Wege zur Sicherheit (Stand: 13.5.2014)

Dieses Paper ist ein sehr knapper Text mit einigen Informationen und Verweisen zu Adressen für die vorgestellten Add-Ons, Programme etc. Sie müssen selbst aktiv werden. Sie müssen sich zu Informationsseiten wagen und lesen und zu Download-Adressen wagen und selbst herunterladen.

Die genannten Netz-Adressen sind dabei nicht als die einzig relevanten oder „guten" zu sehen, ebensowenig als Werbung für bestimmte Anbieter. Sie stellen eine durchaus individuelle Auswahl des Referenten dar (der ebensowenig wie jeder und jede andere *alles* Wichtige im Netz überblicken kann).

Das Paper bezieht sich auf allgemeine Internet- und Mail-Aktivitäten von PCs aus. Die vielfältigen Probleme, die sich aus der Nutzung z.B. von Social Media wie Facebook oder auf Smartphones ergeben können, bleiben hier – nicht zuletzt aus Zeitgründen – weitgehend außen vor. Doch können Sie z.B. bzgl. Smartphones einiges an Überlegungen entsprechend übertragen.

Als gewisse Provokation – und auch angesichts der kürzlichen schweren Sicherheits-Lücke des InternetExplorers von Microsoft – sind alle genannten Maßnahmen auf Firefox bezogen (lassen sich aber häufig auch entsprechend auf anderen Browsern anwenden).

Einstiegsstufen des Aktiv Werdens (Wohlgemerkt: bei bereits vorhandenem Antiviren-Programm!) und des allgemeinen Verhaltens

5Min – Das ist die „5-Minuten-Terrine" (Ok, sie wird ein paar Minuten länger brauchen!)

U1S – Das ist das „Ungefähr 1 Stunde-Programm".

IN KAPITÄLCHEN: allgemeine Verhaltensweisen, die Sie immer praktizieren sollten!

1. Identifizierung beim Surfen	
- wieistmeineip.de	Zeigt Ihnen Ihre aktuelle IP-Adresse an sowie weitere Informationen, die beim Surfen über Sie bekannt werden
- panopticklick.eff.org	Prüft den „Fingerabdruck" des Rechners, der trotz veränderter IP-Adresse, Löschen von Cookies etc. (siehe nächster Punkt) entsteht.
2. Anonym surfen	Google et al. erfahren von Ihnen mehr, als Sie denken – und filtern Ihre Suchergebnisse bezogen auf Ihre angeblichen Vorlieben.
- Drittanbieter-Cookies deaktivieren, Cookies nach Sitzung löschen **5Min**	Über Cookies (kleine auf Ihrem Gerät gespeicherte Textdateien von Seiten, die Sie aufgesucht haben) und weitere Techniken wird Ihr Surfweg auf einzelnen Seiten, aber auch über verschiedene Seiten hinweg verfolgt (unter tatkräftiger Mithilfe z.B. von Google-Diensten) – das läßt sich verhindern! Firefox → EINSTELLUNGEN → DATENSCHUTZ → CHRONIK: Firefox wird eine Chronik **nach benutzerdefinierten Einstellungen anlegen** → Cookies von Drittanbietern akzeptieren: **NIE** → Behalten, bis: **Firefox geschlossen wird** Zum Tracking siehe weiter unten bei Punkt 10 – Ghostery
- Tracking deaktivieren	
- **ADRESSEN, SO BEKANNT, DIREKT EINGEBEN**	oben in die Adreßzeile, nicht in die Zeile der Suchmaschine. Dann ist Google jedenfalls nicht mehr direkt beteiligt.
- **SUCHMASCHINEN-GLASHAUS EINTRÜBEN: ALTERNATIVE SUCHMASCHINEN BENUTZEN** **5Min**	z.B. mit ixquick.com (anonymisierte Google-Suche) oder duckduckgo.com (Mischung aus Suchergebnissen verschiedener Quellen, wie bei ixquick keine Speicherung von IP-Adressen und Nutzerdaten) Informative Vergleiche von DuckDuckGo mit Google (in Deutsch) sind unter diesen Adressen zu finden: *donttrack.us* und *dontbubble.us*
- über anonyme Server (also auf dem Weg Ihrer Surfanfragen zwischen-	Die Identifizierung Ihres Rechners über seine „IP-Adresse" wird verschleiert. So lange Sie den Anbietern der Anonymisierungs-Server vertrauen,

