Windows 10 – Wie man die Datenkrake bändigt

Susanne Weinmann, B.Sc.
Referentin für IT-Sicherheit

AGENDA

1. Ausgangslage
2. IT-Sicherheit bei Windows 10
3. Fazit und Ausblick

Windows 10 – was ist neu?

- Veröffentlichung des Betriebssystems Windows 10
- Neues Konzept: „Windows-as-a-Service“
  - Dauerhafte Fortentwicklung - große Änderungen nicht mehr als SP oder neues Betriebssystem, sondern als normales Update
- Microsoft sieht zukünftiges Geschäft nicht im Verkauf von Betriebssystemen sondern in der Bereitstellung von Dienstleistungen, welche auf der „Plattform“ Windows 10 laufen
- Damit verfolgt Microsoft nun das gleiche Konzept wie Apple und Google es bereits seit Jahren tun.

Ausgangslage in der MPG im August 2015

- Vereinzelte Stand-Alone-Geräte
  - Windows 10 Pro
  - Nicht in der Domäne betrieben
  - Durch lokale IT-Abteilung betreut
- Einschätzung des Betriebssystems hinsichtlich Datenschutz und IT-Sicherheit durch den ITSB aufgrund der öffentlichen Berichterstattung zu Windows 10
- Zusätzlich: Prüfung der neuen Datenschutzbestimmungen von Microsoft

Weitere Entwicklung

- Austausch mit Kollegen aus der MPG und anderen Forschungseinrichtungen
  - Bitte um Feedback und Aufruf zum Erfahrungsaustausch
- Erste Rückmeldungen von Kollegen aus den Max-Planck-Instituten sowie aus Helmholtz-Zentren und von Fraunhofer-Instituten
  - Ergänzung / Aktualisierung des Dokuments
- Präsentation der Ergebnisse bei der AKIF IT-Sicherheitstagung im November 2015
  - Gründung einer Arbeitsgruppe für eine Orientierungshilfe
    - Beteiligte: MPG, TU Dresden, Helmholtz-Zentrum Geesthacht, Fraunhofer SIT, Universität Hohenheim
    - Arbeit an der Orientierungshilfe neben den üblichen Aufgaben

Erster Entwurf einer Orientierungshilfe

- Zusammenführung und Ergänzung der bisherigen Erkenntnisse in ein Dokument
- Berücksichtigung der verschiedenen Einsatzszenarien und der verwendeten Versionen von Windows 10
- Focus auf Aspekten der IT-Sicherheit und Datenschutzkonformität
  - Identifizierung von besonders kritischen Features
  - Eigenschaften der unterschiedlichen Betriebssystemversionen
  - Betrachtung der grundlegenden Neuerungen
- (unvollständige) Sammlung von Konfigurationshilfen für GPOs und Registry
- Dokumentation mit Screenshots

AGENDA

1. Ausgangslage
2. IT-Sicherheit bei Windows 10
3. Fazit und Ausblick

Kritisch betrachtete Features - Beispiele

- Cortana – digitaler Assistent in Windows 10
  - Weitreichender Datenzugriff
  - Übertragung der Daten in Microsoft Cloud zur Auswertung
  - Kann durch Möglichkeit der Sprachsteuerung dauerhaft „lauschen"
- Edge – Browser
  - Nachfolger des Internet Explorers
  - Stark mit Bing verknüpft (übermittelt Daten an Microsoft)
- Taskleisten-Suchfeld / Web-Suche (Suche lokal und im Internet)
  - Mit Bing verknüpft, kann nicht durch andere Suchmaschine ersetzt werden
- Werbe-ID – Einblendung von an persönliche Interessen angepasste Werbung
- Windows Update
  - Updates können nicht verhindert werden, fehlerhafte Updates gefährden das Gesamtsystem
  - ABER: ab Windows 10 Pro ist zumindest der Update-Zeitpunkt steuerbar

WLAN-Optimierung

- ALT (bis Version 1511):
  - Passwort für ein bekanntes WLAN kann mit Kontakten (Skype, Facebook, Outlook) geteilt werden
  - Missbrauch von WLANs durch unberechtigte Dritte ist möglich
  - der normalerweise von Organisationen verwendete Standard zur Authentifizierung in WLANs (802.1x) ist hiervon nicht betroffen
  - ABER: „offen" betriebene WLANs
- NEU (ab Version 1607):
  - Funktion zum „Teilen" verschlüsselter WLANs wurde entfernt
  - Das „Teilen" unverschlüsselter WLANs und Hotspots ist weiterhin möglich

Gruppenrichtlinien

- Ab Pro-Edition – unterschiedliche Ausprägung
  - einige Einstellungen sind dennoch nur im Benutzerprofil möglich
- Bisher aufgetretene Probleme:
  - Einige GPO ändern sich mit Update
  - Einige Einstellungen gehen nach Update verloren
  - Neue GPO für neue Features nach Update
- Als Anhang in der Orientierungshilfe:
  - Sammlung relevanter GPO für Datenschutz- und IT-Sicherheits-Einstellungen
    - NICHT VOLLSTÄNDIG

