

A decorative graphic on the left side of the slide, consisting of white lines and circles on a teal background, resembling a circuit board or data flow diagram.

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“ – Markname: Windows 1.0 (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

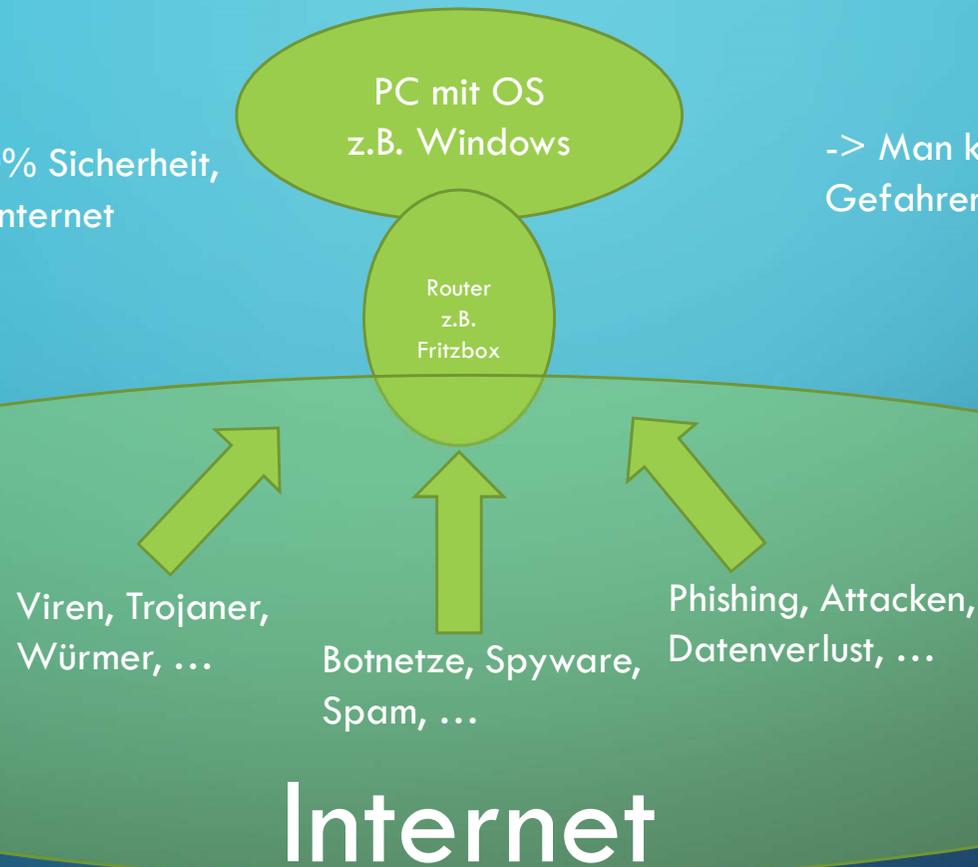
Zeitleiste der Windows-Versionen seit 1985																																						
Typ	1980er					1990er													2000er										2010er									
	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18				
16-Bit-Linie	1.0	2.0		3.0	3.1	3.11																																
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.

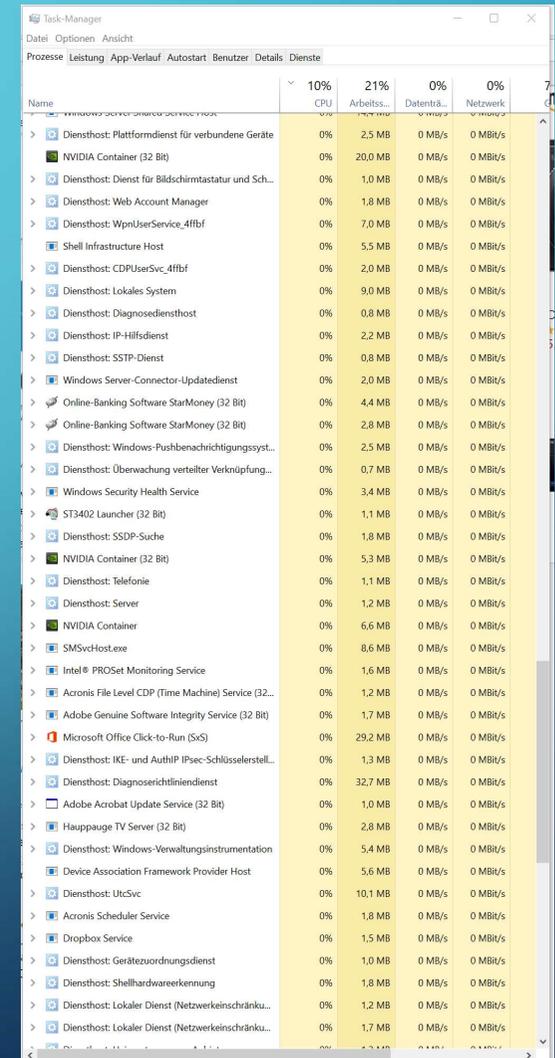
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

