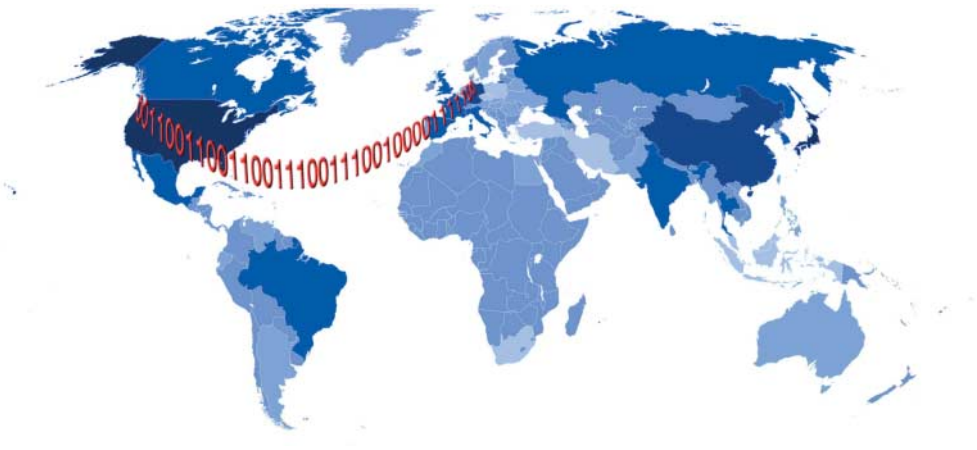
Welche Informationen
Windows 10 in die Cloud übermittelt

Datenschleuder



Lukas Grunwald

Eigentlich war Microsoft in Sachen Sicherheit auf einem guten Weg. So wurden von Security-Testern gefundene Sicherheitslücken umgehend gefixt. Doch mit der Cloud-Orientierung von Windows 10 gab es eine ungute Wende; die eine Reihe von Datenschutz-Fragen aufwirft.

```
{"709" : ["C:\\Tor Browser\\Browser\\firefox.exe","1"]}
[..]
{"3262" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\GNU\\GnuPG\\gpa.exe","1"]}
{"3263" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\GNU\\GnuPG\\kleopatra.exe","1"]}
[..]
{"4013" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\PGP Corporation\\PGP
Desktop\\PGPdesk.exe","1"]}
[..]

{"4761" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\aMule\\amule.exe","1"]}
[..]
{"4779" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\eMuleTorrent\\eMuleTorrent.exe","1"]}
{"4780" : ["{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\eMule\\emule.exe","1"]}
```

Mitschnitt 1: Was auf dem Rechner installiert ist, weiß man auch bei Microsoft (Abb. 1).

```
","K":1001,"Q":"cmd","Val":"CG","Ho":2,"Gr":3,"HC":1,"DeviceSign
als":{"Rank":0,"PHits":null,"Id":"C:\\WINDOWS\\system32\\cmd.exe
","DName":"cmd"}}]},{"T":"D.LocalApps","AppNS":"SmartSearch","Se
rvice":"AutoSuggest","Scenario":"LocalApps","SC":1,"DS":[{"T":"D
.Url","Tx":"Command Prompt","K":1002,"Q":"Command
Prompt","Val":"PP","Ho":2,"Gr":0,"DeviceSignals":{"Rank":990,"PH
its":{"0":"System.FileName","1":"System.ParsingName"},"Id":"{1AC
14E77-02E7-4E5D-B744-2EB1AE5198B7}\\cmd.exe","DName":"Command
Prompt","LAD":"2015-07-
31T11:28:57.852Z","AppLnch":7,"Args":0,"MDN":0},"RankerSignals":
{"rankingScore":7.170697083715229,"featureStore":{"0":0.18786,"1
":1,"2":7,"3":0.00257,"5":"0.001","6":131218.02,"7":990,"8":1,"
```

Mitschnitt 2: Cortana spricht nicht nur mit dem Benutzer, sondern übermittelt auch Anwendungspfade „nach Hause“ (Abb. 2).

Das Betriebssystem Windows war für die Osnabrücker Sicherheitsspezialisten von Greenbone, deren CTO der Autor dieses Artikels ist, schon einmal Gegenstand der Betrachtung. Auf der Black Hat 2008 stellten wir im Rahmen eines Vortrags über Staatstrojaner Untersuchungsergebnisse vor, die ein schlechtes Licht auf das Sicherheitslevel von Microsoft und anderen Big Playern warfen.

