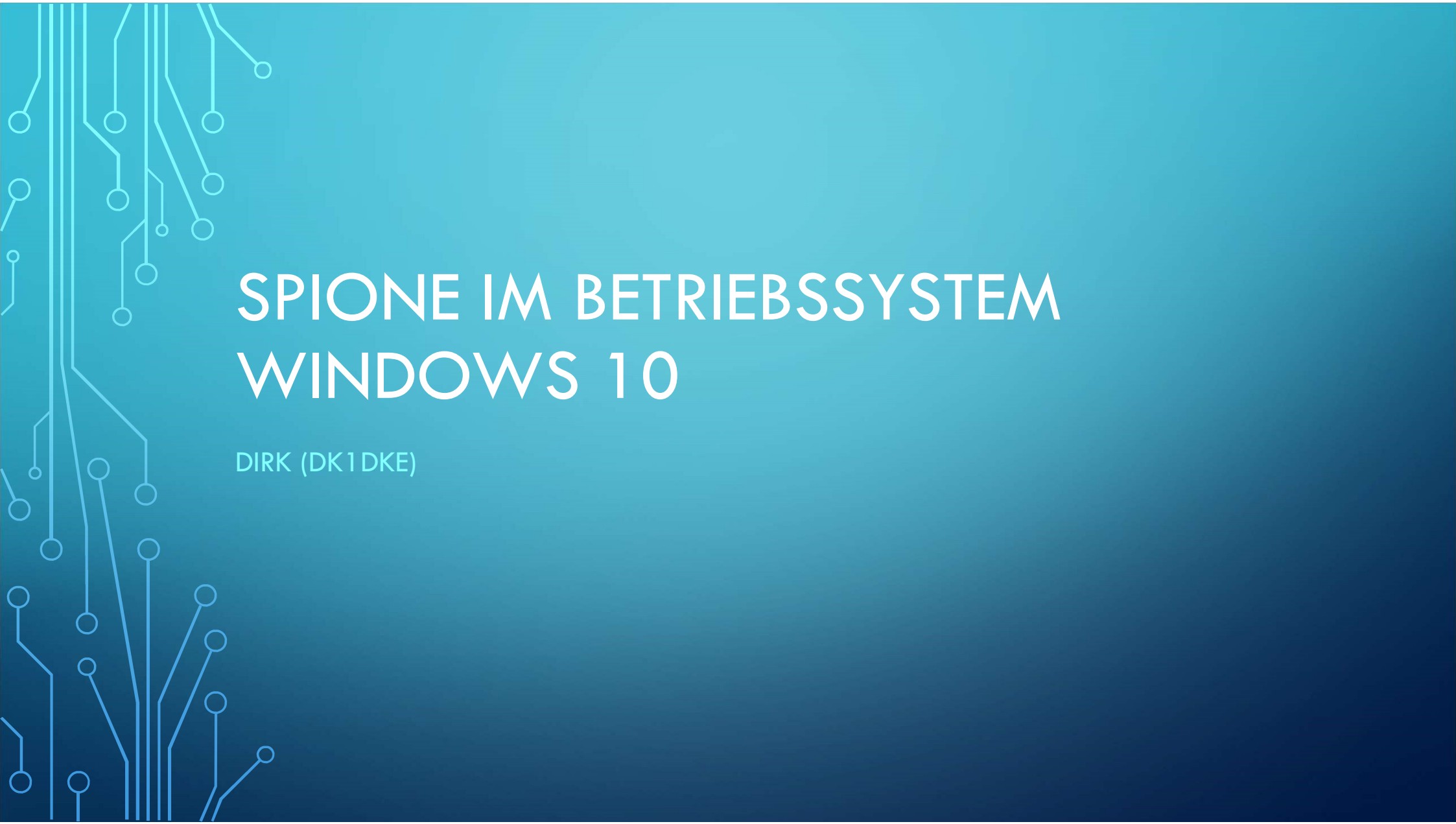


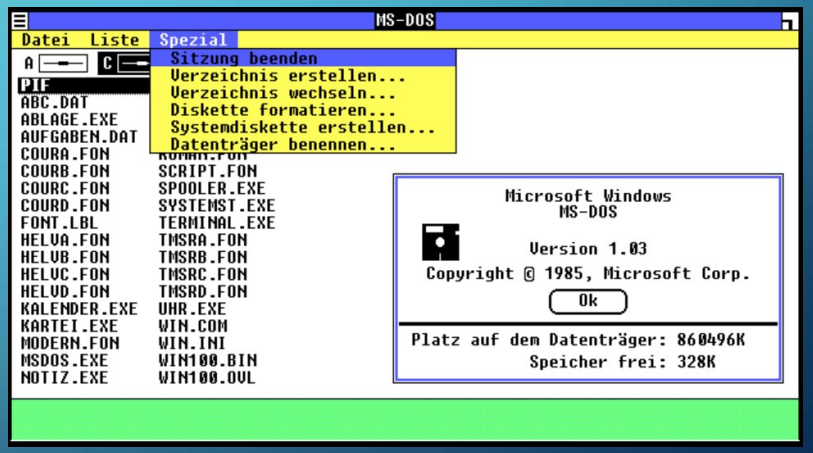
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

