereit gestellten Cloud-Speicher* (Dienstleistungskatalog Position 3104).

Die Daten sind außerdem **nur so sicher wie der Weg** dorthin: wenn Ihr mobiles Gerät sich in einem **offenen WLAN** bewegt oder **gestohlen** wird und dazu nur von einem **einfachen** PIN oder **Sperrmuster** geschützt ist, sind Ihre Daten auch schnell dem Dieb ausgeliefert.

Auch **Schadsoftware** kann Ihr Gerät befallen – und dann auch auf Ihre Daten zugreifen.

Irrtum 2: Öffentliche WLANS: praktisch und kostenlos!

… nur leider nicht sicher …

Viele öffentliche, kostenlose WLANs sind **unverschlüsselt**, d.h. Ihre Daten werden zwischen Ihrem Mobilgerät und dem WLAN Access Point offen übertragen und **können abgefangen oder verändert werden**.

Auch können Sie sich schnell Schadsoftware einfangen.

Achten Sie darauf, dass **auch kostenfreie WLANs mindestens WPA2 verschlüsselt** sind, oder übertragen Sie in offenen WLANs grundsätzlich nur bereits auf Ihrem Gerät verschlüsselte Daten bzw. übertragen alle Daten über ein **VPN.**

Als Angehöriger der TU nutzen Sie am besten „eduroam“ wo immer es geht.

https://doku.rz.tu-bs.de/doku.php?id=netz:wlan

https://rzotrs.rz.tu-bs.de/otrs/public.pl?Action=PublicFAQSearch&Subaction=Search&Submit=yes&Keyword=WLAN

Irrtum 3: eine neu gekauftes Smartphone ist sicher!

Nur, wenn es kein Ladenhüter war …

Sie wissen ja nicht, wie lange das Gerät schon beim Händler liegt und wie viele Sicherheitsupdates zwischen Produktion und Kauf schon heraus gekommen sind.

- **Sie sollten also grundsätzlich sofort nach dem Kauf die Firmware und alle Apps und sonstigen Updates für das Gerät einspielen, zusätzlich auch einen – meist nicht mitgelieferten – Viren/Malware-Scanner installieren.**
- **Überprüfen Sie außerdem die Sicherheitseinstellungen.**
- **Falls möglich, aktivieren Sie die Geräteverschlüsselung.**
- **Zerstören Sie die alte SIM-Karte (falls Sie eine neue bekommen haben) und löschen Sie alle Daten auf dem Vorgängergerät.**

Irrtum 4: automatische Aktualisierung = sicher!

Natürlich sind automatische Updates sinnvoll.

Aber nicht alle Hersteller und Programmierer kümmern sich um Sicherheitslücken.

Außerdem werden **manchmal nicht für alle Geräte oder Betriebssystemvarianten auch Updates bereit gestellt**, oder teilweise mit erheblicher **Verzögerung**.

Informieren Sie sich daher über Schwachstellen und **schalten Sie** ggf. **betroffene Funktionen ab**.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Newsletter/Newsletter_node.html

Bereich 4: Computer / PC-Sicherheit

My home is my castle (engl. Maxime, Sir Edward Coke (1552-1634))

Irrtum 1: Eine Infektion meines Rechner merke ich sofort!

So einfach ist es leider nicht.

Nicht jeder Schädling macht sich auch bemerkbar.

Es gibt **verschiedenste Arten von Schadsoftware**. Wenn das **Ziel** des Angriffs z.B. der Identitätsdiebstahl (Ihre Nutzerkennungen + Passwörter), die Fernsteuerung Ihres Rechners für weitere Angriffe (Ihr Rechner wird Teil einer Distributed Denial of Service-Attacke (DDoS) oder eines Botnetzes) oder das massenhafte Versenden von SPAM ist, dann wird der Angreifer natürlich alles tun, damit sie den **Angriff bzw. die Infektion eben nicht bemerken** – und **das gelingt auch**.

Eine 100%ige Sicherheit vor Infektionen gibt es nicht!

Wenn Sie aber Ihre **Virensoftware aktuell halten** und **auch alle anderen Softwarepakete auf dem neuesten Stand halten**, **vorsichtig sind beim Anklicken von Links** und dem Öffnen von E-Mails und **Software nur von bekannten, vertrauenswürdigen Quellen** herunter laden, sind sie zwar nicht 100% sicher, aber schon ein ganzes Stück weiter.

