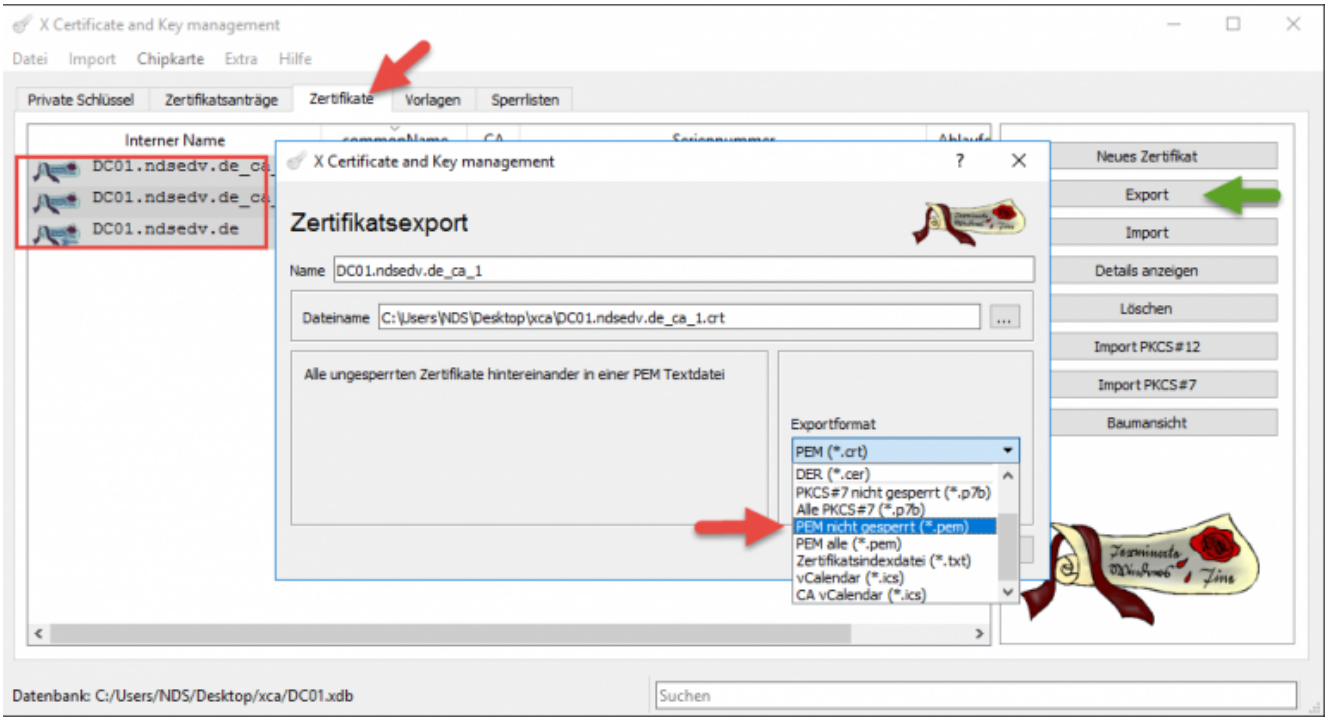


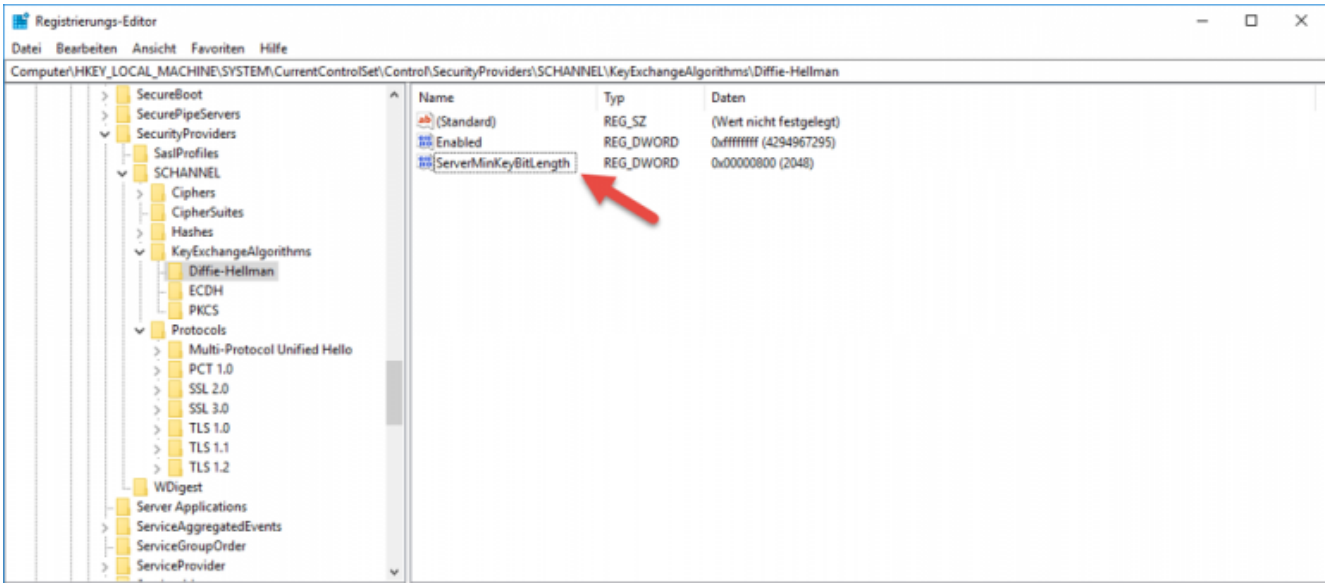
Konvertieren eines .pfx Zertifikat in .pem

PFX to PEM

Das Ziel ist die Erstellung eines Zertifikats im PEM Format. Als Basis dient ein exportiertes Privates Zertifikat von einem Windows Server.

In dieser Anleitung wird eine ganze Zertifikatskette in ein PEM Format konvertiert.