Datenschutz-Einstellungen

- Neu unter Windows 10
  - Datenschutzrelevante Einstellungen zu verschiedenen Funktionen, bspw. Kamera, Spracherkennung, Kalender, E-Mail, etc.
- Können ab Windows 10 Pro weitgehend per GPO konfiguriert werden
- Für einige Funktionen (z.B. Zuteilen und Entziehen von App-Berechtigungen) ist Konfiguration im Benutzerprofil erforderlich
- u.U. gehen Einstellungen bei Updates verloren

AGENDA

1 Ausgangslage

2 IT-Sicherheit bei Windows 10

3 Fazit und Ausblick

Fazit

- Windows 10 verfolgt nicht das „Privacy by design"-Prinzip
  - Derzeit müssen die meisten Features/Einstellungen explizit ausgeschaltet werden („Privacy by default")
- Nach Updates muss gesamtes System geprüft werden hinsichtlich Änderungen oder möglicher zurückgesetzter Einstellungen
- Prüfung von Windows 10 bzw. einiger Funktionen daraus durch Datenschutzaufsichtsbehörden noch nicht abgeschlossen
- Auswirkungen der EU-DSGVO auf Windows 10 noch unklar

Fazit

- Geänderte Rahmenbedingungen erfordern einen umfassenden Einsatz personeller und zeitlicher Ressourcen bei der Prüfung und Einrichtung von Windows 10 für den (datenschutzkonformen) Einsatz in der Organisation
  - Auch finanzielle Ressourcen: Aufbau von Testumgebungen, Anschaffung Testgeräte, Lizenzen
  - gerade kleiner Institute/Organisationen sind nicht in der Lage das Betriebssystem in diesem Umfang zu prüfen
- Eine abschließende Empfehlung kann derzeit nicht gegeben werden
  - Aber (gilt für die MPG): vertretbarer Einsatz von Windows 10 Enterprise LTSB mit restriktiven Einstellungen für den Datenschutz sowie den gängigen Maßnahmen im Rahmen der IT-Sicherheit

Orientierungshilfe

- Bereitstellung der Orientierungshilfe durch den AKIF
- Bietet Informationen und Empfehlungen zur datenarmen Konfiguration von Windows 10
  - **ABER: keine verbindlichen Vorgaben!**
- Ein kleines Team von Experten trägt Erfahrungen zusammen und bündelt diese in einem Dokument
  - Gerade kleine Einrichtungen können davon profitieren
  - Einrichtungen können Entwicklung im Auge behalten und gemeinsam Strategien entwickeln

Ausblick

- Weiterentwicklung der Orientierungshilfe
  - Dauerhaft, da Windows 10 kein abgeschlossenes Betriebssystem ist
  - neue Features können hinzukommen und müssen neu geprüft werden
  - Änderungen in der Konfiguration (z.B. Gruppenrichtlinien) durch Updates
- Wo sind die Dokumente verfügbar?

  https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf

  https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Datenschutzrechtliche_Probleme_bei_der_Einfuehrung_neuer_Betriebssysteme.pdf

Susanne Weinmann
Referentin für IT-Sicherheit
Tel: 089-2108-1436
susanne.weinmann@gv.mpg.de

https://www.it-sicherheit.mpg.de/

Vielen Dank für Ihre Aufmerksamkeit !

TECHNISCHE UNIVERSITÄT DRESDEN

Stabsstelle für Informationssicherheit

Windows 10

Bildquelle: Microsoft Corporation

Untersuchung des Kommunikationsverhaltens

Jens Syckor
Technische Universität Dresden
Stabsstelle für Informationssicherheit
jens.syckor@tu-dresden.de

5. DFN-Konferenz Datenschutz 29. November 2016

Ausgangslage:

- Es ist weitestgehend unbekannt, welche Daten für welche Zwecke an Microsoft übermittelt werden…

Untersuchungsgegenstand:

- Kommunikationsverhalten von Windows 10

Fragestellungen:

- Welche Auswirkungen hat die Konfiguration auf das Kommunikationsverhalten?
- Mit welcher datenarmen Konfiguration ist das Kommunikationsverhalten am geringsten?
- Welche Daten werden an Microsoft bei einer datenarmen Konfiguration übermittelt?

Untersuchungsgegenstand (Editionen)

- Education (Version 1507)
- Enterprise Long Time Servicing Branch (LTSB, Versionen 2015/2016)

Windows 10 Education

- funktional gleichwertig zu Enterprise, speziell für Forschung und Lehre
- seit Version 1607 ohne Cortana

