TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur Datenschutz und Datensicherheit

Datenschutz-Analyse von Windows 10

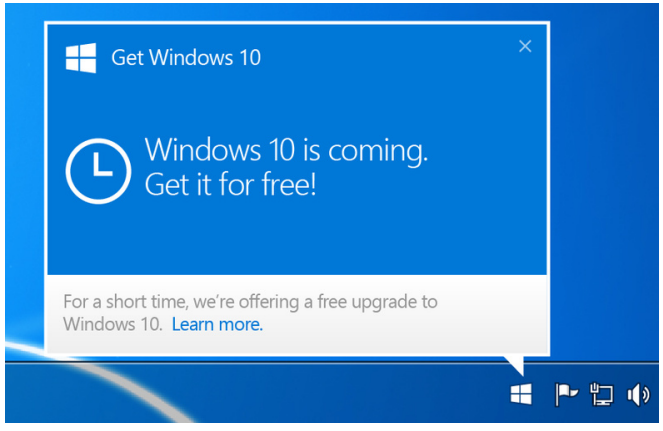
Kilian Becher, Christoph Hofmann, Paul Völker
Technische Universität Dresden

Dresden, 09.06.2016

Übersicht

Motivation

- Microsofts neues Betriebssystem Windows 10
- Offensive Verbreitung seitens Microsoft
- Allgemeine Datenschutzbedenken
  - Neue Funktionen
  - Neue Datenschutzrichtlinien
- Büroeinsatz an der TU Dresden vertretbar?
- Zusätzlich: Untersuchung der Home / Pro Edition



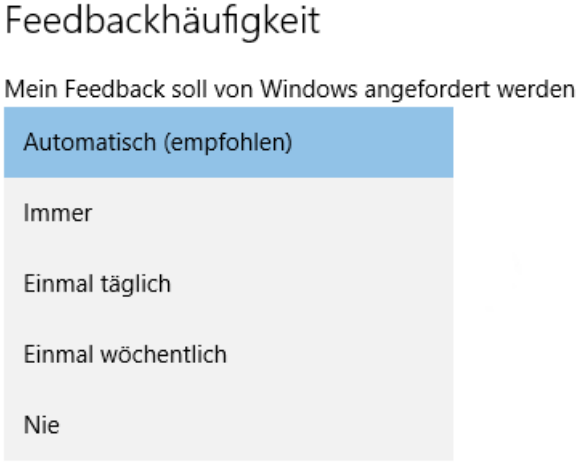
Pressestimmen - ein Auszug

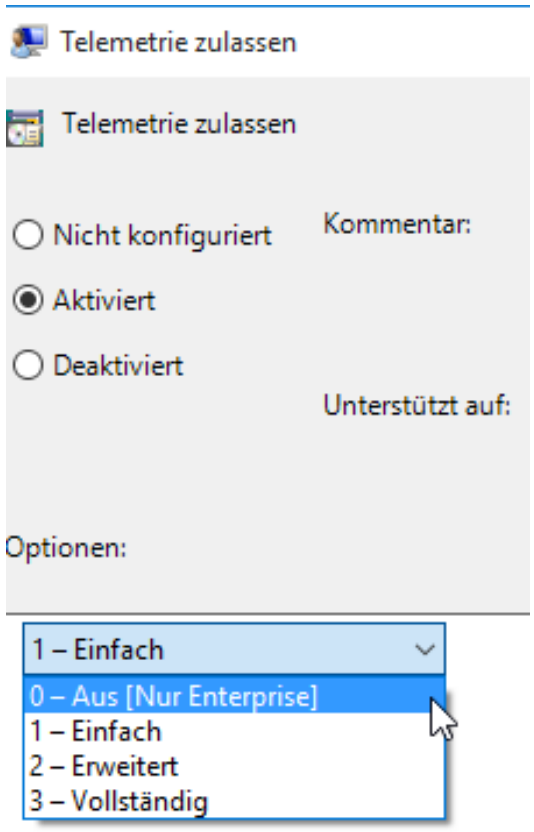
- „Windows 10 Preview has permission to watch your every move“
  The Inquirer (03.10.14)
- „Windows wird zur Datensammelstelle“
  Heise Online (30.07.15)
- „Windows 10 – Überwachung bis zum letzten Klick“
  Verbraucherzentrale Rheinland-Pfalz (10.08.15)
- „Even when told not to, Windows 10 just can’t stop talking to Microsoft“
  Ars Technica (13.08.15)
- „Verbraucherschützer verklagen Microsoft“
  Heise Online (29.02.16)

Pressestimmen - Nutzerprofilierung

Windows 10 Enterprise LTSB

- Zugang zu Long Term Servicing Branch
- Nur wichtige Updates, 10 Jahre Support
- Kein Cortana, kein Edge
  - Besonders im Fokus
- Feedback vollständig deaktivierbar