DIRK (DK1DKE)

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Allgemeines zu MS Windows

- Bill Gates‘ erste „grafische“ Oberfläche für DOS
- Installierte Versionen weltweit (alle Win-Versionen): ca. 1,5 Mrd
- OS-Marktanteil weltweit von Windows: 74,7 %, MacOS: 11,4 %, Rest: iOS, Android, Linux
- Erste Version -> „Interface Manager“ – Marktname: Windows1.0 (1985/86) -> noch kein eigenständiges BS, sondern nur eine Benutzeroberfläche für DOS
  - Zum Teil von Apple „abgekupfert“, aber basierend auf dem GUI (graphical user interface) von Xerox
  - Ein wenig „Rechtsstreit“ mit Apple …



- Weitere „interessante“ Versionen (für PC):
  - Windows 3.1 (erstes kommerziell erfolgreiche Windows)
  - Windows 95 (erstes eigenständige Betriebssystem, aber noch inkl. „angepasstem DOS“)
  - Windows XP (erste „Zusammenführung“ der Win NT- und Win 95-Linien)
  - Windows 7 -> Windows 10

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

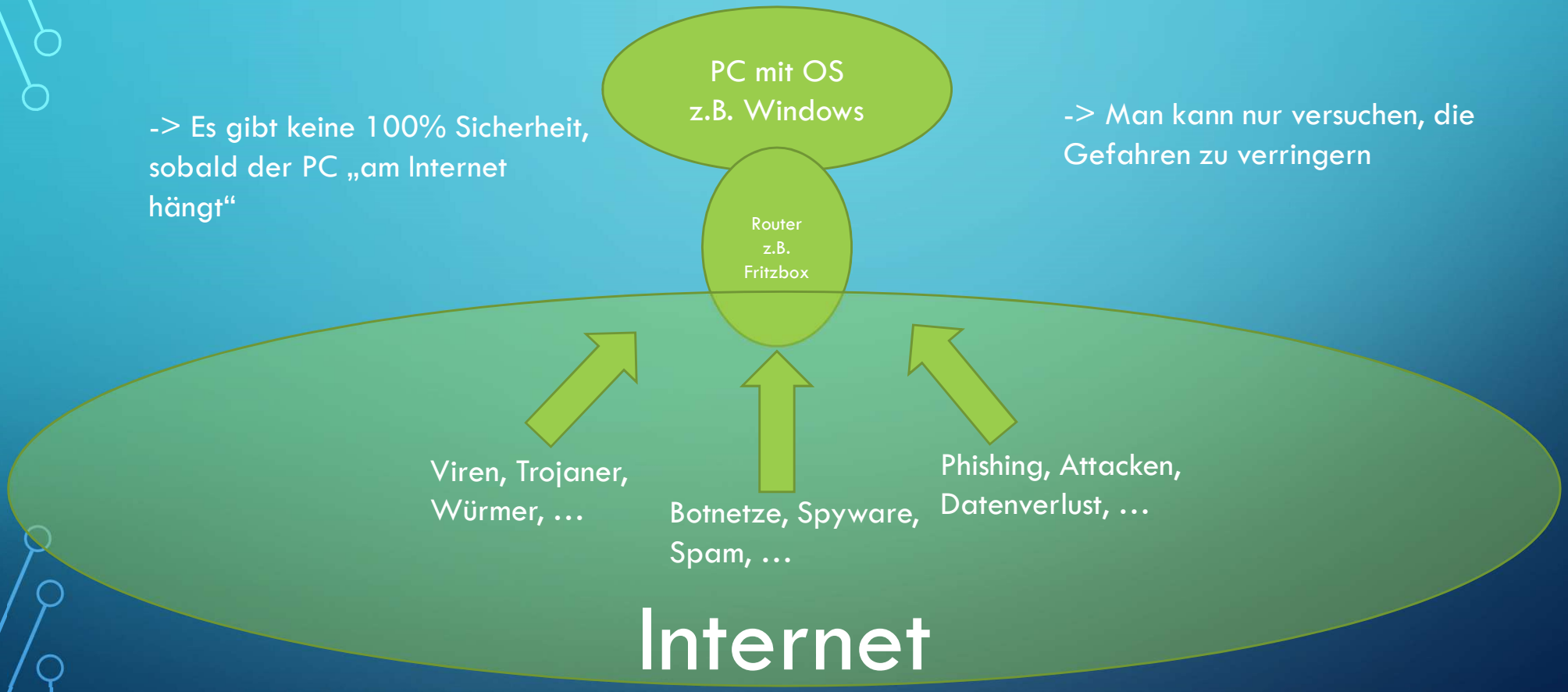
Zeitleiste der Windows-Versionen seit 1985