geschaltete Rechner) surfen	lassen sich Ihre Surf-Aktivitäten dann nicht bis zu Ihnen zurück verfolgen. Trotz aktueller Fraglichkeiten (z.B. bzgl. der Abschottung des TOR-Netzwerks gegen NSA etc.) ein wichtiger Schritt.
o z.B. mit TOR-Browser-Paket **U1S**	Dies ist ein fertig vorbereiteter Firefox, der auf das TOR-Netzwerk eingestellt ist. Sie müssen ihn nur – ggfs. zusätzlich zum „normalen" Firefox – installieren und benutzen. z.B. per chip.de
- hirnbrauser.de	verschiedene Tests, was Ihr Browser beim normalen Surfen so alles von sich preisgibt
3. Antiviren-Programme	unverzichtbarer Basisschutz
- kostenlos z.B.:	Beide Programme haben in kürzlichen (April 2014) Bewertungen nicht die besten Noten in der kostenlosen Version erhalten. In Kombination mit weiteren Sicherheits- und Vorsichts-Aktivitäten hält der Dozent sie aber dennoch für nützlich (und benutzt selbst Avast!).
o Avast	z.B. per chip.de
o Antivir Free Antivirus	z.B. per chip.de
- Sicherheits-DVD Desinfec't/Knoppicillin	umfassende PC-Reinigung DVD leider immer nur in bestimmten Ausgaben der Computerzeitschrift c't (zuletzt in Heft 10/2013)
4. Firewall **5MIN**	blockiert nicht genehmigte Netz-Aktivitäten, die von Ihrem Rechner ausgehen. Die mindestens sinnvolle Windows-Firewall sollte auf jeden Fall aktiv sein: START → SYSTEMSTEUERUNG → WINDOWS FIREWALL. Als Alternative das kostenlose Comodo, z.B. per chip.de. **ABER**: dann Win7-Firewall deaktivieren! Zwei Firewalls vertragen sich nicht gut!
- z.B. Comodo	
5. Rootkit-Schutz	Rootkits sind spezielle Schädinge, die sich so gut im System verstecken können, daß auch Antiviren-Software sie nicht immer findet. Gegen sie gibt es spezielle Programme.
- z.B. Sophos Virus Removal Tool	kostenloses Programm, das zusätzlich zum normalen Antivirenprogramm laufen kann z.B. per chip.de
6. Spionage-Schutz **U1S**	wichtige Ergänzung zu Antiviren-Programmen
- kostenlos z.B. SpyBot	z.B. per chip.de deutsche Anleitung z.B. per: www.netzwelt.de/news/66350-anleitung-spybot-sucht-zerstoert-schaedlinge.html
7. Eingeschränkte-Rechte	Fremdprogramme können sich nicht einnisten, wenn Sie fürs normale Surfen ein Normalkonto verwenden. WIN 7: START → SYSTEMSTEUERUNG → BENUTZERKONTEN
- Administrator ⇔ Normal-Konto **U1S**	
- Sandboxie bzw. auch die Firewall Comodo (siehe Punkt 4)	Sandboxie z.B. per chip.de Solche Programme erstellen einen „abgeschotteten Bereich" auf Ihrem Rechner, in dem dann Programme, gerade auch der Browser, sicher laufen, bzw. getestet werden können.
8. Privater Modus im Browser	Hat nur etwas zu besagen für die Dinge, die Sie direkt in Ihrem Browser speichern wie in der Chronik vermerkte Seiten, die temporären Internetdaten etc. Ihr Surfen selbst wird damit absolut nicht „privatisiert", also anonymisiert.
- z.B. in Firefox: STRG + UMSCH + P	
9. ZIELANZEIGE LINKS UNTEN IM BROWSER, BEI MAUS (OHNE KLICK!) AUF BELIEBIGEM LINK	Sie zeigt – meistens! – an, wohin Sie gelangen würden, wenn Sie jetzt klickten. Mißtrauen ist angesagt, wenn der Linktext und die Zielanzeige sich erheblich unterscheiden. (Dies gilt v.a. auch für Links in Mails – siehe dazu weiter unten!)
10. Sicherheits-AddOns (in FF)	sämtlich (außer HTTPS everywhere) per addons.mozilla.org
- Noscript **5Min**	blockiert von vornherein potentiell problematische Seiten-Elemente
- WOT **5Min**	warnt bei problematischen bis gefährlichen Seiten. Das wird bereits in den Suchergebnissen z.B. von Google oder Ixquick angezeigt.