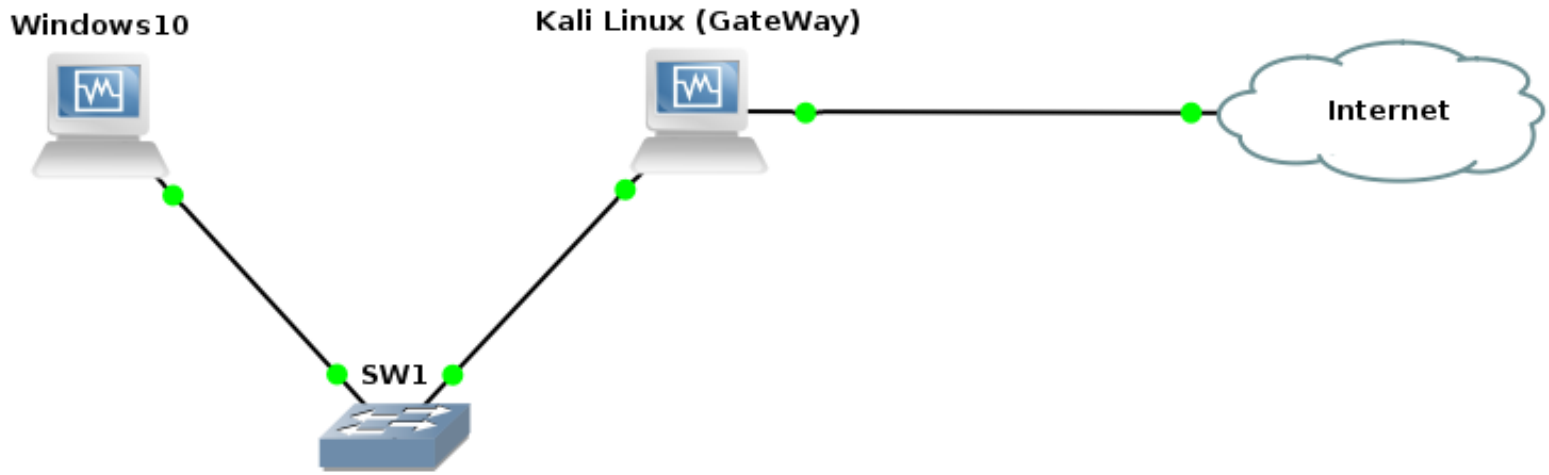


Versuchsaufbau - Umsetzung

- Wireshark
- Burp-Suite (MitM-Proxy)

- Kali Linux:
  - Dnsmasq
  - IPtables

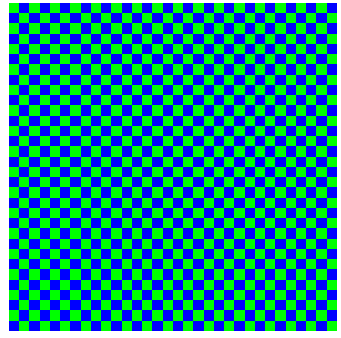
- Virtuelle Maschinen
- Hardwaretest



Versuchsdurchführung - Konventionen

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

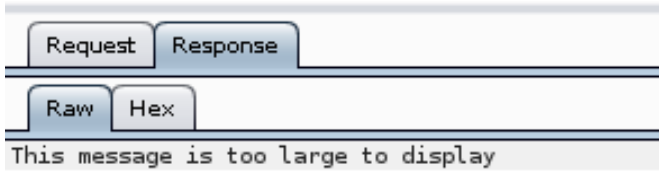
Verwendete Nutzerdaten	
Benutzername	AABBCC112233KCP
Kennwort	aabbcc
Kennworthinweis	Ersten 6 Zeichen klein



Live Demo

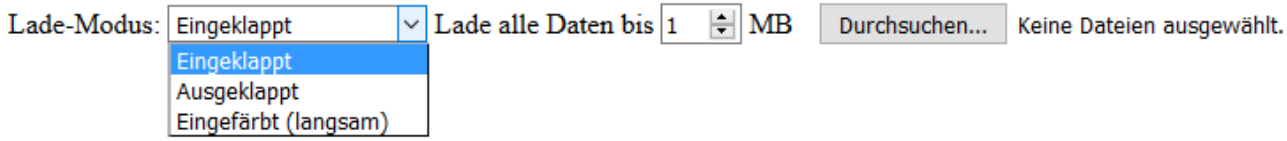
Einschränkungen des Versuchsaufbaus

- Burp Suite Free Version mit Einschränkungen → VisualizerTool
- Fehlverhalten bei schwachen Ressourcen → Erhöhung der Ressourcen
- Einschränkungen bei großen Downloads (z.B. Windows Updates)
- Sinn oder genaue Bedeutung von Hashes und IDs oft unklar



