NETSEC.CO
THE NETWORK SECURITY COMPANY

Secure Client mit Always On VPN

White Paper

AUTOR	Thomas Gusset
TYP	technische Dokumentation
ABSTRACT	Konzept und Blueprint Umsetzung One Client Strategie mit Microsoft Always On VPN und Windows Bordmitteln
STATUS	Final
SPRACHE	german
VERTRAULICHKEIT	C0 - öffentlich
VERSION	2.0
DOKUMENT ID	XZ7T7MFERA7N-791038266-77

Inhaltsverzeichnis

Kurzfassung

Homeoffice wurde in der Corona Krise von vielen Firmen und Organisationen eingeführt und wird auch in Zukunft eine wichtige Rolle spielen. Die Anzahl Mitarbeitende, die ausserhalb des Firmennetzwerkes arbeiten, hat stark zugenommen. Viele Firmen setzen dabei auf mobile Endgeräte, mit denen ihre Mitarbeitende auch im Homeoffice und unterwegs komfortabel arbeiten können.

Mit einer **One Client Strategie** braucht es dafür keine zusätzlichen Geräte. Die Mitarbeitenden erhalten ein Notebook, mit dem sie sowohl im Büro als auch mobil arbeiten können. Im Büro werden Monitore und Peripherie über einen USB-C Port Replikator mit einem einzigen Kabel angeschlossen. Die Netzwerkanbindung erfolgt dabei direkt über LAN. Wird der Client mobil genutzt, erfolgt eine automatische Anbindung über *Always On VPN*, sobald das Gerät mit dem Internet verbunden ist. Sämtlicher Netzwerkverkehr wird dabei über den VPN Tunnel geroutet, so dass die Sicherheitseinrichtungen im Firmennetzwerk nicht umgangen werden.

Der mobile Client ist mit *Bitlocker* und *Windows Firewall* so abgesichert, dass im mobilen Betrieb derselbe Schutzlevel erreicht wird, wie beim Betrieb im Firmennetzwerk. Die Authentifizierung am VPN-Server erfolgt über ein an die TPM des Endgeräts gebundenes Benutzerzertifikat. Optional kann mit *Windows Hello for Business* eine passwortlose Authentifizierung am Gerät implementiert werden, wodurch die Sicherheit weiter erhöht wird.

Ausgangslage

Homeoffice hat an Bedeutung gewonnen, Arbeiten an verschiedenen Orten ist im Trend. Daher muss ein digitaler Arbeitsplatz heute komfortables Arbeiten sowohl im Büro und auch ausserhalb der Firma ermöglichen. Dabei sind insbesondere auch hohe Anforderungen an die Sicherheit zu erfüllen.

In vielen IT-Umgebungen wird einerseits mit typischen Client/Server-Anwendungen gearbeitet, bei denen die Daten auf einem Backendsystem liegen. Andererseits wird direkt mit Dateien gearbeitet, die entweder auf internen Fileservern liegen oder auf Cloud-Speichern wie OneDrive oder SharePoint.

Ein modernes Sicherheitsdispositiv, welches das Firmennetzwerk schützt, setzt einerseits auf *Endpoint Protection* und andererseits auf Edge Firewalls mit *content filtering*. Oft werden auch *Proxies* verwendet, um auf das Internet zuzugreifen. IDS/IDP/XDR-Systeme dienen der Erkennung oder Verhinderung von Angriffen. Alle diese Schutzmassnahmen bedingen einen Zugriff auf den Netzwerkverkehr der Clients.

One Client Strategie

Idee

Das Ziel einer **One Client Strategie** ist es, dass pro Mitarbeitendem nur ein Endgerät benötigt wird. Dieses Gerät wird sowohl im Büro als auch beim Arbeiten ausserhalb der Firma verwendet.

Umsetzung mit Windows Bordmitteln

In vielen Betrieben sind heute sowohl im Server- als auch im Client-Bereich Microsoft Windows Systeme im Einsatz. Da drängt sich ein Ansatz auf, der auf die bereits im Einsatz stehenden Systeme aufsetzt und keine zusätzlichen Lizenzen benötigt.

Basierend auf einem mobilen Gerät (Notebook) wurde daher ein Windows 10 Client entwickelt, der sowohl im internen Netzwerk als auch mobil (Homeoffice, ...) verwendet werden kann. Für den Nutzer spielt es keine Rolle, wo er arbeitet. Im Büro wird das Notebook über ein lokales Netzwerk angebunden. Sobald das Gerät extern betrieben wird, baut es einen VPN Tunnel auf und ist dadurch logisch auch wieder im Firmennetzwerk. Das Ganze erfolgt transparent, der Benutzer muss nicht explizit eine VPN Verbindung aufbauen.