Irrtum 2: Ich habe doch nicht zu verbergen – ich bin kein Ziel!

Sind Sie sich da ganz sicher? Wirklich?

Gilt das auch für Ihre Zugangsdaten zum **Online-Banking**, zur **Krankenkasse**, zu Online-**Shops** und für Ihre **Kreditkartendaten** oder an der Uni Ihre **Prüfungsergebnisse** oder gar Ihre **Krankengeschichte**?

Jeder, der sich online bewegt, online einkauft, kostenpflichtige Dienste nutzt, **ist ein potentielles Angriffsziel**.

Selbst wenn Sie nicht direkt vom Angreifer geschädigt werden – es existiert ein **schwunghafter illegaler Handel mit persönlichen Daten**.

Darüber hinaus können Sie auch schnell Opfer von Ransom-Ware werden – Ihre Festplatte wird verschlüsselt und Sie müssen Lösegeld für Ihre eigenen Daten zahlen – sofern Sie kein aktuelles Backup haben. Außerdem kann ein schlecht geschütztes Gerät z.B. als Teil eines Botnets wiederum als Sprungbrett für Angriffe auf andere Ziele werden.

Irrtum 3: Backup? Quatsch – Cloud-Speicher ist einfacher!

Natürlich sind **Cloudspeicher praktisch** und bieten – bei seriösen Anbietern – auch einen **hohen Sicherheitsstandard**. Aber: **Sicherheitskopien sind KEIN Backup** …

Der **Zugriff erfolgt aber naturgemäß immer über das Internet**. Wenn es *technische Probleme* gibt, der *Anbieter seinen Dienst einstellt* oder *pleite geht* oder auch nur Ihre *Internetverbindung gestört* ist – laufen Sie Gefahr, **gar nicht mehr an Ihre Daten heran zu kommen**. Denken Sie auch daran, dass außereuropäische Anbieter nicht unter das europäische oder gar deutsche Datenschutzgesetz fallen. Dienstliche Daten dürfen Sie dort nicht speichern (Datenschutzgesetz, Auftragsdatenverarbeitung).

Als **Angehöriger der TU Braunschweig** nutzen Sie bitte den **vom GITZ bereit gestellten Cloud-Speicher** (Dienstleistungskatalog Position 3104) (PowerFolder mit 100 GB).

Sofern der **Cloudspeicher als Netzwerklaufwerk** in Ihren Rechner eingebunden ist, können Ihre Daten dort ebenfalls Opfer von Ransom-Ware werden.

Um ein **Backup oder zumindest Sicherungskopien** auf einem **getrennten Speicher** kommen Sie also nicht herum. Das **GITZ bietet für Institute und Einrichtungen** der TU Braunschweig einen **Backup- und Archiv-Service** an (Dienstleistungskatalog Position 3103).

Irrtum 4: Papierkorb geleert – Daten gelöscht!

Das ist schlicht falsch.

Beim **Löschen** und anschließend **Leeren des Papierkorbs** bleiben die **Daten vollständig erhalten**, lediglich die Verweise im „Inhaltsverzeichnis“ werden gelöscht.

Es gibt einfach zu beschaffende Tools, mit denen man solche Daten leicht wieder herstellen kann, solange Sie nicht überschrieben wurden.

Das **gezielte Überschreiben** der Daten ist die einzige sichere Methode, die Daten wirklich zu löschen, wenn Sie beispielsweise Ihren Rechner inkl. Festplatte verkaufen wollen – außer der **physischen Zerstörung des Datenträgers** natürlich. Hinweise gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html

Achtung: Speicher auf Basis von *Flash-Technologie*, also z.B. *USB-Sticks* oder *SSD*-Festplatten, **lassen sich nicht sicher löschen, außer durch Zerstörung**!

Weitere Infos:
https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec
und beim IT-Service-Desk des Gauß-IT-Zentrums
Tel. +49.531.391.55555
it-service-desk@tu-braunschweig.de **https://www.tu-braunschweig.de/it/service-desk**

Vielen Dank für Ihre Aufmerksamkeit!