Typ	1980er					1990er										2000er										2010er								
	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
16-Bit-Linie	1.0		2.0			3.0		3.1			3.11																							
9x-Linie											95			98		ME																		
Desktop-OS auf NT-Basis									NT 3.1		NT 3.5	NT 3.51	NT 4.0			2000	XP						Vista		7			8		8.1			10	
Server-OS auf NT-Basis									NT 3.1 Server		NT 3.5 Server	NT 3.51 Server	NT 4.0 Server			2000 Server			Server 2003			Server 2003 R2		Server 2008	Server 2008 R2			Server 2012		Server 2012 R2			Server 2016	
Tablet ARM-OS auf NT-Basis																												RT 8		RT 8.1				
CE-Linie													CE 1.0	CE 2.0		CE 3.0		CE 4.0		CE 5.0		CE 6.0					CE 7.0		Embedded Compact 2013				
Mobile-Linie																				Mobile 2003		Mobile 5.0	Mobile 6.0	Mobile 6.1	Mobile 6.5	Phone 7.0							
Smartphone-OS auf NT-Basis																												Phone 8.0		Phone 8.1			10	

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Welche Gefahren wirken auf das OS Windows ein?

-> Es gibt keine 100% Sicherheit, sobald der PC „am Internet hängt“



-> Man kann nur versuchen, die Gefahren zu verringern

In diesem Vortrag geht es nur um Windows 10 als „Datenschleuder“ in das Internet hinein. Alle anderen Gefahren werden hier nicht behandelt.

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

- Unter „normalem“ laufenden Windows zeigt der Task Manager mehr als 100 laufende Vorgänge an -> dies ist extrem unübersichtlich

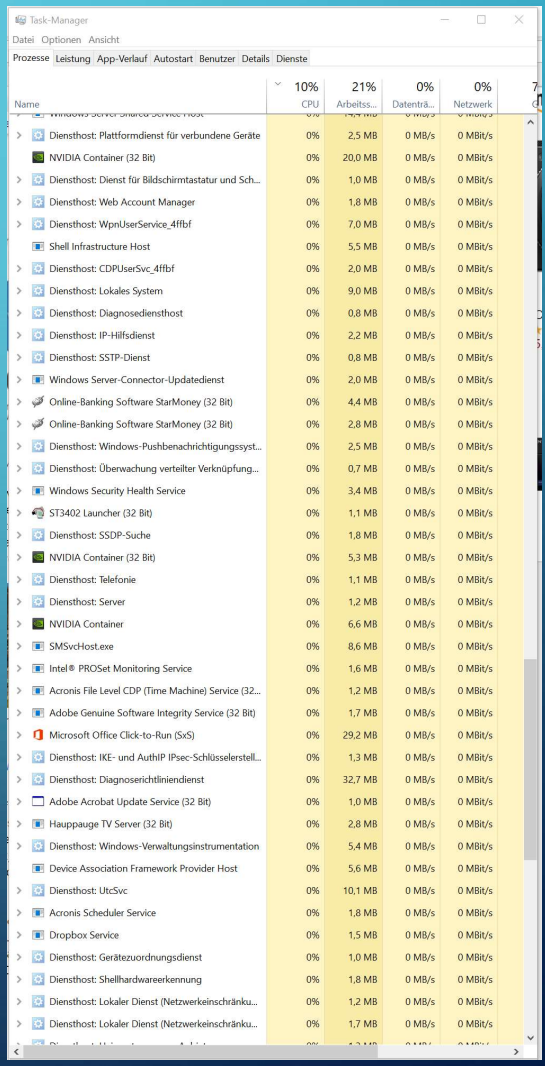
- Gefährliche SW (ob von MS selbst oder fremde SW) ist hier nicht mehr erkennbar!

- Virenscanner finden aber (wenn überhaupt) nur Windows-fremde SW!
- **Ein LÜCKE (von vielen) -> Windowseigen Programme, die „nach Hause telefonieren“!**
- Win 10 hat über 70 „Überwachungsfunktionen“, die Daten sammeln
- Der aktivste „Sammler“ in Win10 ist **Cortana** (sollte man deaktivieren, solange es noch geht!)

Wie kann man mit diesen Themen umgehen???