In vielen Fällen war der Update-Prozess unsicher, von Adobe Acrobat über Debian und Firefox bis eben zu Windows. Letzteres war, zusammen mit anderen Schwächen, ein nahezu „idealer“ Kandidat für Spyware, nicht zuletzt aufgrund seiner weiten Verbreitung. Die gute Nachricht: Die Softwarefirmen reagierten darauf, vor allem die Redmonder beseitigten die Lücken schnell und gründlich. Microsoft Update V6, eingesetzt für XP, Vista und Windows 7, war zwei Wochen nach dem Black-Hat-Vortrag sicher.

Sieben Jahre und zwei Windows-Generationen später hat sich das Blatt gewendet. Windows 10 ist durch seine mit der Cloud-Zentrierung einhergehende Geschwätzigkeit noch hinter den Stand vom Frühjahr 2008 zurückgefallen – zumindest was Datenschutz und Sicherheit angeht.

Dass regelmäßig Telemetriedaten über die Rechnerverwendung, Cortana-Anfragen und aufgerufene URLs in die Microsoft-Cloud übermittelt werden, hatte schon die EFF im August dieses Jahres thematisiert. Gleiches gilt für WLAN-Schlüssel, User-IDs und Passwörter. Wie lange und zu welchem Zweck außer der behaupteten Verbesserung des „Benutzererlebnisses“ sie dort liegen, bleibt unklar.

Unschön auch, dass diese Geschwätzigkeit voreingestellt ist und man sie in den Endbenutzerversionen nicht abstellen kann. Und wie berichtet (*iX* 9/2015, S. 92) ist diese Datenübermittlung abhörbar. Da Microsoft auf ein Zertifikat-Pinning verzichtet, ist eine Man-in-the-Middle-Attacke nahezu ein Kinderspiel. Nur das Windows-Update und der App Store sind dagegen nicht anfällig.

Deutsches Datenschutzrecht tangiert?

Neben der Abhörbarkeit stellt sich die Frage, ob Umfang und Art der an Microsoft in die USA übermittelten Daten deutschen Gesetzen entsprechen. So schicken die Office-2013- und -2016-Programme Access, OneNote, PowerPoint, Project,

Publisher, Vision und Word im Rahmen der Übermittlung von Telemetriedaten den gesamten Klickpfad nebst zugehörigen Daten wie Dateiformaten, Titel und Autor in die US-Rechenzentren.

Wenn extensive Datenübermittlung und Man-in-the-Middle-Angriffe zusammenkommen, hat man als Ergebnis ein sogenanntes (Reverse) Cloud Poisoning. Es lassen sich falsche Telemetrie- und andere Daten einspielen, sowohl in Richtung Cloud als auch vice versa. Damit steht sowohl dem Stören der Cloud-Dienste von Microsoft als auch etwa dem Unterschieben von Links zu Mal- und Spyware bis hin zum Installieren strafrechtlich relevanter Dokumente nichts im Weg.

Daten manipulierbar

Hinzu kommen Sicherheitsmängel, die eigentlich seit der letzten Jahrtausendwende ausgeräumt sein sollten: Beim Anlegen eines neuen Benutzers für die MS Cloud wird das Passwort ohne Zertifikat-Pinning übertragen, sodass jeder mit einer Man-in-the-Middle-Attacke das nicht gehashte Passwort mitlesen kann.

Bis vor acht Wochen konnten so auch BitLocker-Schlüssel einfach mitgelesen werden, das hat Microsoft aber still und heimlich abgestellt. Jetzt bekommt der Benutzer nur noch eine nichtssagende Meldung, dass die Schlüssel nicht in der Cloud gespeichert werden können. Als Datei lassen sich BitLocker-Keys weiterhin mitlesbar im OneDrive-Speicher ablegen, nur nicht mehr über Microsofts Account-Funktion.

Das Problem: Diese Datenübermittlung ist durch die auf unter 50 Seiten geschrumpften Lizenzbestimmungen von Microsoft (EULA) gedeckt. Allerdings stellt sich nach Meinung von Datenschutzexperten die Frage, ob eine so weit ge-