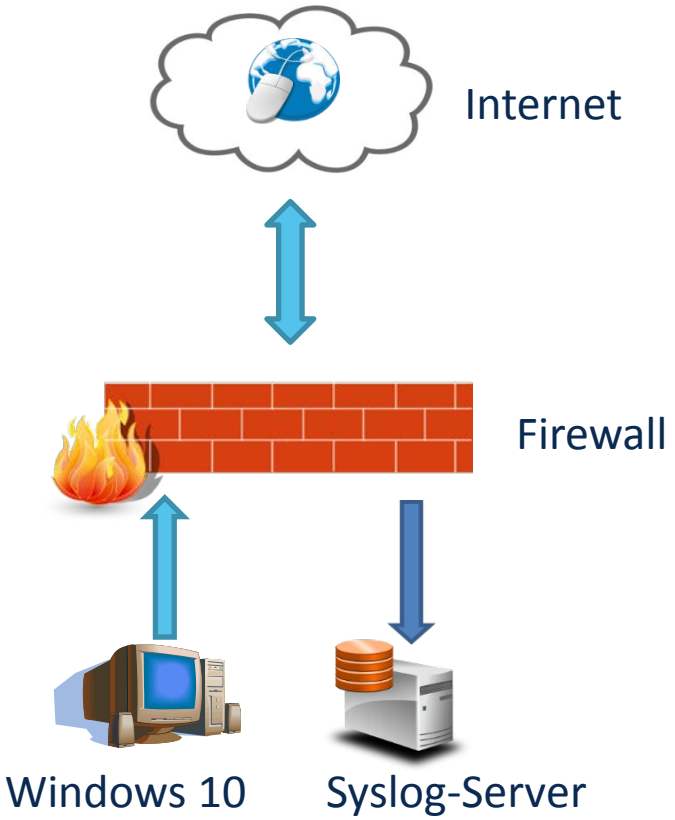
Windows 10 Enterprise LTSB („stripped down edition“)

- nur Sicherheits- und Stabilitäts-Updates, keine neue Funktionalitäten
- enthält nicht: Windows Store, Cortana, Edge Browser, Universal Apps
- enthält als Browser standardmäßig Internet-Explorer
- langer Supportzeitraum (10 Jahre)

Untersuchungsgegenstand (Drehbuch):

- Betrachtung des Betriebssystems als Black-Box
- Installation und Konfiguration mit verschiedenen Einstellungen zum Datenschutz und IT-Sicherheit (Szenarien)
- Einsatz einer Firewall vor dem Windows-10 Client
- Konfiguration eines Benutzers
- Auswertung das Kommunikationsverhaltens ohne Benutzerinteraktion

Windows 10 / Szenarien



WIN 10 EDU
I) Expressinstallation (ohne MS Konto)
1. ausgehend nichts erlaubt
2. ausgehend nur TUD-DNS erlaubt

WIN 10 LTSB
II) Expressinstallation (ohne MS Konto)
1. ausgehend nichts erlaubt
2. ausgehend nur TUD-DNS erlaubt
3. ausgehend alles erlaubt

WIN 10 EDU
III) Nutzergeführte Installation (ohne MS Konto)
ausgehend alles erlaubt / mit Nutzung "Einstellungen/Datenschutz“

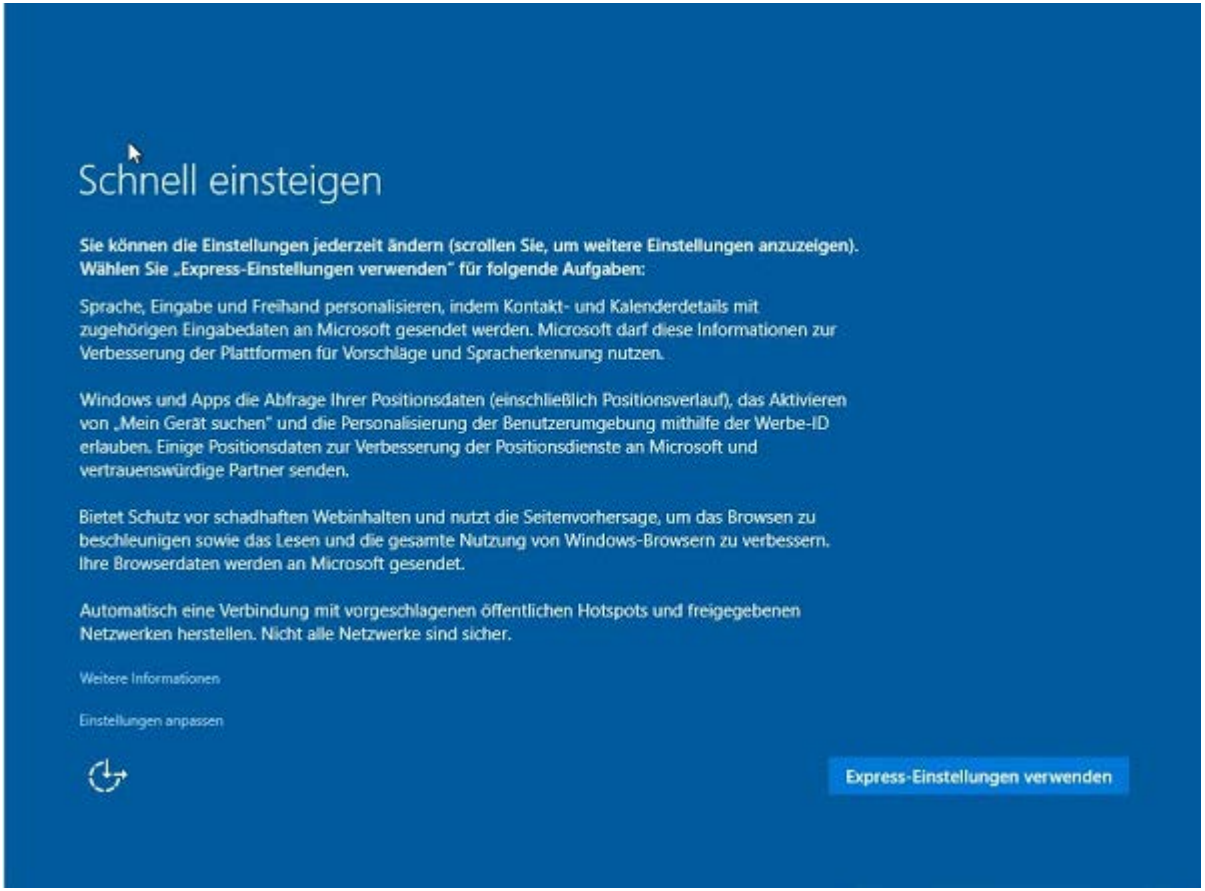
WIN 10 LTSB
IV) Nutzergeführte Installation (ohne MS Konto)
1. ausgehend alles erlaubt / mit Nutzung "Einstellungen/Datenschutz“
2. ausgehend alles erlaubt / mit AKIF-Orientierungshilfe