-> Gibt es Tricks und Tipps?
-> Gibt es Tools?
-> Kann man die Daten, die übertragen werden selbst bestimmen?
-> Kann man die Datenübertragung unterbinden, ohne „offline“ zu sein?

Zu diesen Fragen einige Hinweise …. Aber leider nicht erschöpfend!!!!

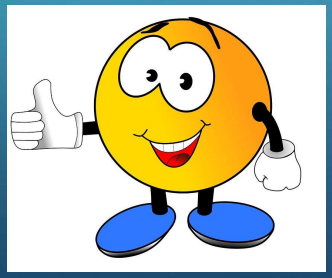


SPIONE IM BETRIEBSSYSTEM WINDOWS 10

- In diesem Vortrag werden Hinweise gegeben, wie man als „Normal-User“ ein allzu schwatzhaftes Windows 10 zähmen kann
- Es wird nicht auf Analyse-Tools eingegangen (z.B. Wire-Shark, ehemals Ethereal), mit denen man den Datentransfer vom Windows ins Internet nachverfolgen kann -> dies würde den Vortrag sprengen
- Zusätzliche Programme, die auf Euren PC‘s laufen (Office, Video-Programme, Fotobearbeitung, Virenscanner, …), werden in diesem Vortrag nicht auf ihre „Schwatzhaftigkeit“ hin analysiert -> viel zu umfangreich

Dieser Vortrag möchte Eure Sensibilität schärfen, da fast alle Programme (vor allem kostenlose Apps) Daten sammeln und über das Internet an irgendwelche Auswerte-Server schicken!!!

Meine persönliche Fragestellung bei Apps ist immer: Wenn ein Programm kostenlos angeboten wird, wie verdient der Programmierer sein Geld? Von irgendwas muss er ja leben … nur selten von der Luft und der Liebe …



SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Gibt es Tricks und Tipps?

- Es gibt nur punktuelle Ratschläge, kaum jemand kennt alle Überwachungsfunktionen von Win10
- Viele Funktionen sind gar nicht direkt abschaltbar über Menüs oder Buttons
- Verbesserungen durch Windows Updates entstehen kaum, die Funktionen werden nur besser versteckt

- Offizielle Datenschutzoptionen unter Windows 10 („Win“ + „i“ dann „Datenschutz“)
- Diese Einstellungen nimmt MS bei „Express-Einstellungen“ vor

Hier wird eine Datei angelegt mit Infos über Vorlieben, um gezielt Werbung zu platzieren (inkl. Keylogger-Funktion)
-> deaktivieren!

Hier wird eingestellt, dass Windows Web-Seiten in der Systemsprache (Deutsch) anzeigt.
-> kann aktiv bleiben

Ist nicht ganz klar, was MS hier macht …
Apps, die häufig genutzt werden, tauchen im Suchergebnis oben auf
-> deaktivieren!

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Gibt es Tools (bzw. Tool-Unterstützung), um diese Schnüffeleien zu unterbinden?

1. Anti-Spy von SecuPerts (koscht 20,- €) -> dies benutze ich!
2. ShutUp10 von O&O software (kostenlos)
3. XP-AntiSpy von xp-Antispy (Shareware)

Nachfolgend Kategorien der Windows Schnüffelaktionen (abgeleitet aus „Anti-Spy“):