Die im internen Netzwerk etablierten Sicherheitskomponenten müssen auch im VPN Betrieb aktiv sein, weshalb der der gesamte Netzwerkverkehr inkl. Internetzugriff durch den VPN Tunnel geleitet wird.

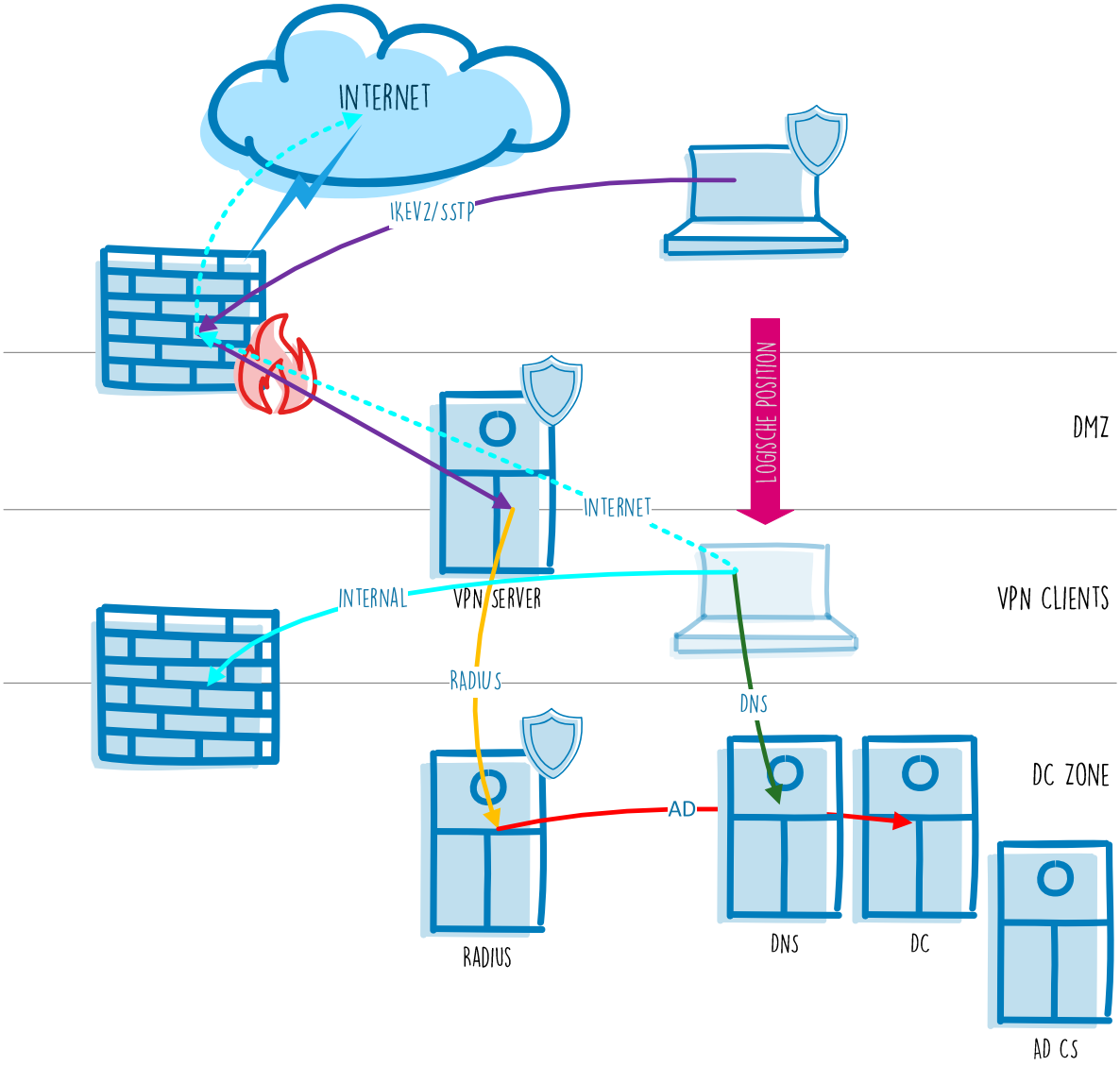

Abbildung 1 - Always On VPN Infrastruktur mit Windows Bordmitteln

Herausforderungen

Anwenderfreundlichkeit hat bei solchen Projekten eine hohe Priorität. Der Nutzer soll möglichst nichts merken von der verwendeten Technologie. Er soll immer gleich arbeiten können, unabhängig vom Arbeitsort. Dabei muss der Zugriff auf Daten und Applikationen immer gewährleistet sein.