- 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!
- Virens Scanner finden aber (wenn überhaupt) nur Windows-fremde SW!
- **Ein LÜCKE (von vielen) -> Windowseigenen 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!!!!



The screenshot shows the Windows Task Manager window with the 'Services' tab selected. The table displays various system services and their resource usage. The columns are: Name, CPU, Arbeits... (Working Set), Datenträ... (Data Transfer), and Netzwerk (Network). The services listed include various Windows services like 'Diensthost: Plattformdienst für verbundene Geräte', 'NVIDIA Container', 'Diensthost: Dienst für Bildschirmstatur und Sch...', 'Diensthost: Web Account Manager', 'Diensthost: WpnUserService_4ffb', 'Shell Infrastructure Host', 'Diensthost: CDPUserSvc_4ffb', 'Diensthost: Lokales System', 'Diensthost: Diagnosedienst', 'Diensthost: IP-Hilfsdienst', 'Diensthost: SSTP-Dienst', 'Windows Server-Connector-Updatedienst', 'Online-Banking Software StarMoney (32 Bit)', 'Diensthost: Windows-Pushbenachrichtigungssyst...', 'Diensthost: Überwachung verteilter Verknüpfung...', 'Windows Security Health Service', 'ST3402 Launcher (32 Bit)', 'Diensthost: SSDP-Suche', 'NVIDIA Container (32 Bit)', 'Diensthost: Telefonie', 'Diensthost: Server', 'NVIDIA Container', 'SMSvcHost.exe', 'Intel® PROSet Monitoring Service', 'Acronis File Level CDP (Time Machine) Service (32...', 'Adobe Genuine Software Integrity Service (32 Bit)', 'Microsoft Office Click-to-Run (SxS)', 'Diensthost: IKE- und AuthIP IPsec-Schlüsselerstell...', 'Diensthost: Diagnoseerichtliniendienst', 'Adobe Acrobat Update Service (32 Bit)', 'Hauptpage TV Server (32 Bit)', 'Diensthost: Windows-Verwaltungsinstrumentation', 'Device Association Framework Provider Host', 'Diensthost: UtcSvc', 'Acronis Scheduler Service', 'Dropbox Service', 'Diensthost: Gerätezuordnungsdienst', 'Diensthost: Shellhardwareerkennung', 'Diensthost: Lokaler Dienst (Netzwerkeinschränku...', and 'Diensthost: Lokaler Dienst (Netzwerkeinschränku...'. The CPU usage for most services is 0%, while the Working Set and Data Transfer columns show varying amounts of memory and data usage.