WIN 10 EDU
V) Nutzergeführte Installation (mit MS Konto)
1. ausgehend alles erlaubt / ohne Nutzung "Einstellungen/Datenschutz“
2. ausgehend alles erlaubt / mit Nutzung "Einstellungen/Datenschutz“

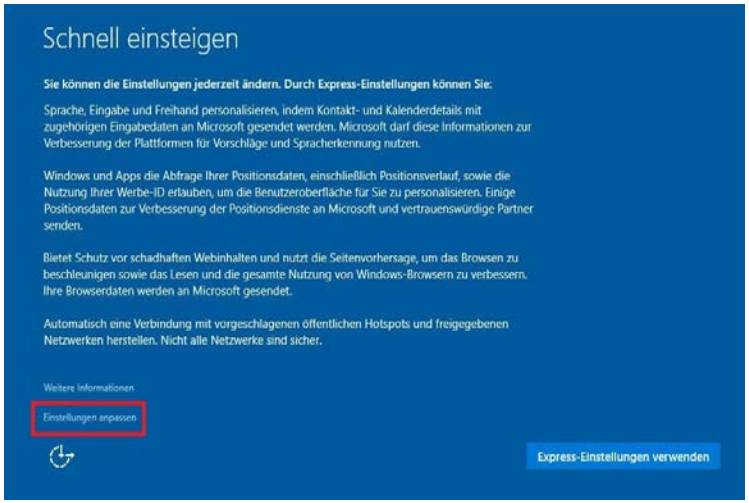
WIN 10 LTSB
VI) Nutzergeführte Installation (mit MS Konto)
1. ausgehend alles erlaubt / ohne Nutzung "Einstellungen/Datenschutz"
2. ausgehend alles erlaubt / mit Nutzung "Einstellungen/Datenschutz“

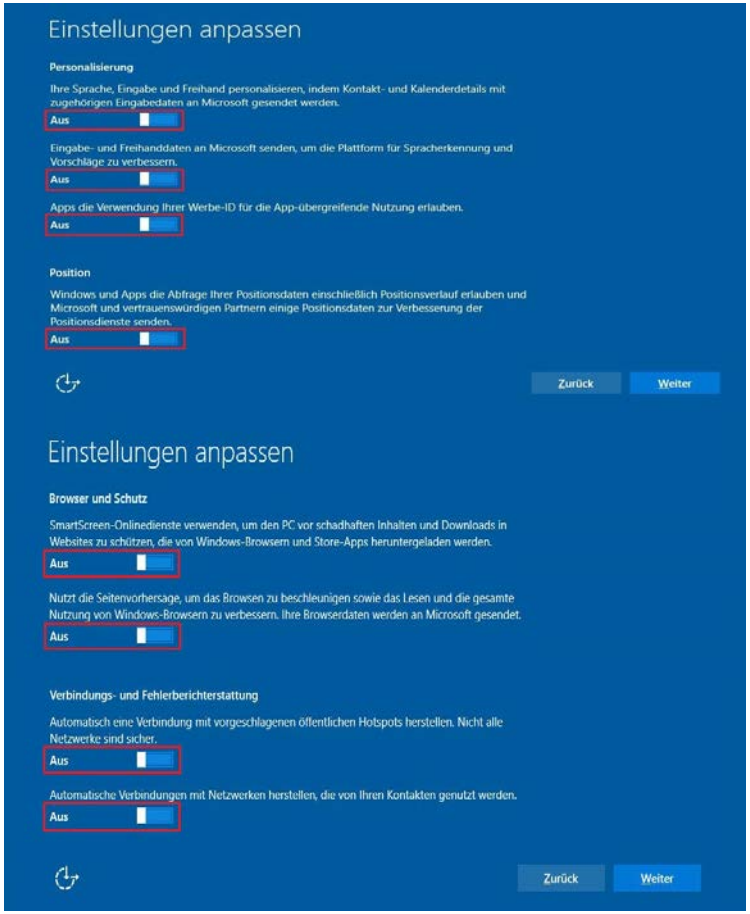
Inhalt der Logfiles:
Alle aufgebauten und abgewiesenen Anfragen/Verbindungen

Hauptszenarien: Expressinstallation



Hauptszenarien: Nutzergeführte Installation





Hauptszenarien: Administrative Installation mit Orientierungshilfe der AKIF-Arbeitsgruppe