Analyse - Visualisierungstool

+ Bessere Suche
+ Vergleichbarkeit
+ Keine Beschränkung der Post-Daten
+ Formatierung und Highlighting
– Begrenzung auf 256 MB Dateien



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	Vermutlich zum Zweck von Profilierung bzw. anderweitige ernste Gefahren

Ergebnisse - Traces

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
⇒ Eindeutige Identifizierung möglich

dmd.metaservices.microsoft.com

Viele Hardwareinformationen und Hardwareveränderungen
⇒ Könnte erforderlich sein

go.microsoft.com

Weiterleitung
keine kritischen Daten
⇒ Kann für die Umgehung von Firewall-Regeln genutzt werden

Kritische Kommunikationen

telecommand.telemetry.microsoft.com

Persistente Cookies, IDs und Systemkonfigurationen
⇒ Eindeutige Identifizierung möglich

dmd.metaservices.microsoft.com

Viele Hardwareinformationen und Hardwareveränderungen
⇒ Könnte erforderlich sein

go.microsoft.com

Weiterleitung
keine kritischen Daten
⇒ Kann für die Umgehung von Firewall-Regeln genutzt werden

Kritische Kommunikationen

bing.com

Persistente Cookies und IDs,
Nicht verständliche Daten (Bsp. Cortana-Manifest)
⇒ Eindeutige Identifizierung möglich

login.live.com/ppsecure/deviceaddcredential.srf

Daten nicht verständliche
Zweck nicht ersichtlich

vortex.data.microsoft.com

Unauffällige Daten
Einmal Datensicherheitskritisch

Kritische Kommunikationen

bing.com

Persistente Cookies und IDs,
Nicht verständliche Daten (Bsp. Cortana-Manifest)
⇒ Eindeutige Identifizierung möglich

login.live.com/ppsecure/deviceaddcredential.srf

Daten nicht verständliche
Zweck nicht ersichtlich

vortex.data.microsoft.com

Unauffällige Daten
Einmal Datensicherheitskritisch

Kritische Kommunikationen

bing.com

Persistente Cookies und IDs,
Nicht verständliche Daten (Bsp. Cortana-Manifest)
⇒ Eindeutige Identifizierung möglich

login.live.com/ppsecure/deviceaddcredential.srf

Daten nicht verständliche
Zweck nicht ersichtlich

vortex.data.microsoft.com

Unauffällige Daten
Einmal Datensicherheitskritisch

Auffälligkeiten

- Nicht reproduzierbare Kommunikationen
- Scheint ineffizient
  - Forwarding
  - Doppelte IDs im Header
  - Erneutes Senden von Nachrichten

Zusammenfassung

- 3 Monate aktive Untersuchung
- Längster Test 1 Woche
- 30 Einzeltests
- Ca. 10 GB Daten
- Reduziert auf 62 Gruppen

Zusammenfassung

- Weniger Kommunikation in Enterprise LTSB
- Blockieren:
  - telecommand.telemetry.microsoft.com
  - dmd.metaservice.microsoft.com
  - vortex.data.microsoft.com
- Updates über zentralen Server (CDN)

Zusammenfassung

- Weniger Kommunikation in Enterprise LTSB
- Blockieren:
  - telecommand.telemetry.microsoft.com
  - dmd.metaservice.microsoft.com
  - vortex.data.microsoft.com
- Updates über zentralen Server (CDN)