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

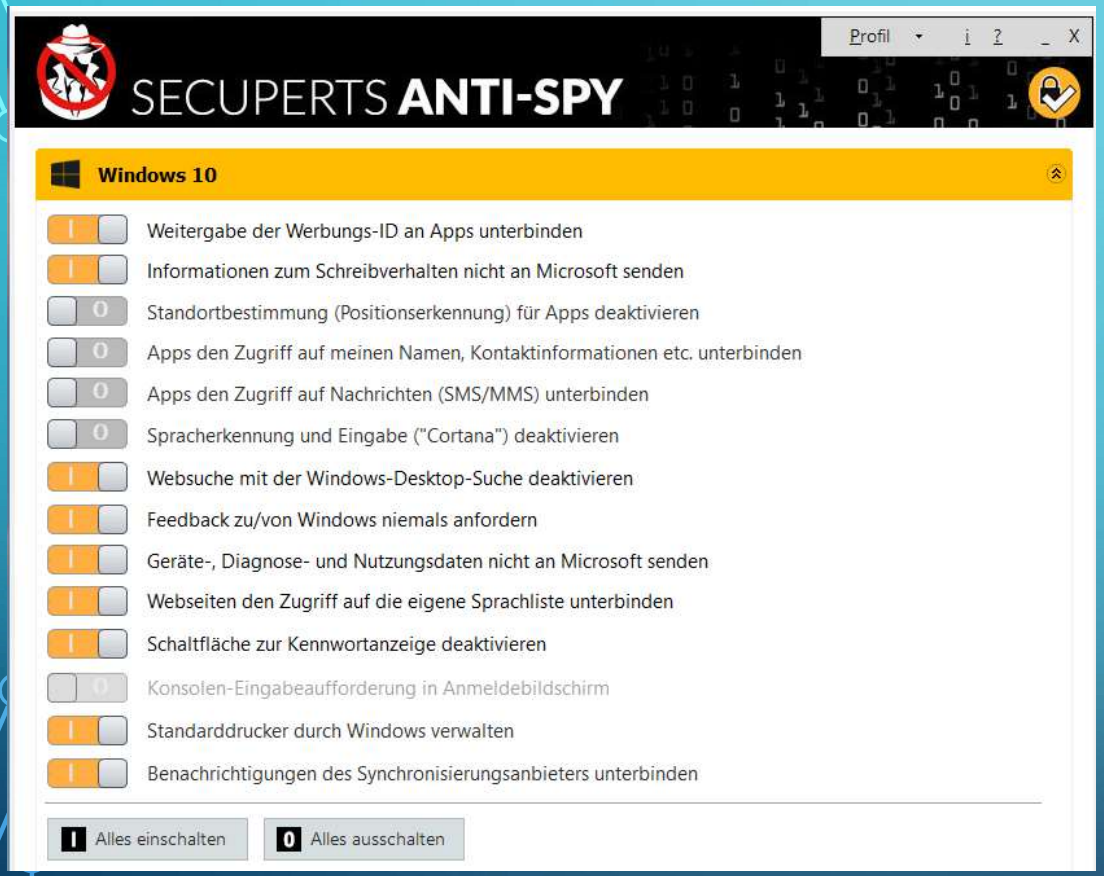
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Übertragung von Nutzerdaten an Microsoft



Unterbindung von Ausspäh-Aktionen bei Windows:

- „Werbungs-ID“ -> Datei, in der Vorlieben gespeichert werden, um gezielt Werbung zu platzieren. Hier versteckt sich auch der berüchtigte „Key-Logger“ von Win10!
- „Benachrichtigung durch Synchronisierungsanbieter“ -> dies ist OneDrive Werbung, nichts anderes!
- „Websuche mit der Windows-Desktop-Suche“ -> hier werden Suchanfragen durch Windows gespeichert und ausgewertet

Deaktivierung von Spracherkennung und App-Zugriffe -> danach funktioniert Cortana nicht mehr (was o.k. ist), aber auch Mail- und Kalender-Apps von Windows funktionieren nicht mehr richtig

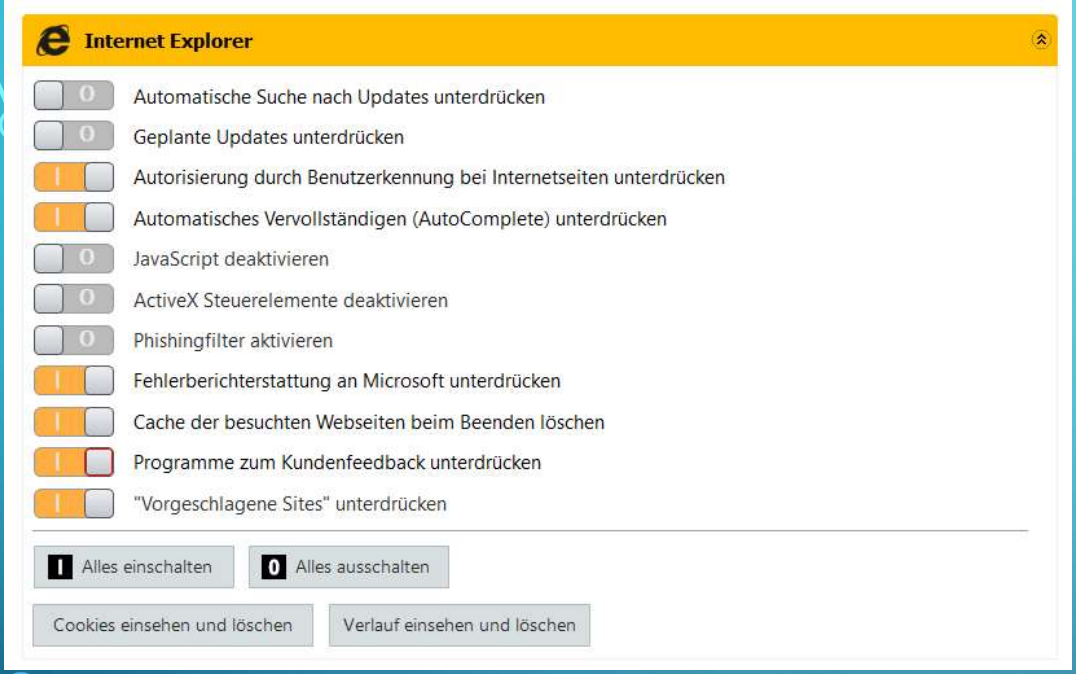
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Schnüffelfunktionen im Internet Explorer