- VirusTotal Scan Url **U1S**	prüft vor dem Anklicken Seiten auf Virusgefahr hin, indem diese Seite von verschiedenen online-Scannern geprüft wird
- HTTP**S** everywhere **U1S**	versucht wo immer möglich automatisch eine verschlüsselte SSL-Verbindung zu einer Seite herzustellen (nicht nur bei Banking etc.) z.B. per heise.de/download
- Flagfox **U1S**	zeigt tatsächlichen Standort und weitere Informationen des Servers einer Seite
- Ghostery **U1S**	blockiert insbesondere Verfolgungsmöglichkeiten Ihrer Aktivitäten (Tracking) im Netz
- AdBlock **U1S**	blockiert Werbung (Informieren Sie sich über Kritik am Konzept!), aber auch Tracking und entfernt z.B. „Like-Buttons“
- Lightbeam	zeigt Ihnen, mit welchen anderen Seiten Verbindungen der Seite, die Sie aktiv angesteuert haben, bestehen
11. Downloads	
- **NIEMALS DOWNLOAD DIREKT ÖFFNEN**	Immer zuerst auf dem Rechner abspeichern, damit Antiviren-Programm die Gelegenheit zur Prüfung bekommt.
- Dateinamenserweiterungen anzeigen **U1S**	Dann wissen Sie besser, was für eine Art von Dokument Sie wirklich als Mailanhang etc. bekommen haben. Im Windows-Explorer ab Win7: ORGANISIEREN → ORDNER- UND SUCHOPTIONEN → Register ANSICHT → Haken entfernen bei „Erweiterungen bei bekannten Dateitypen ausblenden“
12. Gefahren beim Mailen, daher die folgenden Aktivitäten	Die sogenannten HTML-Mails mit der Möglichkeit zu ausgiebiger Formatierung können Schadcode enthalten! Tricky ist auch, daß dann beim Öffnen der Mail unsichtbare Bildchen, sogenannte „Zählpixel“, aus dem Internet nachgeladen werden können: Sie verraten, daß Sie diese Mail geöffnet haben und mehr...
- ohne Vorschau arbeiten **5Min**	jedenfalls, sofern Sie Mails als HTML-Mails empfangen lassen. in Thunderbird: ANSICHT → FENSTERLAYOUT → Haken weg bei „Nachrichtenbereich“
- Umstellen Ansicht auf pure Text-Mails **U1S**	in Thunderbird im Prinzip voreingestellt! Individuelle Umstellmöglichkeiten per AddOn „Allow HTML Temp“ (EXTRAS → ADDONS → ADDONS DURCHSUCHEN)
- Versand von HTML-Mails und Text-Mails → auf letztere umstellen **U1S**	Thunderbird: EXTRAS → KONTENEINSTELLUNGEN → VERFASSEN UND ADRESSIEREN → Haken weg bei „Nachrichten im HTML-Format verfassen
- Links in Mails	
o **ZIELANZEIGE LINKS UNTEN AUCH IM MAILPROGRAMM**	Bei Maus auf Link (ohne zu klicken): Sie zeigt meistens an, wohin Sie gelangen würden, wenn Sie jetzt hier klickten.
o **PHISHING ERKENNEN UND ABWEHREN**	Phishing ist die Verlockung, durch einfaches Anklicken von Links zu vertraut wirkenden Seiten zu gelangen, auf denen Sie persönliche Angaben „verifizieren“ sollen! Seriöse Firmen verlangen das **NIE!**
- **MAIL-ANHÄNGE**	Grundsätzlich nie direkt öffnen, sondern auf PC speichern, sodaß Antivirenprogramm sie prüfen kann. Erwägen, ob Absender vertrauenswürdig ist – bzw. wirklich weiß, was sein PC „tut“! Lieber vor dem Öffnen nachhaken.
- Virenschutz für Mail-Programm	Wird häufig schon von Mail-Provider bereitgestellt. Ergänzende Programme möglich. z.B. auch als Teil von kommerziellen Antiviren-Programmen
13. PERSÖNLICHE ANGABEN BEIM ANMELDEN, EINKAUFEN ETC.	als Einstieg hierzu: www.kaufenmitverstand.de Prüfen Sie z.B. bei kostenlosen Programmen, ob nicht nur der Download, sondern auch die Benutzung wirklich kostenlos ist.
14. PAßWORT-SICHERHEIT	absolute Basics: mindestens 8 Zeichen, Mischung aus Buchstaben, Ziffern und Sonderzeichen, absolut keine Namen von Partnern, Haustieren und ähnlich vertrauten „Objekten“