Name	CPU	Arbeits...	Datenträ...	Netzwerk
Diensthost: Plattformdienst für verbundene Geräte	0%	2.5 MB	0 MB/s	0 MB/s
NVIDIA Container (32 Bit)	0%	20.0 MB	0 MB/s	0 MB/s
Diensthost: Dienst für Bildschirmstatur und Sch...	0%	1.0 MB	0 MB/s	0 MB/s
Diensthost: Web Account Manager	0%	1.8 MB	0 MB/s	0 MB/s
Diensthost: WpnUserService_4ffb	0%	7.0 MB	0 MB/s	0 MB/s
Shell Infrastructure Host	0%	5.5 MB	0 MB/s	0 MB/s
Diensthost: CDPUserSvc_4ffb	0%	2.0 MB	0 MB/s	0 MB/s
Diensthost: Lokales System	0%	9.0 MB	0 MB/s	0 MB/s
Diensthost: Diagnosedienst	0%	0.8 MB	0 MB/s	0 MB/s
Diensthost: IP-Hilfsdienst	0%	2.2 MB	0 MB/s	0 MB/s
Diensthost: SSTP-Dienst	0%	0.8 MB	0 MB/s	0 MB/s
Windows Server-Connector-Updatedienst	0%	2.0 MB	0 MB/s	0 MB/s
Online-Banking Software StarMoney (32 Bit)	0%	4.4 MB	0 MB/s	0 MB/s
Online-Banking Software StarMoney (32 Bit)	0%	2.8 MB	0 MB/s	0 MB/s
Diensthost: Windows-Pushbenachrichtigungssyst...	0%	2.5 MB	0 MB/s	0 MB/s
Diensthost: Überwachung verteilter Verknüpfung...	0%	0.7 MB	0 MB/s	0 MB/s
Windows Security Health Service	0%	3.4 MB	0 MB/s	0 MB/s
ST3402 Launcher (32 Bit)	0%	1.1 MB	0 MB/s	0 MB/s
Diensthost: SSDP-Suche	0%	1.8 MB	0 MB/s	0 MB/s
NVIDIA Container (32 Bit)	0%	5.3 MB	0 MB/s	0 MB/s
Diensthost: Telefonie	0%	1.1 MB	0 MB/s	0 MB/s
Diensthost: Server	0%	1.2 MB	0 MB/s	0 MB/s
NVIDIA Container	0%	6.6 MB	0 MB/s	0 MB/s
SMSvcHost.exe	0%	8.6 MB	0 MB/s	0 MB/s
Intel® PROSet Monitoring Service	0%	1.6 MB	0 MB/s	0 MB/s
Acronis File Level CDP (Time Machine) Service (32...	0%	1.2 MB	0 MB/s	0 MB/s
Adobe Genuine Software Integrity Service (32 Bit)	0%	1.7 MB	0 MB/s	0 MB/s
Microsoft Office Click-to-Run (SxS)	0%	29.2 MB	0 MB/s	0 MB/s
Diensthost: IKE- und AuthIP IPsec-Schlüsselerstell...	0%	1.3 MB	0 MB/s	0 MB/s
Diensthost: Diagnoseerichtliniendienst	0%	32.7 MB	0 MB/s	0 MB/s
Adobe Acrobat Update Service (32 Bit)	0%	1.0 MB	0 MB/s	0 MB/s
Hauptpage TV Server (32 Bit)	0%	2.8 MB	0 MB/s	0 MB/s
Diensthost: Windows-Verwaltungsinstrumentation	0%	5.4 MB	0 MB/s	0 MB/s
Device Association Framework Provider Host	0%	5.6 MB	0 MB/s	0 MB/s
Diensthost: UtcSvc	0%	10.1 MB	0 MB/s	0 MB/s
Acronis Scheduler Service	0%	1.8 MB	0 MB/s	0 MB/s
Dropbox Service	0%	1.5 MB	0 MB/s	0 MB/s
Diensthost: Gerätezuordnungsdienst	0%	1.0 MB	0 MB/s	0 MB/s
Diensthost: Shellhardwareerkennung	0%	1.8 MB	0 MB/s	0 MB/s
Diensthost: Lokaler Dienst (Netzwerkeinschränku...	0%	1.2 MB	0 MB/s	0 MB/s
Diensthost: Lokaler Dienst (Netzwerkeinschränku...	0%	1.7 MB	0 MB/s	0 MB/s

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, Virens Scanner, ...), 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!

Allgemein

Datenschutzoptionen ändern

Apps erlauben, die Werbe-ID zu verwenden, um Ihnen anhand Ihrer App-Nutzung für Sie interessante Werbung anzuzeigen (bei Deaktivierung wird Ihre ID zurückgesetzt).