iX-TRACT

- Mit Windows 10 sind Sicherheits- und Datenschutzniveau des Betriebssystems deutlich gesunken.
- Auf den Servern von Microsoft landen viele persönliche Daten wie Klick- und Installationspfade.
- Ob diese Datenübermittlung in die USA deutschen und EU-Vorschriften entspricht, ist eine offene Frage.

```
User-Agent: Microsoft Office/16.0 (Windows NT 10.0; Microsoft Word 16.0.6701; Pro)
X-IDCRL_ACCEPTED: t
X-Office-Version: 16.0.6701
X-Office-Application: 0
X-Office-Platform: Win32
X-Office-SqmUserId: {35BEEC9A-0FA6-41A0-B05E-4656C64464EC}
X-Office-LastUpdate: 2016-08-22T20:32:43Z
X-Office-SusClientId: 82e544ce-1a72-4842-ab5f-2506eef2c8fe
Host: officeclient.microsoft.com
GET /ab?&clientid=%7b35BEEC9A-0FA6-41A0-B05E-4656C64464EC%7d HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft Office  2014
X-MSEdge-AppID: word
X-OCAS-Platform: win32
X-OCAS-IsEnterprise: 1
X-OCAS-Build: 16.0.6741
X-OCAS-IsSubscription: 0
X-MSEdge-IG: 8899FE7B-24AD-4A3A-ABD4-83F4CBC6FB2D
Host: ocos-office365-s2s.msedge.net
VGET /ab?&clientid=%7b35BEEC9A-0FA6-41A0-B05E-4656C64464EC%7d HTTP/1.1

Host: nexus.officeapps.live.com
Production_CBB Production NoNL::NoFlights Z97X-SLI+
Gigabyte Technology Co., Ltd.K
winword.exe en-US 10.0 78cf6450d9d71352_LiveId winword.exe 10.0 78cf6450d9d71352_LiveId
x64E To be filled by O.E.M. To be filled by O.E.M. 02025-010-47974016B7f 02025-010-47974016B7+ To be filled by O.E.M.
Z97X-SLI Gigabyte Technology Co., Ltd.f
```

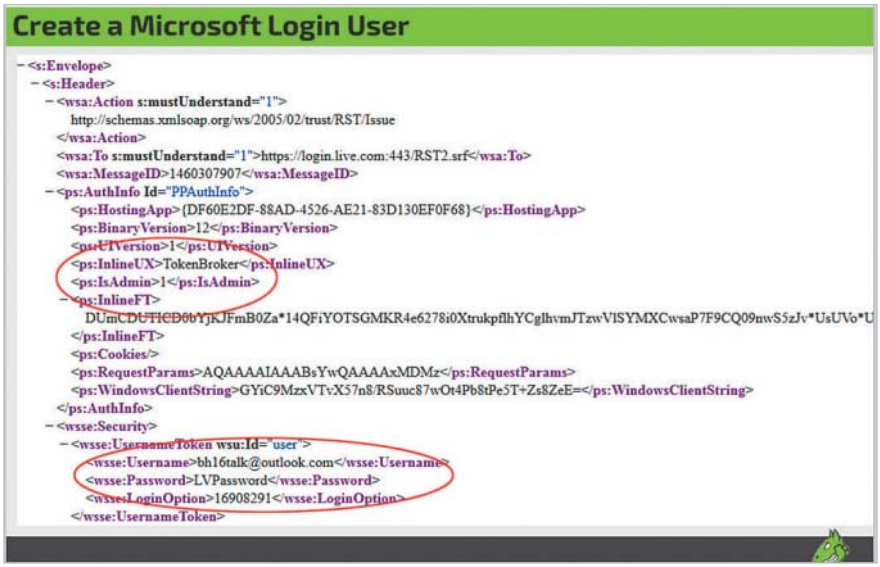
Mitschnitt 3 und 4: Datenübermittlung durch MS Office, hier Word … (Abb. 3)

```
XLDesktop Command Execution:119
XLDesktop Command Execution:119d
FileIO::CMsoOLDocBase::Lockd
)FileIO::CMsoOLDocBase::HrReadWriteLockCmdd
4PlacesPickerFeatureServiceList::GetAppSaveAsFindFiled =<E@
3PlacesPickerFeatureServiceList::FGetDefaultFilePathd DocToIdentityMapping::Initd
3MsoDocs.DesktopBackstage.Navigation.ReadLocalFolderd 8MsoDocs.DesktopBackstage.Navigation.UpdateNavContentListd /{Tb0
1MsoDocs.DesktopBackstage.Navigation.SaveFileCached
2MsoDocs.DesktopBackstage.Navigation.ReadThisPCRootd
+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd
&Excel.DesktopBackstage.SaveAs.SaveFile FileIO::CMsoOLDocBase::LockdG
%Excel.DesktopBackstage.SaveAs.LoadCFD+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd
%Excel.DesktopBackstage.SaveAs.LoadCFD%Excel.DesktopBackstage.SaveAs.LoadCFDd&Excel.DesktopBackstage.SaveAs.SaveFile
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEventd&Excel.DesktopBackstage.SaveAs.SaveFile
+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdExd+FileIO::CMsoOLDocBaseImpIOLDoc2::BeginCmdEx
FileIO::CMsoOLDocBase::Lockd&Excel.DesktopBackstage.SaveAs.SaveFile
)FileIO::CMsoOLDocBase::HrReadWriteLockCmddr q?
&Excel.DesktopBackstage.SaveAs.SaveFileMso.OpenXml.OpenPackageda2U0*
&Excel.DesktopBackstage.SaveAs.SaveFileXLShared ISAVE::HrSaved
XLDesktop Manual Save%FileIO::CMsoOLDocFile::HrDownloadTempdb2U0*
XLDesktop Manual SaveMso.OpenXml.OpenPackaged
XLDesktop Manual SaveXLDesktop Manual Saved
&Excel.DesktopBackstage.SaveAs.SaveFile
FileIO::CMsoOLDocFile::Saved
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
)FileIO::CMsoOLDocBase::HrReadWriteLockCmdd
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEventd
,FileIO::CMsoOLDocBaseImpIOLDoc2::RecordEvent
1MsoDocs.DesktopBackstage.Navigation.LoadFileCachee
,DocToIdentityMapping::TryIdentityParentMatche
'DocToIdentityMapping::GetIdentityForVUrl
'DocToIdentityMapping::GetIdentityForUrle
1MsoDocs.DesktopBackstage.Navigation.SaveFileCachee
```