	am besten keine Paßwörter auf PC speichern → Papier!!! Sehr guter aktueller Artikel bei der *taz* (taz.de) – dort mit Suchphrase „*Sichere und merkbare Passwörter*“ zu finden
15. Banking	ein aktueller Artikel z.B. in „PcGo 06/2014“ absolute Basics: niemals von Mail-Link aus zur Bank-Website wechseln, immer auf „http**s**“ in Adreßzeile plus Schloßsymbol achten (SSL-Verschlüsselung)
16. Mail-Verschlüsselung	
- z.B. enigmail für Thunderbird	Asymmetrische Verschlüsselung. Das Programm erstellt einen öffentlichen Schlüssel, mit dem Personen, die Mails an Sie verschicken wollen, diese verschlüsseln können (gewissermaßen ein Vorhängeschloß für Ihre Mails, das Sie an die potentiellen Sender verteilen) sowie einen privaten Schlüssel, mit dem nur Sie diese Mails entschlüsseln und lesen können (gewissermaßen der einzig passende Schlüssel für Ihre verteilten Vorhängeschlösser).
17. Datenverschlüsselung allgemein	
- z.B. drag’n’crypt ultra	z.B. per pcwelt.de
18. PROGRAMMVORSICHT	
- Nur von erprobten Seiten downloaden	z.B. per chip.de
- Programme aktualisiert halten	
o Eigenaktualisierungen	automatisch oder mit Nachfrage (je nach Programm und Einstellung)
o Hilfsprogramme	Sie prüfen den Aktualitätsstand auch von vielen Programmen auf Ihrem PC, die das nicht selbst tun. Ein Beispiel: Secunia (z.B. per chip.de)
- Installationen notieren	Um ggfs. nachzuvollziehen, ab wann „seltsame Dinge“ begannen → Über die Systemwiederherstellung des Rechners läßt sich dann, wenn gewünscht, ein früherer Zustand des PCs vor der Installation zurückholen. START → SYSTEMSTEUERUNG → WIEDERHERSTELLUNG
19. RECHNERSÄUBERUNG ALLG.	
- z.B. mit Ccleaner	ein etabliertes kostenloses Programm für vielfältigen Einsatz z.B. per chip.de
20. weitere Spezialthemen	Hier müssen Sie selbst recherchieren.
- Keylogger	Programme, die Ihre Tastatureingaben auslesen können
- Beobachtung durch die eigene Web-Kamera	aktuell für alle, die eine Kamera in Ihrem PC haben!
o taz- und SPIEGELonline-Artikel	Verschiedene Artikel zum Thema finden Sie per Suchen mit ixquick und diesen Suchphrasen: *Baby-Kamera gehackt* / *Ich kann dich streamen* / *Cyber-Spanner beobachten Frauen heimlich per Webcam* / *Wie wichtig Computersicherheit auch im privaten Umfeld ist, zeigt ein aktueller Fall aus Kalifornien*
- unauffällige Filmkameras überall	Surfen Sie einmal zum Elektronik-Versand „Pearl“ (www.pearl.de) und suchen Sie dort nach „Octacam-Produkten“. Sie werden sich gruseln. Es gibt Kameras inzwischen schon in Kravatten eingebaut.

Allgemein seien empfohlen zur Weiterinformation

- die Webseiten von etablierten Computerzeitschriften wie „PC-Welt“, „CHIP“, „c’t“ und anderen. Dort finden sich häufig aktuelle, tendenziell leichter verständliche Informationen auch zu Sicherheitsfragen, Programmtips – und durchaus Kritik dazu in den Kommentaren von Nutzern.
- Der Dozent hat Ihnen für Downloads v.a. chip.de genannt, da er die hier vorhandenen Informationen zu einzelnen Programmen für sehr übersichtlich hält. Außerdem können Sie bei einer solchen Download-Sammlung auch nach weiteren Alternativen Ausschau halten.