Die *Always On VPN* Technologie baut die Verbindung ohne Zutun des Benutzers bei Bedarf auf. Das bedeutet aber auf der anderen Seite auch, dass es keine zusätzliche starke Authentifizierung beim Aufbau der VPN Verbindung gibt. Folglich muss der Zugriff auf den mobilen Client ausreichend geschützt werden. Da mit modernen Technologien wie OneDrive, Teams und SharePoint immer mehr lokale Kopien von Daten auf dem Client liegen, ist dies aber ohnehin ein Gebot der Stunde.

Technologie

VPN

Als VPN Technologie wird Microsoft *Always On VPN* (AoVPN) eingesetzt. AoVPN kann verschiedene VPN Protokolle nutzen und ist in Windows 10/11 integriert. Es gibt zwei Typen von VPN Tunnels. Der *user tunnel* ist an einen Benutzer gebunden und wird erst aktiviert, wenn sich der Benutzer angemeldet hat. Der *device tunnel* wird unabhängig vom Benutzer aufgebaut und kommt z.B. zum Einsatz, wenn das *onboarding* des Benutzers nicht im lokalen Firmennetzwerk erfolgen kann. Im *always on* Modus wird die VPN Verbindung automatisch ohne Zutun des Benutzers aufgebaut.

VPN Protokolle

Der AoVPN Client unterstützt verschiedene Protokolle, wobei IKEv2 als offener Standard als auch SSTP als proprietäres Microsoft Protokoll in Frage kommen.

IKEv2 verwendet IPSec (ISAKMP und ESP) als Tunnelprotokoll und ist dadurch sehr effizient. Da der Client in der Regel hinter einer NAT Firewall steht, wird *ESP over UDP* verwendet. Dabei werden die ESP Pakete in UDP Paketen gekapselt vom VPN Client zum VPN Server übertragen. IKEv2 unterstützt *mobility*, wodurch Unterbrüche bei der Netzwerkverbindung oder *roaming* z.B. zwischen LAN und WLAN oder mobile Internet nicht zu Unterbrüchen der VPN Verbindung führen.

SSTP ist *PPP over TLS*. Die IP-Pakete, die durch den VPN Tunnel transportiert werden müssen, werden dabei in einem TLS Stream übertragen, was zu zusätzlichem Overhead führt. Es können *cipher suites* mit hohem Sicherheitslevel eingesetzt werden, da keine Rücksicht auf ältere Betriebssysteme oder Browser genommen werden muss.

Eine gängige Strategie ist es, IKEv2 als Standardprotokoll zu nutzen und SSTP als Alternative (*fallback*), falls die Verbindung über IKEv2 nicht möglich ist (was z.B. bei public WLANs in Hotels oder anderen öffentlichen Orten vorkommen kann).

VPN-Server

Wird IKEv2 verwendet, können auch VPN-Server von Drittherstellern verwendet werden. Mit der RRAS Rolle des Windows Servers kann ein stabiler und skalierbarer VPN-Server mit Windows Bordmitteln realisiert werden, der sowohl IKEv2 als auch SSTP unterstützt.

Wird der Server hinter einer Edge Firewall betrieben und ausreichend gehärtet, kann ein hoher Sicherheitslevel erreicht werden. Unter Verwendung des in Windows Server integrierten *load balancers* NLB kann ein redundanter Cluster mit 2 bis 32 Servern realisiert werden.

Authentifizierung beim VPN-Server

Die Authentifizierung des VPN-Clients erfolgt über EAP mit Benutzerzertifikaten gegen einen RADIUS-Server. Dieser prüft die Gültigkeit des Zertifikats sowie die Gruppenzugehörigkeit zur AD-Gruppe der VPN-Benutzer.

Das Benutzerzertifikat wird von der internen PKI ausgestellt und ist über das TPM an das Gerät gebunden. Zusammen mit den Windows Credentials ergibt sich dadurch eine Multifaktor-Authentifizierung, wobei das Gerät den Faktor *something you have* darstellt.

Authentifizierung beim Client

Bei vielen Lösungen für mobile Clients ist die Authentifizierung des Benutzers eine heikle Schwachstelle. In der Regel kommen hier Benutzername und Passwort zum Einsatz. Wurden die Zugangsdaten gestohlen (z.B. mit Phishing), kann sich ein Angreifer auf einem gestohlenen oder gefundenen Client anmelden und erlangt Zugriff sowohl auf die lokal gespeicherten Daten als auch auf alle Services und Dateien, auf die der Benutzer Zugriff hat.