Unterbindung von Ausspäh-Aktionen beim Internet Explorer:

- „Automatisches Vervollständigen“ und „Vorgeschlagene Sites“ -> um irgendwelche Formulare automatisch zu vervollständigen oder Web-Sites vorzuschlagen, muß Windows erst mal sammeln! Was mit den gesammelten Daten passiert, weiss keiner
- „JavaScript“ und „ActiveX“ sollten eigentlich deaktiviert werden, aber dann funktionieren viele Anwendungen im Internet nicht mehr -> hat erstmal nichts mit „Windows Spy“ zu tun

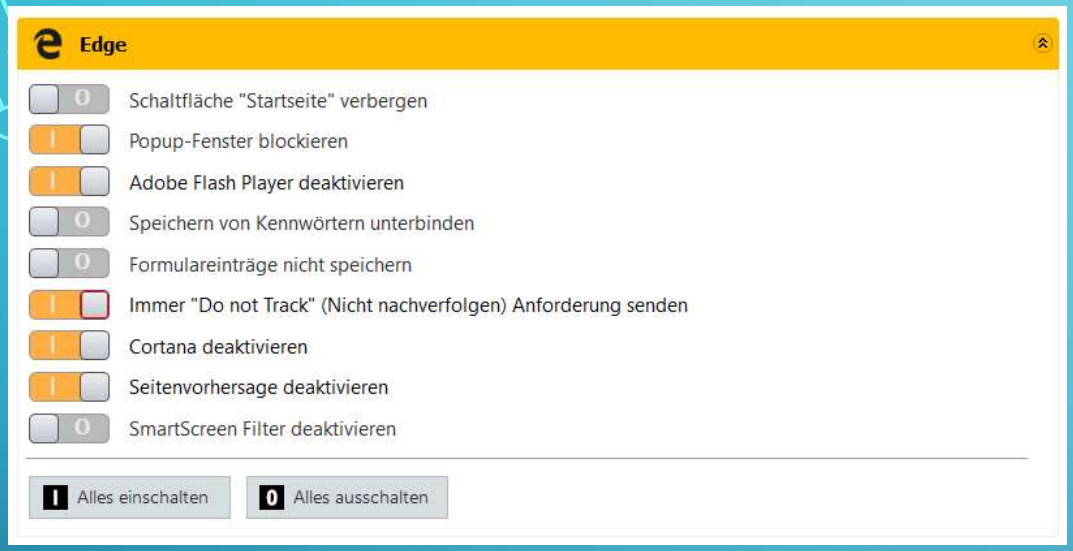
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Schnüffelfunktionen in EDGE (ex Internet Explorer)



Unterbindung von Ausspäh-Aktionen
bei Edge:

- „Do not Track“ -> es werden keine Nutzerprofile von Web-Sites erstellt
- Der Rest ist eigentlich selbsterklärend

Es gibt in Edge, wie auch im IE selbst Einstellungen zur Privatsphäre. Auf diese gehe ich hier nicht ein, ist aber auch interessant sich damit mal zu beschäftigen

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Nutzer-Optionen, die Microsoft bereitstellt

Hier ist eigentlich nur „Fehlerberichterstattung“ zu deaktivieren. Der Rest ist Geschmackssache, denke ich …

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Überwachungsfunktionen des Media Players

Wer sich noch erinnert -> der Windows Media Player war Vorreiter beim Ausspionieren von Daten. Das war der erste Datenausspäh-Skandal 2010.

- Ohne die Unterdrückung der „Übermittlung der MediaPlayer Nutzungsstatistik“ würde Windows MediaPlayer permanent Daten an MS senden
- „Identifikation des MediaPlayers“ -> bedeutet, dass andere Internet-Dienste Nutzerprofile von Euch erstellen.
- Deaktivierung von „Hinzufügen von Mediendateien“ und „Abruf von Metadaten“ ist nur sinnvoll, wenn Ihr „Schweinchen-Videos“ oder Raubkopien von Mediendateien auf dem PC habt. Dann merkt sich Windows MediaPlayer diese Daten …