Script (Powershell)

```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\
LocationAndSensors" -name "DisableWindowsLocationProvider"
-value "1" -propertyType dword -force
```

Script (Powershell)

```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Device Metadata"
-name "PreventDeviceMetadataFromNetwork" -value "1" -
propertyType dword -force
```

Script (Powershell)

```
1)
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name
"DontOfferThroughWUAU" -value "1" -propertyType dword
-force
2)
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name "
DontReportInfectionInformation " -value "1" -propertyType
dword -force
```

Ergebnisse:

- Übermittlung von Daten an Microsoft bereits während der Installation
- Nutzergeführte Installation („Schieberegler“) erzeugt höheres Kommunikationsverhalten als administrative datenarme Installation
- Edition Education erzeugt deutlich erhöhtes Kommunikationsverhalten mit Microsoft, auch bei datenarmer Einstellung (Ziele: 49)
- Edition LTSB 2015/2016 mit geringeren Kommunikationsverhalten (Ziele: 14/36)

- Geringstes Kommunikationsverhalten beim Einsatz von Windows 10 LTSB mit datenarmer Konfiguration nach der AKIF-Orientierungshilfe

Kommunikationsbeziehungen Windows 10 LTSB 2015

1	UDP	141.30.66.135	53		DNS TU Dresden
2	TCP	23.37.42.235	80	a23-37-42-235.deploy.static.akamaitechnologies.com	
3	TCP	65.55.113.12	80	CloudFare ohne DNS-Namen	Microsoft Hosting
4	TCP	204.79.197.200	443	bing.com, www.bing.com, *.platform.bing.com, *.bing.com, ieonline.microsoft.com, *.windowssearch.com, cn.ieonline.microsoft.com, *.origin.bing.com, *.mm.bing.net, *.api.bing.com, ecn.dev.virtualearth.net, *.cn.bing.net, *.cn.bing.com, *.ssl.bing.com, *.appex.bing.com, *.platform.cn.bing.com, ssl-api.bing.com, ssl-api.bing.net, *.api.bing.net, bingsandbox.com, www.bingsandbox.com, *.bingapis.com, *.working-bingapis-int.com, *.staging-bingapis-int.com, *.working-bingapis-int.net, *.staging-bingapis-int.net, feedback.microsoft.com, feedback-int.microsoft.com,	
5	TCP	65.55.252.92	443	*.big.telemetry.microsoft.com, *.telemetry.microsoft.com, telemetry.microsoft.com, *.phx.gbl	
6	TCP	191.232.139.253	443	settings.data.microsoft.com, groups.data.microsoft.com	
7	TCP	191.237.208.126	443	spynet2.microsoft.com, spynetalt.microsoft.com, spynet.microsoft.com, SpyNetFrontEnd-DC1-TiP.cloudapp.net, SpyNetFrontEnd-DC2-TiP.cloudapp.net, SpyNetFrontEnd-EAS-TiP.cloudapp.net, SpyNetFrontEnd-SAS-TiP.cloudapp.net, SpyNetFrontEnd-NEU-TiP.cloudapp.net, SpyNetFrontEnd-WEU-TiP.cloudapp.net, SpyNetFrontEnd-BRA-TiP.cloudapp.net, SpyNetFrontEnd-JPE-TiP.cloudapp.net, SpyNetFrontEnd-JPW-TiP.cloudapp.net, SpyNetFrontEnd-AUE-TiP.cloudapp.net, SpyNetFrontEnd-AUS-TiP.cloudapp.net	
8	TCP	134.170.53.30	443	fe2.update.microsoft.com	
9	TCP	212.201.100.142	80	a212-201-100-142.deploy.akamaitechnologies.com	
10	TCP	23.37.45.183	443	cp201-prod.do.dsp.mp.microsoft.com, disc201-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, kv201-prod.do.dsp.mp.microsoft.com	
11	TCP	65.52.108.135	443	array102-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com	
12	TCP	95.101.46.117	443	cp101-prod.do.dsp.mp.microsoft.com, kv101-prod.do.dsp.mp.microsoft.com, disc101-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com	
13	TCP	191.234.4.50	80	c-0001.c-msedge.net	Microsoft Bing
14	TCP	157.55.133.204	443	sls.update.microsoft.com	