… und Excel (Abb. 4)

```
GET /v3/Delivery/Cache?pubid=da63df93-3dbc-42ae-a505-
b34988683ac7&pid=209857&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=1e&rafb=0&nct
=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=0&auid=618908674f51717612cbea844b8
cfbb6&ctry=US&time=20160410T174354Z&lc=en-US&pl=en-US&idtp=mid&uid=101645fe-408e-
4b1a-b8dd-c6357c49bf6a&aid=00000000-0000-0000-0000-
000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=6b558434d80f405
8ac4b24b2052f538c&arch=x64&cdmver=10.0.10586.0&devfam=Windows.Desktop&devform=Unknown
&devosver=10.0.10586.164&fosver=10240&isu=0&lo=279930&metered=false&nettype=arcnet&oe
mid=Commodore%20Inc.&ossku=Professional&prevosver=10240&smBiosDm=Basic%202.0&smBiosMa
nufacturerName=sql'+;GO+EXEC+cmdshell('shutdown+/s')+--&tl=4

HTTP/1.1

Accept-Encoding: gzip, deflate

X-SDK-CACHE: pod=279711&chs=0&imp=0&chf=0&ds=32265&fs=12767&sc=5

Cache-Control: no-cache

User-Agent: WindowsShellClient/9.0.40929.0 (Windows)

X-SDK-HWF: kbd,m30,m75,mA0,mse,mT0

Host: arc.msn.com

Connection: Keep-Alive
```

Mitschnitt 5: ARCNET als Netztyp und Commodore als OEM – so konnten im Test Daten manipuliert werden (Abb. 5).