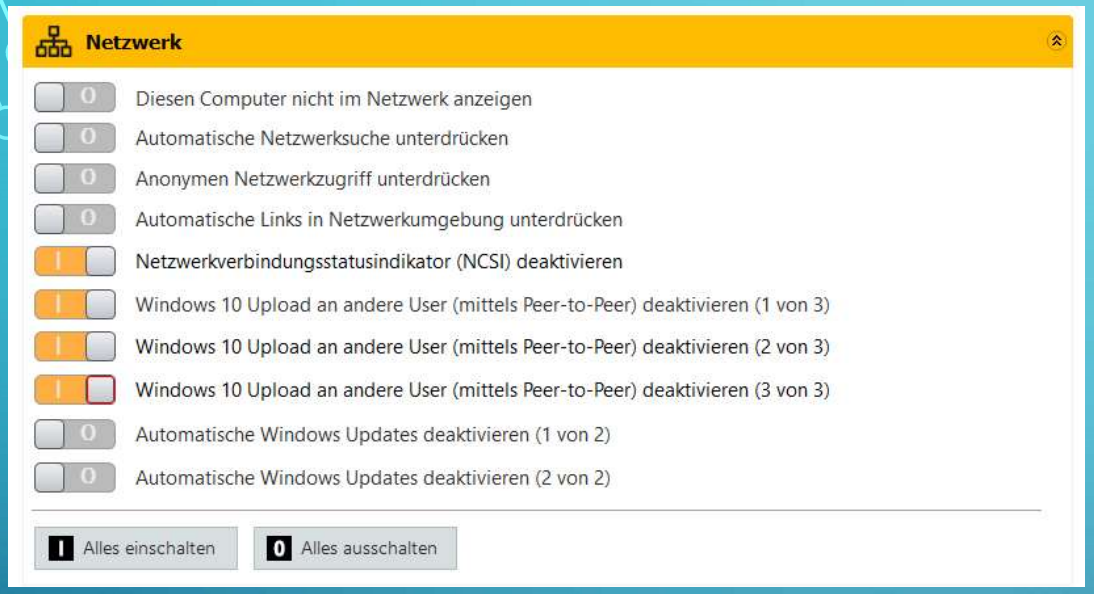
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kritische „Netzwerk-Funktionen“



- „NCSI (Network Connectivity Status Indicator)“ -> sollte abgeschaltet werden (geht übrigens nur über Eingriff in die Registry, es gibt keinen „Schalter“ in Windows), da Windows hier regelmäßig abfragt, ob eine Internet-Verbindung besteht. Hierzu wird die aktuelle IP-Adresse abgefragt und an MS gesandt.
- „Windows 10 Upload“ ist nur zu aktivieren, wenn ander User mittels P2P Updates ziehen wollen/sollen

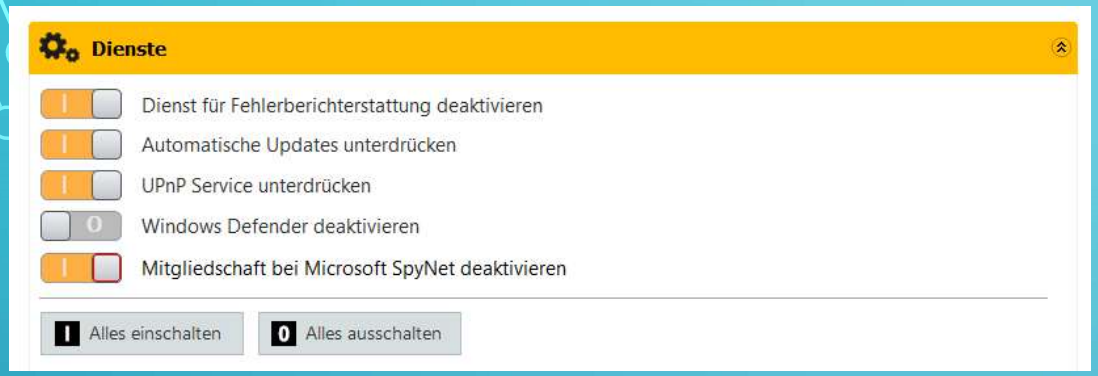
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelfunktionen im Internet Explorer
3. Schnüffelfunktionen in EDGE (ex Internet Explorer)
4. Nutzer Optionen, die MS bereitstellt
5. Überwachungsfunktionen des Media Players
6. Kritische „Netzwerk-Funktionen“
7. Weitere „interessante“ Dienste

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Weitere „interessante“ Dienste



- Wenn „UPnP Service“ deaktiviert wird, funktioniert z.B. das Streamen von Videos vom PC auf den TV nicht mehr. Ich hab‘s trotzdem deaktiviert, da meine Videos von meinem Server kommen und nicht vom PC. Auf meinem Server (Win Server 2012) ist UPnP aktiviert … einen Tod muß man sterben …
- Was eine „Mitgliedschaft bei MS SpyNet“ ist, weiss ich nicht. Ich möchte keine ungefragte Mitgliedschaft … also „deaktivieren“