Ein

Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

Ein

Windows erlauben, das Starten von Apps nachzuverfolgen, um Start und Suchergebnisse zu verbessern

Ein

Vorgeschlagene Inhalte in der Einstellungs-App anzeigen

Ein

[Meine Daten verwalten, die in der Cloud gespeichert sind](#)

[Datenschutzbestimmungen](#)

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. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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 Ausspääh-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

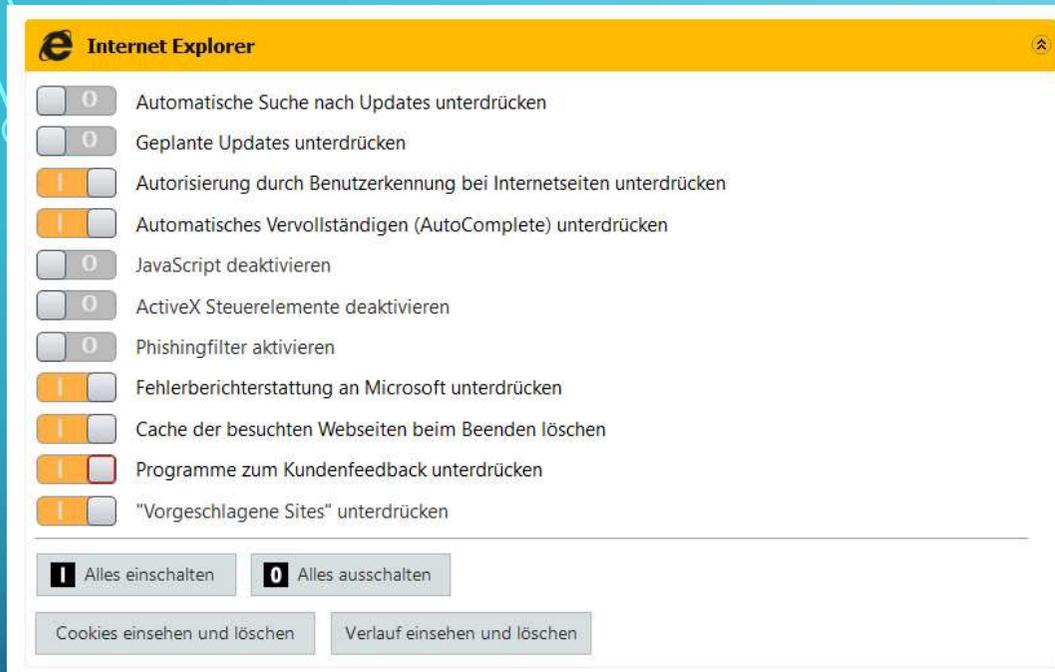
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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

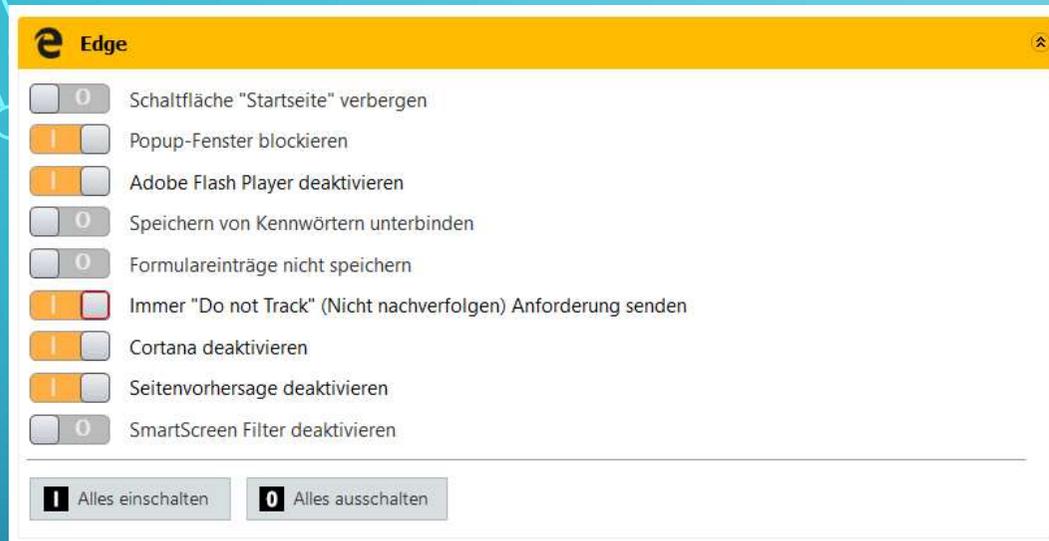
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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 Ausspääh-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. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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

...