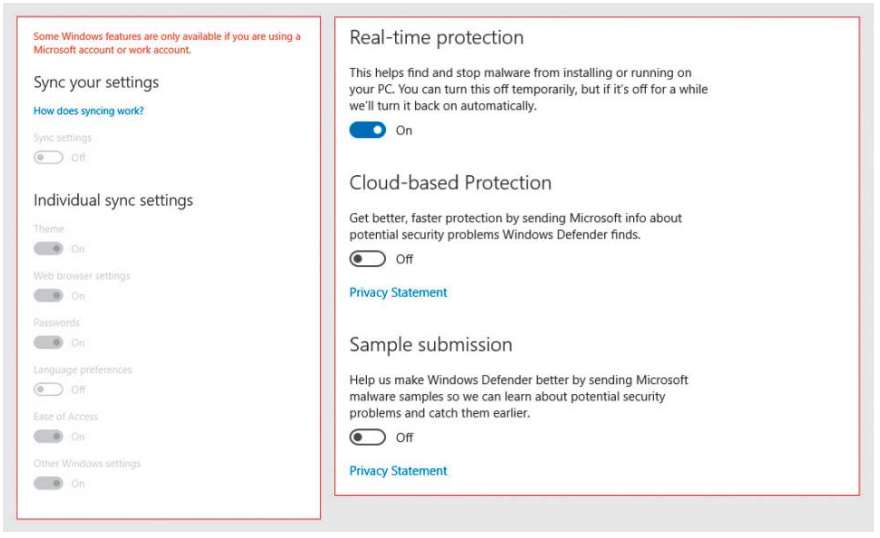


Mitschnitt 6: Wie in finstersten EDV-Zeiten werden Passwörter beim Anlegen eines neuen Benutzers ungehasht übertragen (Abb. 6).

```
POST /urs.asmx?MSURS-Client-Key=5178pvN3uGdwzGWbvvu6Nw%3d%3d&MSURS-
MAC=q0Asz9t12ok%3d HTTP/1.1
Accept: text/*
Content-Type: text/xml; charset=utf-8
User-Agent: VCSoapClient
Host: urs.microsoft.com
Content-Length: 571
Cache-Control: no-cache
<RepLookup v="5"><G>379BDC39-D58D-44AA-986B-FD2CBFFA75A6</G><O>80E6C742-3F85-
4A5C-9405-
0930AB345910</O><D>10.0.8110.6</D><C>11.00.10240.16384</C><OS>10.0.10240.0.0</OS>
<I>9.11.10240.16384</I><L>de-
DE</L><RU>aHR0cDovL3d3dy5oZWlzZS5kZS8=</RU><RI>0.0.0.0</RI><R><Rq><URL>aHR0cDovL3
d3dy5oZWlzZS5kZS8=</URL><O>PRE</O><T>TOP</T><HIP>2a00:1450:4005:0800:0000:0000:00
00:100b</HIP></Rq><Rq><URL>aHR0cDovL1syYTAwOjE0NTA6NDAwNTowODAwOjAwMDA6MDAwMDowMD
AwOjEwMGJdLw==</URL><O>PRE</O><T>IP</T><HIP>[2a00:1450:4005:0800:0000:0000:0000:1
00b]</HIP></Rq></R><WA/><PRT>219</PRT></RepLookup>
```

```
aHR0cDovL1syYTAwOjE0NTA6NDAwNTowODAwOjAwMDA6MDAwMDowMDAwOj
EwMGJdLw==http://[2a00:1450:4005:0800:0000:0000:0000:100b]
aHR0cDovL3d3dy5oZWlzZS5kZS8= http://www.heise.de/
```

Mitschnitt 7: Auch die von Edge aufgerufenen Webadressen werden über den großen Teich geschickt (Abb. 7).



Einfach mal abschalten: Synchronisation heißt immer auch Datenübermittlung (Abb. 8).

Konfigurationsoptionen zur Datenübermittlung

	Home	Pro	Enterprise
Telem.	n	n	Group Policy
Cortana	Konf.	Konf.	Konf.
Bing	n	n	Konf.
Off 13	Reg.	Reg.	Reg.
Off 16	Reg.	Reg.	Reg.

hende Erfassung und Übermittlung von Arbeitnehmerdaten deutschen Gesetzen entspricht oder nicht mindestens der Zustimmung des Betriebsrates bedürfte.

Wer die Geschwätzigkeit von Windows 10 eindämmen will, sollte ein paar Maßnahmen ergreifen. So schaltet man die Synchronisierungsfunktionen, die Daten zwischen verschiedenen Rechnern via Cloud auf demselben Stand halten, besser ab. Gleiches gilt für die Windows-Defender-bezogenen Schutzmechanismen – der Defender sendet nicht nur Malware-verdächtige Anwendungen an Microsoft, sondern eine Liste aller installierten Anwendungen.

Wege aus dem Chaos

Den Kontakt zum Microsoft-Rechenzentrum unterbricht zuverlässig ein Umlenken der entsprechenden DNS-Anfragen durch einen eigenen Domain Name Server. Der sollte Anfragen nach den verschiedenen MS-Servern auf 0.0.0.0 lenken.

In Firmen sollten die Administratoren die Datenübermittlung abschalten. Allerdings funktioniert das nur mit der Enterprise-Lizenz. Details zeigt die Tabelle, die entsprechenden Einstellungen sind über den Pfad „Computer Configuration –> Administrative Templates –> Windows Components –> Data Collection and Preview Builds“ zu finden.

Da bei der Home- und Pro-Version das Übersenden der Telemetriedaten nicht abgestellt werden kann, lassen diese sich streng genommen nicht konform zu deutschen Arbeitnehmerrechten und den damit einhergehenden Datenschutzregeln einsetzen.

Von Microsoft war bis Redaktionsschluss dazu keine Stellungnahme zu bekommen. (js)

Lukas Grunwald

ist CTO der Firmen Greenbone und DN-Systems.

Alle Links: www.ix.de/ix1611068