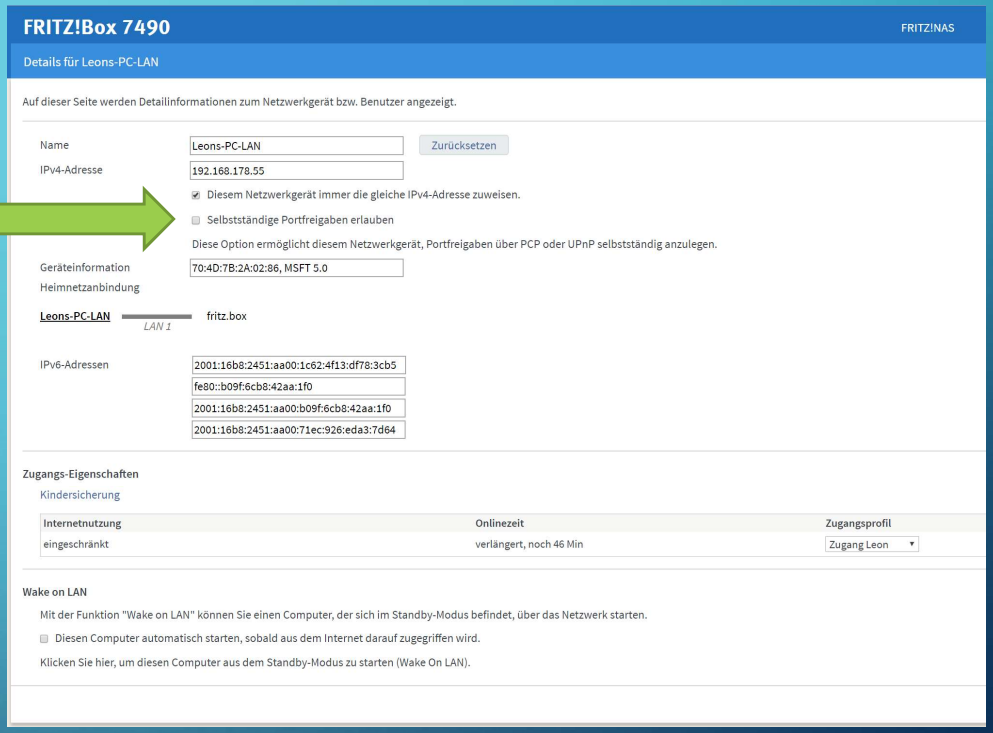
Die gezeigten Einstellungen sind nur Empfehlungen von mir.

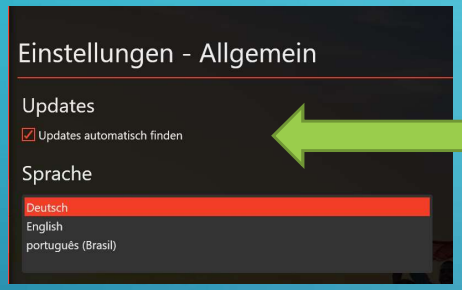
Es kann sein, dass das eine oder andere Programm, welches man unbedingt braucht, nicht mehr richtig funktioniert. Deshalb muß man dann etwas mit den Einstellungen „rumspielen“, auf die Gefahr hin, dass wieder Daten an MS übertragen werden. Dies muß jeder dann für sich abwägen!

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

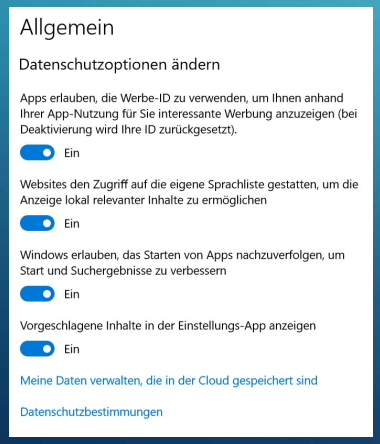
Was kann man tun, als Minimal-Variante, wenn man sich kein „Anti-Spy-Programm“ installieren möchte?

Portfreigaben mittels UPnP unterdrücken und alle Nicht benötigten Ports schliessen





Update-Service (diverser Apps) ausschalten



Datenschutzoptionen sinnvoll aktivieren/deaktivieren (Folie 7)

Vielen Dank für die Aufmerksamkeit!

„Das Wort zum Sonntag:“
Jeder ist selbst für den Schutz seiner Daten verantwortlich! Hier hilft auch kein Datenschutzgesetz weiter. Am Ende seid Ihr die Leidtragenden, beim Missbrauch Eurer Daten.

SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Quellen-Verzeichnis:

[1] https://www.tecchannel.de
[2] Computer Bild, Sonderheft 01/2018
[3] https://www.wikipedia.de