Konvertieren eines .pfx Zertifikat in .pem



TLS 1.2 Diffie-Hellman Key Length

Diffie-Hellman Schlüssellänge

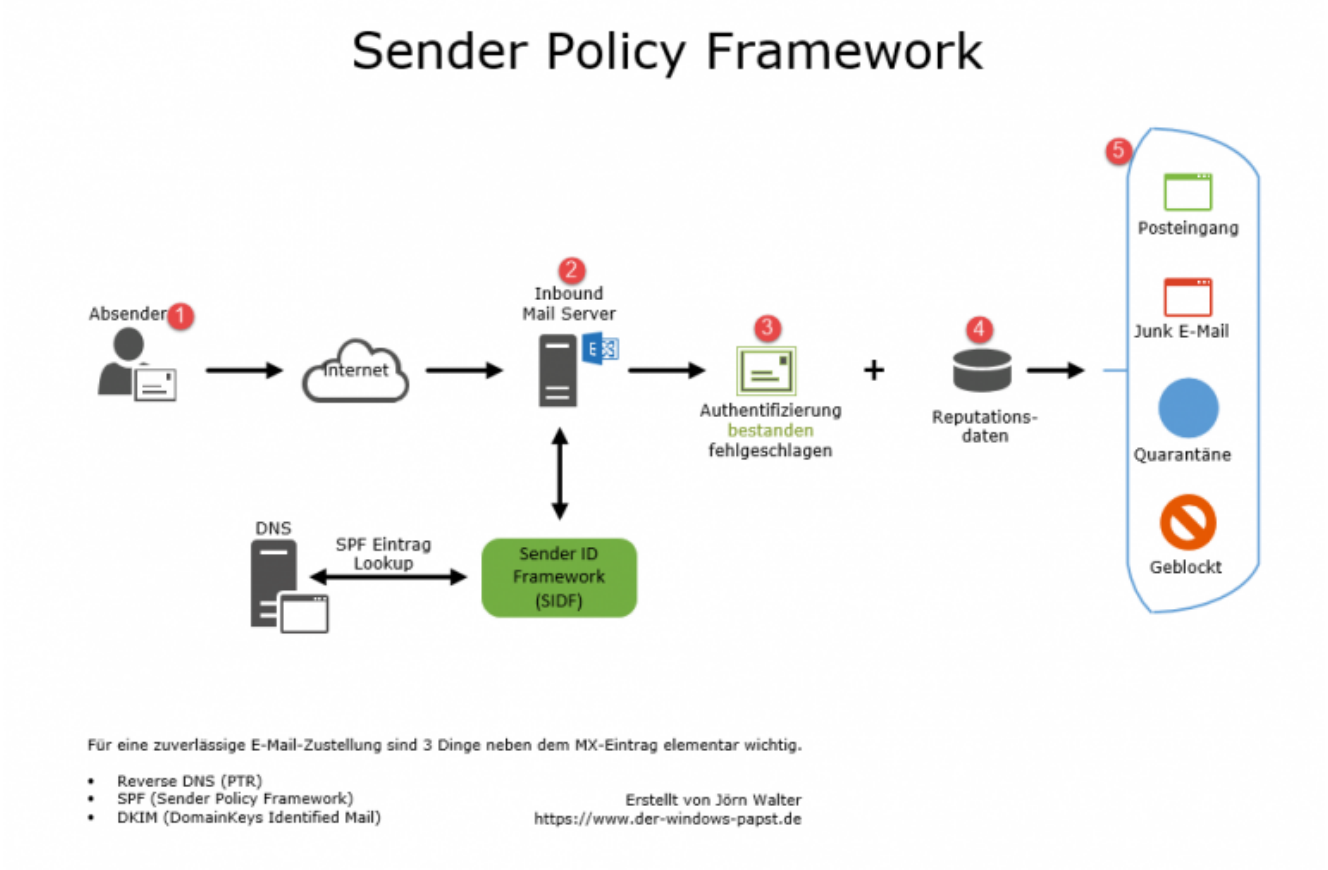
Wer den Key-Exchange-Algorithmus „DH” einsetzt sollte darauf achten, dass die minimale Schlüssellänge auf 2048 Bit eingestellt ist.

Mögliche Schlüssellängen sind: 1024, 2048, 3072 und 4096

Über einen zusätzlichen Registrierungseintrag lässt sich das Verhalten steuern.

Öffnen die Registry und navigieren zu:

TLS 1.2 Diffie-Hellman Key Length



Sender ID Framework (SDIF)

SPF (Sender Policy Framework)

Das SPF (Sender Policy Framework) ist ein Verfahren zur Sender-Authentifizierung und räumt dem empfangenden Mailserver die Möglichkeit ein, zu überprüfen, ob die E-Mail tatsächlich von einem berechtigten Mailserver (Absender) stammt oder nicht. Der Domaininhaber bestimmt durch einen Eintrag in seiner DNS Zone wer als valider Absender infrage kommt.

Hinweis: Ein SPF schützt nicht vor Spam.

Sender ID Framework (SDIF)

Sicher verschlüsseln mit Bitlocker

Verschlüsselung ist nicht alles, aber ohne Verschlüsselung ist alles nichts

Die Bitlocker Laufwerksverschlüsselung ist ein in Windows integriertes Feature, das Daten vor Bedrohungen durch Datendiebstahl oder durch Offenlegung verlorener, gestohlener oder nicht ordnungsgemäß außer Betrieb gesetzter Computer schützen soll.

Der Schutz von Festplatteninformationen gehört ja mittlerweile zum Standard, sei es im Server- oder Clientumfeld.

Clientsysteme gehören für mein Ve

rständnis immer geschützt, egal ob es sich dabei um eine Workstation oder ein Notebook handelt. Auch Serversysteme in lokalen Niederlassungen, ohne Anbindung an ein Rechenzentrum, gehören abgesichert.