Kommunikationsbeziehungen Windows 10 LTSB 2016

1	UDP	141.30.66.135	53		DNS TU Dresden
2	TCP	13.107.4.52	80		Microsoft NTP
3	UDP	40.118.103.7	123		
4	TCP	23.60.205.224	80	a23-60-205-224.deploy.static.akamaitechnologies.com	
5	TCP	52.164.240.59	80		Microsoft Azure
6	TCP	157.56.77.140	443	sls.update.microsoft.com	Microsoft Corporation
7	TCP	104.121.76.17	80	a104-121-76-17.deploy.static.akamaitechnologies.com	
8	TCP	191.232.80.58	443	fe2.update.microsoft.com	Microsoft Corporation
9	TCP	104.121.76.24	80	a104-121-76-24.deploy.static.akamaitechnologies.com	
10	TCP	131.253.61.84	443	gateway.login.live.com	login.live.com, loginnet.passport.com, msnia.login.live.com, pst.microsoftpassportsupport.net, api.login.live.com, tools.login.live.com, xml.login.live.com, ipv6.login.live.com, nexus.passport.com, login.passport.com, msnialogin.passport.com, gateway.api.live.com, gateway.login.live.com, active.api.live.com, active.login.live.com, g1.login.live.com, g2.login.live.com
11	TCP	23.63.139.27	80	a23-63-139-27.deploy.static.akamaitechnologies.com	
12	TCP	23.63.136.70	443	auth.gfx.ms	clientconfig.passport.net, auth.gfx-int.ms, auth.gfx.ms, clientconfig.passport-int.net
13	TCP	23.60.199.167	443	sdx.microsoft.com	sdx.microsoft.com, fss.live.com, familysafety.live.com, familysafety.microsoft.com
14	TCP	141.30.61.207	1688		KMS TU Dresden
15	TCP	65.52.98.233	443	co2.activation-v2.sls.microsoft.com	
16	TCP	23.57.22.139	443		*.microsoft.com.
17	TCP	64.4.54.116	443	array203-prod.do.dsp.mp.microsoft.com	array203-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com
18	TCP	23.57.18.199	443	geover-prod.do.dsp.mp.microsoft.com	cp201-prod.do.dsp.mp.microsoft.com, disc201-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, kv201-prod.do.dsp.mp.microsoft.com
19	TCP	134.170.104.154	80	dm2301-skpfe.onedrive.live.com	
20	TCP	13.107.4.50	80		Microsoft Azure
21	TCP	157.55.240.220	443	sls.update.microsoft.com	
22	TCP	157.56.77.141	443	sls.update.microsoft.com	
23	TCP	65.55.138.186	443	fe2.update.microsoft.com	
24	TCP	65.52.108.135	443	array102-prod.do.dsp.mp.microsoft.com	array102-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com
25	TCP	104.121.76.33	80	a104-121-76-33.deploy.static.akamaitechnologies.com	
26	TCP	198.78.212.126	80		
27	TCP	8.254.201.30	80		
28	TCP	8.254.201.78	80		
29	TCP	8.27.137.254	80		
30	TCP	64.4.54.98	443	array201-prod.do.dsp.mp.microsoft.com	array201-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com
31	TCP	191.237.208.126	443		
32	TCP	134.170.165.248	443	wdcp.microsoft.com	wdcp.microsoft.com, spynet2.microsoft.com, wdcpalt.microsoft.com, spynetalt.microsoft.com, spynetfrontend-dc1-tip.cloudapp.net, spynetfrontend-dc2-tip.cloudapp.net, spynetfrontend-eas-tip.cloudapp.net, spynetfrontend-sas-tip.cloudapp.net, spynetfrontend-neu-tip.cloudapp.net, spynetfrontend-weu-tip.cloudapp.net, spynetfrontend-bra-tip.cloudapp.net, spynetfrontend-aue-tip.cloudapp.net, spynetfrontend-eus-tip.cloudapp.net, spynetfrontend-wus-
33	TCP	104.121.76.10	80	a104-121-76-10.deploy.static.akamaitechnologies.com	
34	TCP	65.55.138.149	443	sls.update.microsoft.com	
35	TCP	191.234.72.188	443	fe2.update.microsoft.com	
36	TCP	40.77.226.218	443	array402-prod.do.dsp.mp.microsoft.com	array402-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com

Schlussfolgerungen:

- Installation von Windows 10 ohne Zugang zum Internet
- datenarme Konfiguration nur durch administrative Einstellungen möglich
- zusätzlich eigener Time- und Update-Service

- Es ist weiterhin weitestgehend unbekannt, welche Daten im Einzelnen für welche Zwecke an Microsoft übermittelt werden!

- Forderung nach mehr Transparenz
- Forderung nach Privacy-by-Default

TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur Datenschutz und Datensicherheit

Datenschutz-Analyse von Windows 10

5. DFN-Konferenz Datenschutz

Christoph Hofmann, Kilian Becher, Paul Völker

Technische Universität Dresden

Hamburg, 29.11.2016

Pressestimmen - ein Auszug

- „Windows 10 Preview has permission to watch your every move“
  The Inquirer (03.10.14)
- „Windows wird zur Datensammelstelle“
  Heise Online (30.07.15)
- „Windows 10 – Überwachung bis zum letzten Klick“
  Verbraucherzentrale Rheinland-Pfalz (10.08.15)
- „Even when told not to, Windows 10 just can’t stop talking to Microsoft“
  Ars Technica (13.08.15)