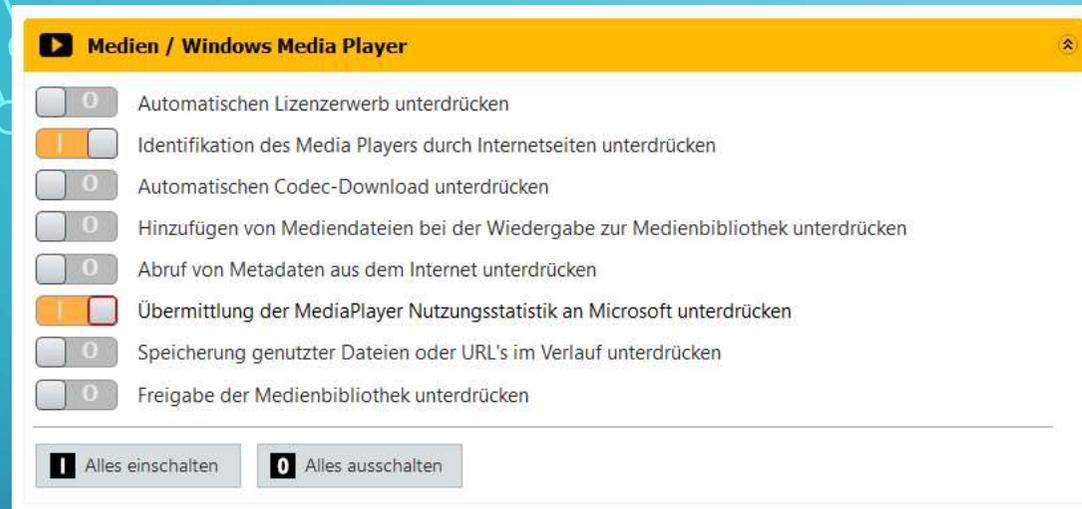
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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 ...



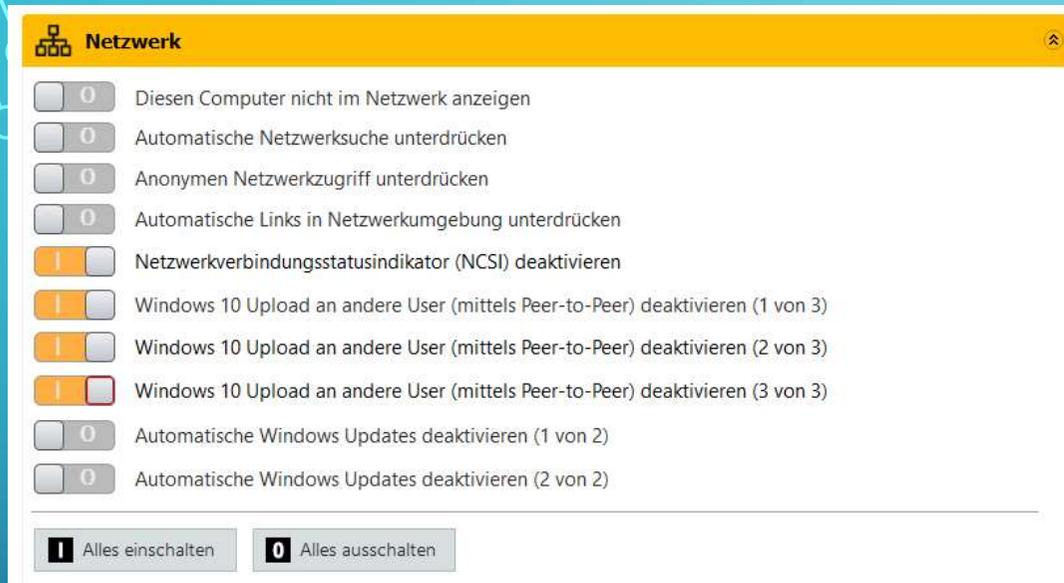
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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