Was benötigen wir für eine Verschlüsselung mit Bitlocker?

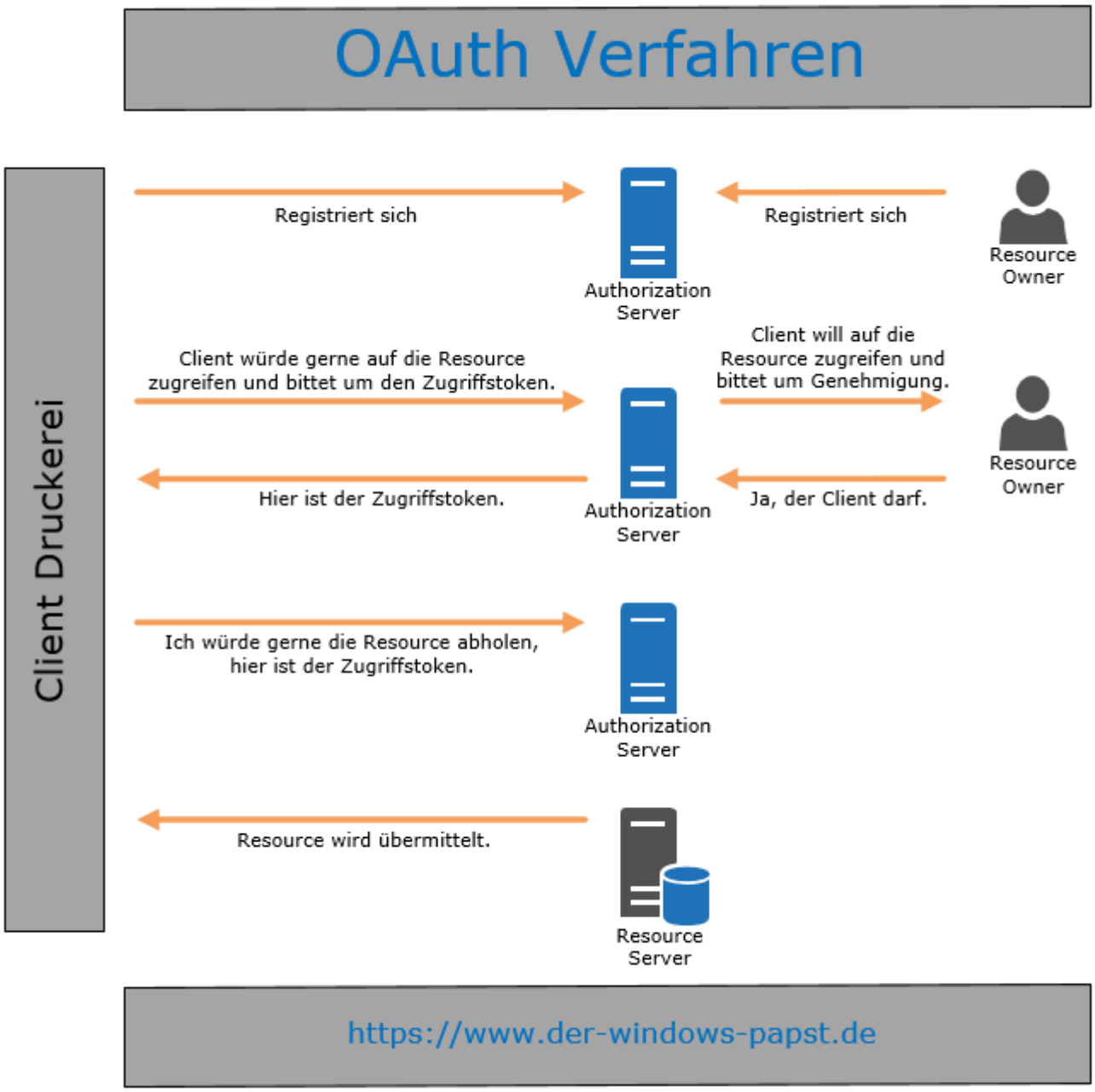
Es gibt heute kaum noch ein Businessgerät, in dem kein TPM-Modul verbaut ist. TPM steht für (Trusted Platform Module) und überwacht die integrierte Hardware in einem Computer. Sollte die mit Bitlocker verschlüsselte Festplatte ausgebaut werden, wird diese ihren Dienst in einem anderen Computer verweigern. Denn die verschlüsselte Festplatte benötigt für die Entschlüsselung, das TPM Modul mit dem diese auch verschlüsselt wurde.