Pressestimmen - ein Auszug

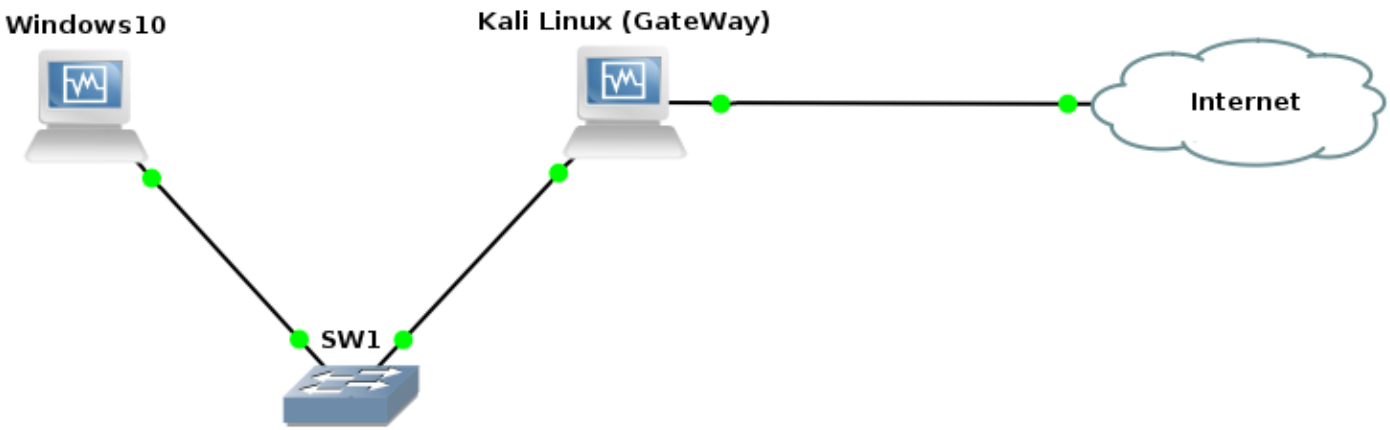
- „Windows 10 Preview has permission to watch your every move“
  The Inquirer (03.10.14)
- „Windows wird zur Datensammelstelle“
  Heise Online (30.07.15)
- „Windows 10 – Überwachung bis zum letzten Klick“
  Verbraucherzentrale Rheinland-Pfalz (10.08.15)
- „Even when told not to, Windows 10 just can’t stop talking to Microsoft“
  Ars Technica (13.08.15)

Ausgangspunkt und Zielsetzung

Zielsetzung:	Bewertung der Datenschutz(un)freundlichkeit von Windows 10 im Kontext der TU Dresden
Ausgangspunkt:	Angepasste Windows 10 LTSB Version nach Vorgaben des AKIF
Vorgehen:	Mitschnitt und Bewertung aller ein- und ausgehenden Kommunikation
Herausforderung:	Viele Verbindungen erfolgen verschlüsselt (TLS/SSL)

Versuchsaufbau

- Aufbrechen der verschlüsselten Kommunikation durch Man-in-the-Middle-Angriff
- Verbindungsaufbau zum Internet über zweiten Rechner der als Router agiert
- Aufbrechen verschlüsselter Kommunikation mittels MITM-Proxy im Router
- Zertifikat des MITM-Proxy als Root-Zertifikat in Windows 10 hinterlegt



Versuchsdurchführung

- Strukturiertes Vorgehen nach festgelegten Szenarien
- Stetige Steigerung der Nutzungsintensität
- Detaillierte Dokumentation von Aktionen und Reaktionen

- 3 Monate aktive Untersuchung
- 30 Einzeltests
- Ca. 10 GB Kommunikation
- Reduziert auf 62 Gruppen

Gruppierung

- Gruppierung nach Domainnamen
- Einstufung nach Bedenklichkeit

Ampelsystem			
Rq	**Rs**	**Bedeutung**	**Einstufungskriterien**
		Unbedenklich	Klar erkennbarer Nutzen, keine bzw. kaum Profilierung möglich
		Wenig bedenklich	Klar erkennbarer Nutzen, Potential zur Profilierung gegeben (z.B. Cookies)
		Bedenklich	Aussage schwierig, möglicherweise nützlich, großes Potential zur Profilierung (z.B. wiederkehrende IDs)
		Sehr bedenklich	Mutmaßlich für Profilierung, kein Nutzen erkennbar bzw. anderweitige ernste Gefahren

Traces - Ausschnitt

Gruppierte Traces			
Rq	**Rs**	**Domain**	**Begründung**
		officeclient.microsoft.com	Nützlich, keine Profilierung möglich
		fs.microsoft.com	Nützlich, keine Profilierung möglich
		ctldl.windowsupdate.com	Nützlich, keine Profilierung möglich
		sls.update.microsoft.com	Request unauffällig, Response inhaltlich nicht verständlich, verdeckter Kanal möglich
		msftncsi.com	Nützlich, keine Profilierung möglich
		go.microsoft.com	Erkennbarer Nutzen, kann für Angriffe genutzt werden (Forwarding umlenken), kann Firewallregeln etc. umgehen durch flexibles Forwarding; unnötiges Senden von Informationen obwohl nur Forwarding-Request, ohne Verschlüsselung
		dmd.metaservices.microsoft.com	Request mit hardwarebezogenen IDs, Senden bei Änderung der angesteckten Hardware, Zweck möglicherweise in Kompatibilität und Versorgung mit passenden Treibern

Kritische Kommunikationen

telecommand.telemetry.microsoft.com

Persistente Cookies, IDs und Systemkonfigurationen im Request
⇒ Eindeutige Identifizierung möglich

dmd.metaservices.microsoft.com

Viele Hardwareinformationen und Hardwareveränderungen
⇒ Kann erforderlich sein bspw. für automatische Treiberinstallation

go.microsoft.com

keine kritischen Daten, aber beliebige Weiterleitungen
⇒ Kann für die Umgehung von Firewall-Regeln genutzt werden