$\Rightarrow$ Ergebnis: Einsatz vertretbar

Live Demo

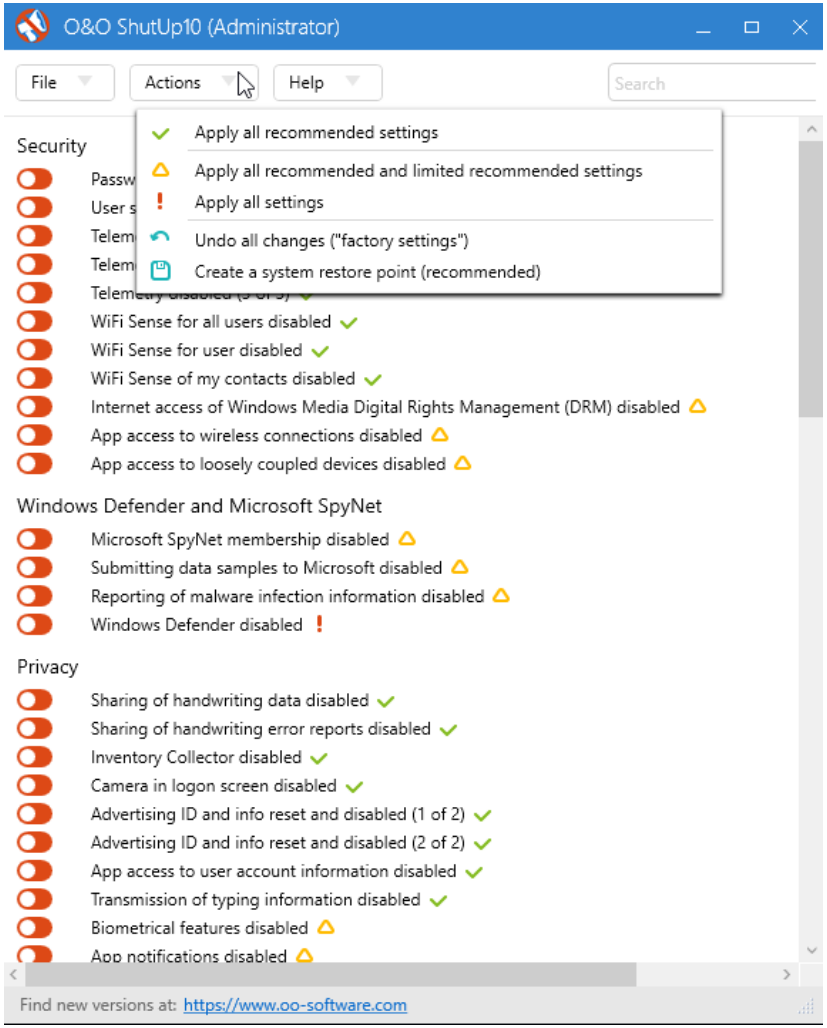
Windows 10 Home / Pro

Windows 10 Home bzw. Pro Edition Untersuchung

- Bei Windows 10 Home / Pro kommen deutlich mehr Pakete und viele neue Dienste
- Passwort wird im Klartext bei Erstanmeldung mit MS-Online-Konto und bei Fehleingabe (Vertipper!!) übertragen

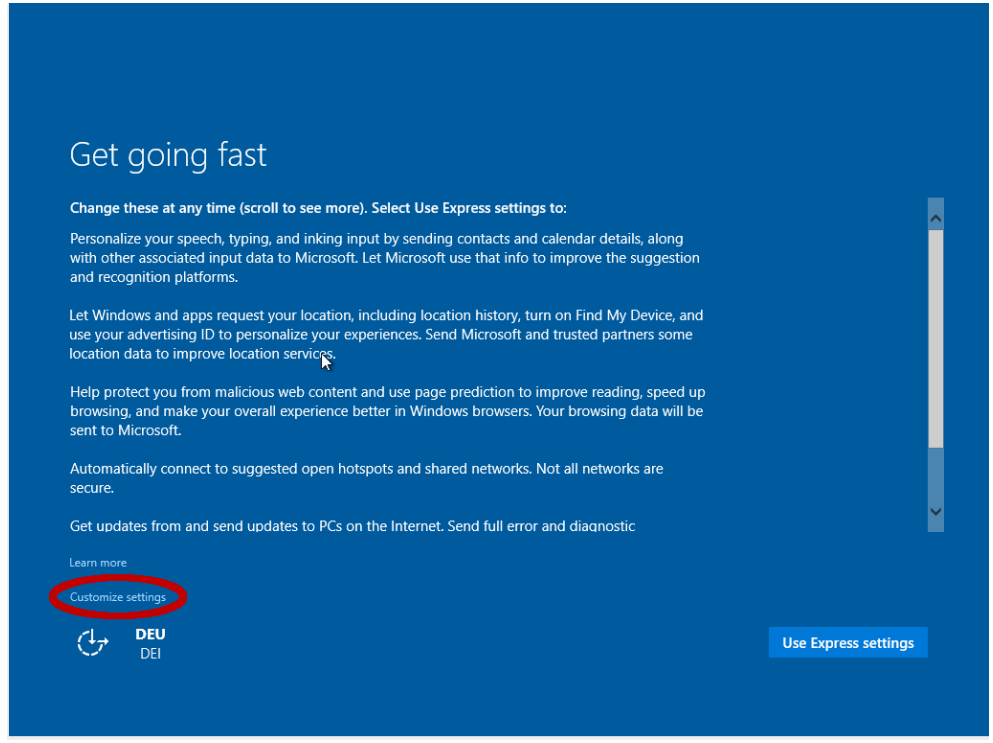
ShutUp 10 von O&O Software

- Alle Einstellungen auf einen Blick
- Verschiedene Einstellungsstufen
- Einstellungen Importier- und Exportierbar
- **Tipp**: Als Administrator starten und ab und zu auf Änderungen kontrollieren (mglws. Autostart?)
- **Achtung**: Systemwiederherstellungspunkt erstellen!



Fazit

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



Ausblick

Viele weitere Untersuchungen möglich

- Mehr Testrechner
- Langzeittests
- Andere Windows-Versionen
- Anti-Spy-Tools?
- Windows 7 und 8.1?
- Apple und Google?

Fragen?