Wie prüfen wir denn ob ein TPM Modul verbaut ist?

Über die CMD führen wir den Befehl tpm.msc aus:

[Sicher verschlüsseln mit Bitlocker]

https://www.der-windows-papst.de/2018/01/06/windows-bitlocker-benutzer-handbuch-user-guide/



Was ist LDAP und was ist OAuth 2.0

LDAP und Open Authorization

In diesem Dokument beschreibe ich was LDAP und OAuth ist und wofür es eingesetzt wird.

Ein kurzer Einblick…

LDAP ist ein offenes und plattformübergreifendes Protokoll für die Verzeichnis-Dienste-Authentifizierung. LDAP stellt eine Kommunikationssprache bereit, die Anwendungen verwenden, um mit Verzeichnisdiensten zu kommunizieren.

OAuth ist ebenfalls ein offenes aber Token basiertes standarisiertes Protokoll. OAuth erlaubt eine sichere Autorisierung und Authentifizierung beim Einsatz von Desktop-, Web- und API- basierten Anwendungen.

Authentisierung = Ist der Nachweis einer Identität
Authentifizierung = Bestätigung der Identität
Autorisierung = ist eine Berechtigung

LDAP & OAuth 2.0

Security für Windows 10 – Registry

Hacks

Security Registry Hacks

Mit diesen Registry Hacks lassen sich folgende Sicherheitseinstellungen vornehmen:

Enable DEP and isolation in Internet Explorer

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main" /v "DEPOff" /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main" /v "Isolation64Bit" /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable SSLv3 fallback, and the ability to ingore certificate errors, in Internet Explorer

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings" /v "CallLegacyWCMPolicies" /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings" /v "EnableSSL3Fallback" /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings" /v "PreventIgnoreCertErrors" /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable Flash Player in Edge

```
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\MicrosoftEdge\Addons” /v “FlashPlayerEnabled” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Addons” /v “FlashPlayerEnabled” /t REG_DWORD /d 0 /f
```

Hack anzeigen

Enable Edge Phising Filter

```
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter” /v “EnabledV9” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter” /v “EnabledV9” /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable and configure Windows Remote Desktop and Remote Desktop Services

```
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Terminal Services” /v “AllowSignedFiles” /t REG_DWORD /d 0 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Terminal Services” /v “AllowUnsignedFiles” /t REG_DWORD /d 0 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows NT\Terminal Services” /v “DisablePasswordSaving” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Conferencing” /v “NoRDS” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS” /v “AllowRemoteShellAccess” /t REG_DWORD /d 0 /f
```

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “AllowSignedFiles” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “AllowUnsignedFiles” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “CreateEncryptedOnlyTickets” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “DisablePasswordSaving” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “fAllowToGetHelp” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “fAllowUnsolicited” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services” /v “fDenyTSConnections” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client” /v “fEnableUsbBlockDeviceBySetupClass” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client” /v “fEnableUsbNoAckIsochWriteToDevice” /t REG_DWORD /d 80 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client” /v “fEnableUsbSelectDeviceByInterface” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\RemoteAdminSettings” /v “Enabled” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Services\RemoteDesktop” /v “Enabled” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Services\UPnPFramework” /v “Enabled” /t REG_DWORD /d 0 /f
```