Kritische Kommunikationen

bing.com

Persistente Cookies und IDs,
Nicht verständliche Daten (z.b. Cortana-Manifest)
$\Rightarrow$ Eindeutige Identifizierung möglich

vortex.data.microsoft.com

Teils Unauffällige Daten
Teils Datensicherheitskritisch (z.b. Liste besuchter Webadressen)

Zusammenfassung und Empfehlung

- Erheblich reduzierte Kommunikation in Enterprise LTSB mit entsprechenden Einstellungen
- Evtl. Blockieren: (mglw. Einschränkungen in Kauf nehmen!)
  - telecommand.telemetry.microsoft.com
  - dmd.metaservice.microsoft.com
  - vortex.data.microsoft.com
- Updates über eigenen zentralen Server (CDN)

Zusammenfassung und Empfehlung

- Erheblich reduzierte Kommunikation in Enterprise LTSB mit entsprechenden Einstellungen
- Evtl. Blockieren: (mglw. Einschränkungen in Kauf nehmen!)
  - telecommand.telemetry.microsoft.com
  - dmd.metaservice.microsoft.com
  - vortex.data.microsoft.com
- Updates über eigenen zentralen Server (CDN)

$\Rightarrow$ Ergebnis: Einsatz vertretbar

Windows 10 Home / Pro

- Deutlich erhöhtes Kommunikationsaufkommen
- Viele neue Dienste und Kommunikationspartner

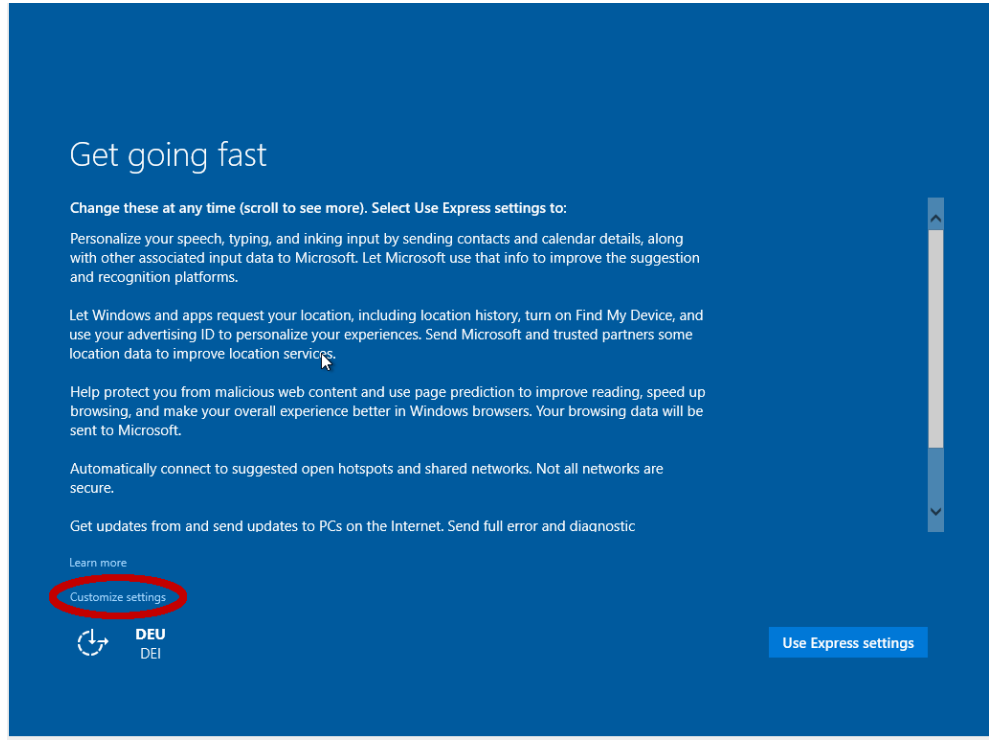
Windows 10 Home / Pro

- Deutlich erhöhtes Kommunikationsaufkommen
- Viele neue Dienste und Kommunikationspartner
- Bei Nutzung eines Microsoft Online-Kontos wird das Passwort bei Erstanmeldung und Fehleingabe ungehasht übertragen!

```
<wsse:Security>
    <wsse:UsernameToken wsu:Id="user">
        <wsse:Username>[redacted]@outlook.de</wsse:Username>
        <wsse:Password>AAbbcc!!2233</wsse:Password>
        <wsse:LoginOption>16908291</wsse:LoginOption>
    </wsse:UsernameToken>
    <wsu:Timestamp wsu:Id="Timestamp">
        <wsu:Created>2016-06-01T09:17:53Z</wsu:Created>
        <wsu:Expires>2016-06-01T09:22:53Z</wsu:Expires>
    </wsu:Timestamp>
</wsse:Security>
```

Fazit

- Benutzerdefinierte Installation
- Feedbackhäufigkeit auf „Nie“
- Regler für Datenschutzeinstellungen auf „Aus“
  - Regelmäßig überprüfen



Vielen Dank für die Aufmerksamkeit

Fragen?

christoph.hofmann@tu-dresden.de