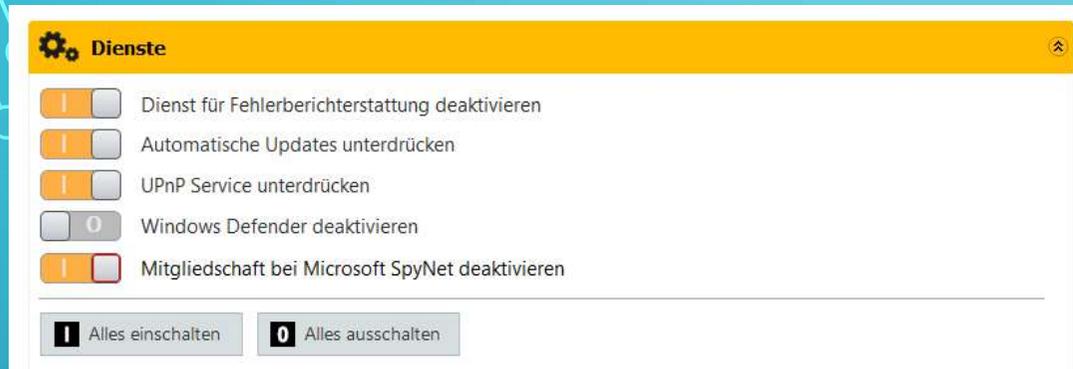
SPIONE IM BETRIEBSSYSTEM WINDOWS 10

Kategorien der Windows Schnüffelaktionen:

1. Übertragung von Nutzerdaten an MS
2. Schnüffelaktionen im Internet Explorer
3. Schnüffelaktionen 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



FRITZ!Box 7490 FRITZ!NAS

Details für Leons-PC-LAN

Auf dieser Seite werden Detailinformationen zum Netzwerkgerät bzw. Benutzer angezeigt.

Name:

IPv4-Adresse:

Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen.

Selbstständige Portfreigaben erlauben

Diese Option ermöglicht diesem Netzwerkgerät, Portfreigaben über PCP oder UPnP selbstständig anzulegen.

Geräteinformation
Heimnetzanzbindung:

Leons-PC-LAN LAN 1 fritz.box

IPv6-Adressen

2001:16b8:2451:aa00:1c62:4f13:df78:3cb5
fe80::b09f:6cb8:42aa:1f0
2001:16b8:2451:aa00:b09f:6cb8:42aa:1f0
2001:16b8:2451:aa00:71ec:926:eda3:7d64

Zugangs-Eigenschaften

Kindersicherung		
Internetnutzung	Onlinezeit	Zugangsprofil
eingeschränkt	verlängert, noch 46 Min	Zugang Leon

Wake on LAN

Mit der Funktion "Wake on LAN" können Sie einen Computer, der sich im Standby-Modus befindet, über das Netzwerk starten.

Diesen Computer automatisch starten, sobald aus dem Internet darauf zugegriffen wird.

Klicken Sie hier, um diesen Computer aus dem Standby-Modus zu starten (Wake On LAN).

Einstellungen - Allgemein

Updates

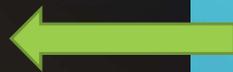
Updates automatisch finden

Sprache

Deutsch

English

português (Brasil)



Update-Service (diverser Apps) ausschalten

Allgemein

Datenschutzoptionen ändern

Apps erlauben, die Werbe-ID zu verwenden, um Ihnen anhand Ihrer App-Nutzung für Sie interessante Werbung anzuzeigen (bei Deaktivierung wird Ihre ID zurückgesetzt).

Ein

Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

Ein

Windows erlauben, das Starten von Apps nachzuverfolgen, um Start und Suchergebnisse zu verbessern

Ein

Vorgeschlagene Inhalte in der Einstellungs-App anzeigen

Ein

Meine Daten verwalten, die in der Cloud gespeichert sind

[Datenschutzbestimmungen](#)



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>