Hack anzeigen

Block Macros and other Content Execution for Office 2016

```
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\access\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\excel\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\excel\security” /v “blockcontentexecutionfrominternet” /t REG_DWORD /d 1 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\excel\security” /v “excelbypassencryptedmacroscan” /t REG_DWORD /d 0 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\ms project\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\ms project\security” /v “level” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\outlook\security” /v “level” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\powerpoint\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\powerpoint\security” /v “blockcontentexecutionfrominternet” /t REG_DWORD /d 1 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\publisher\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\visio\security” /v
```

“vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\visio\security” /v “blockcontentexecutionfrominternet” /t REG_DWORD /d 1 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\word\security” /v “vbawarnings” /t REG_DWORD /d 4 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\word\security” /v “blockcontentexecutionfrominternet” /t REG_DWORD /d 1 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\word\security” /v “wordbypassencryptedmacroscan” /t REG_DWORD /d 0 /f
reg add “HKEY_CURRENT_USER\Software\Policies\Microsoft\office\common\security” /v “automationsecurity” /t REG_DWORD /d 3 /f

Hack anzeigen
Enable Automatic Updates for Office

reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\16.0\common\officeupdate” /v “enableautomaticupdates” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\16.0\common\officeupdate” /v “hideenabledisableupdates” /t REG_DWORD /d 1 /f

Hack anzeigen
Enable Enhanced Face Spoofing Protection

reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatu

```
res" /v "EnhancedAntiSpoofing" /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable Pushing of Apps for Installation from the Windows Store

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PushToInstall" /v "DisablePushToInstall" /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable Projecting (Connect) to the Device, and require a PIN for pairing

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent" /v "AllowProjectionToPC" /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent" /v "RequirePinForPairing" /t REG_DWORD /d 1 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WirelessDisplay" /v "EnforcePinBasedPairing" /t REG_DWORD /d 1 /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\PresentationSettings" /v "NoPresentationSettings" /t REG_DWORD /d 1 /f
```

Hack anzeigen

Force enable Data Execution Prevention (DEP)

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer" /v "NoDataExecutionPrevention" /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System" /v
```

“DisableHHDEP” /t REG_DWORD /d 0 /f

Hack anzeigen

Disable Autorun

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” /v “NoAutorun” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” /v “NoDriveTypeAutoRun” /t REG_DWORD /d 255 /f
```

Hack anzeigen

Disable Active Desktop

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” /v “ForceActiveDesktopOn” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” /v “NoActiveDesktop” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” /v “NoActiveDesktopChanges” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop” /v “NoAddingComponents” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop” /v “NoComponents” /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable Desktop Gadgets

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar” /v “TurnOffSidebar” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar” /v “TurnOffUnsignedGadgets” /t REG_DWORD /d 1 /f
```

Hack anzeigen

Force Process digital Certificates when running Executables

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers” /v “authenticodeenabled” /t REG_DWORD /d 1 /f
```

Hack anzeigen

Disable Picture Passwords

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System” /v “BlockDomainPicturePassword” /t REG_DWORD /d 1 /f
```

Hack anzeigen

Enable SmartScreen

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System” /v “EnableSmartScreen” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System” /v
```

```
“ShellSmartScreenLevel” /t REG_SZ /d “Warn” /f
```

Hack anzeigen

Disable Windows Update deferrals

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate” /v “DeferFeatureUpdates” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate” /v “DeferQualityUpdates” /t REG_DWORD /d 0 /f
```

Hack anzeigen

Enable Windows Defender

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” /v “DisableAntiSpyware” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” /v “ServiceKeepAlive” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableIOAVProtection” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableRealtimeMonitoring” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan” /v “CheckForSignaturesBeforeRunningScan” /t REG_DWORD /d 1 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan” /v “DisableHeuristics” /t REG_DWORD /d 0 /f
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Polici
```

es\Attachments” /v “ScanWithAntiVirus” /t REG_DWORD /d 3 /f

Hack anzeigen

Do not allow Users and Apps to connect to Malicious Websites

reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection” /v “EnableNetworkProtection” /t REG_DWORD /d 1 /f

Hack anzeigen