Um hier eine Erhöhung des Sicherheitslevels zu erreichen, bietet sich ein weiteres Windows Feature an, nämlich *Windows Hello for Business*, der Microsoft Lösung für eine sichere und passwortlose Authentifizierung. Zum Einsatz kommt dabei ein Zertifikat, das auf dem TPM abgelegt und somit physisch an den Client gebunden ist. Das Zertifikat wird mit einem PIN geschützt, wobei der *Brute Force* Schutz wiederum durch das TPM sichergestellt wird. Bei Bedarf kann auch ein biometrisches Element verwendet werden, um die Benutzerfreundlichkeit zu erhöhen. Der *Logon Provider* für Benutzername/Passwort wird auf dem Client deaktiviert.

Referenzlösung

Im Folgenden wird eine Referenzlösung skizziert, wie sie in vielen IT-Infrastrukturen umgesetzt werden kann.

Sicherheitskonzept mobiler Client

Da der mobile Client den geschützten Bereich des Firmennetzwerkes physisch verlässt, sind die Sicherheitsanforderungen hoch. Aktuelle Technologien wie *OneDrive* oder *SharePoint* speichern Daten lokal und synchronisieren sie bei Bedarf mit dem Backend. Daher muss davon ausgegangen werden, dass vertrauliche Daten auf dem mobilen Client liegen.

Das Sicherheitskonzept basiert daher auf mehreren Schichten.

Festplattenverschlüsselung

In der untersten Schicht wird die Festplatte verschlüsselt. Dazu wird *Bitlocker* eingesetzt, ebenfalls ein Windows Bordmittel. Der Bitlockerschlüssel ist im TPM abgelegt und mit

einem PIN geschützt. Beim Einschalten des Gerätes muss dieser PIN eingegeben werden. Das TPM ist *tamper resistant*, wodurch *Bruteforce* Angriffe auf den PIN verhindert werden können. Durch den Einsatz von *Bitlocker Network Unlock* entfällt die PIN-Eingabe im sicheren Firmennetzwerk. Mit geeigneten Energieeinstellungen wird dafür gesorgt, dass der Client nach einer gewissen Zeit in den Ruhezustand (*hibernate*) wechselt, so dass der PIN-Schutz auch dann aktiv wird, wenn das Notebook einfach zugeklappt und mitgenommen wird.

Firewall

Im Firmennetzwerk ist der Client durch Edge Firewalls ausreichend gegen unerlaubte Zugriffe aus dem Internet geschützt. Wird er jedoch ausserhalb dieser geschützten Umgebung betrieben, muss die lokale Firewall den notwendigen Schutz sicherstellen. Eingesetzt wird die in Windows integrierte Firewall *Windows Defender Firewall*. Die Konfiguration erfolgt über *Group Policies*, wodurch verhindert werden kann, dass Applikationen selbst Firewallregeln erzeugen. Die Firewall Policy ist sehr strickt – es werden nur die für den Betrieb absolut notwendigen Verbindungen zugelassen. Dazu gehören etwa DHCP, Zugriff auf lokale DNS-Server und die Verbindung zum VPN-Gateway. Eingehende Verbindungen werden ebenso geblockt wie direkte ausgehende Verbindungen ins Internet. Befindet sich der Client im Firmennetzwerk, gilt eine weniger restriktive *Firewall Policy*. Diese wird auch auf den VPN-Tunnel angewandt.

VPN-Protokolle

Bei der Umsetzung wurde IKEv2 als primäres Protokoll mit einem *fallback* auf SSTP implementiert. SSTP kommt dann zum Einsatz, wenn die für IKEv2 benötigten Ports clientseitig blockiert sind. Das ist typischerweise bei WLANs in Hotels oder bei öffentlichen WLANs der Fall.

Kryptographie

Sowohl bei IKEv2 als auch bei SSTP entsprechen die standardmässig verwendeten *crypto suites* nicht den heutigen Anforderungen. Diese müssen daher angepasst werden.

Bei IKEv2 wird AES-128 Bit Verschlüsselung mit SHA256 und DH Group 14 verwendet.

Bei SSTP wird ein ECC Zertifikat mit 256 Bit Schlüssel eingesetzt, schwache *crypto suites* für TLS und ältere TLS Versionen werden auf dem VPN-Server deaktiviert. Dies ist problemlos möglich, da keine Rücksicht auf ältere Betriebssysteme oder Browser genommen werden muss.

VPN-Server

Als VPN-Server wird ein Windows Server 2019 mit RRAS Rolle eingesetzt. Der Server hat zwei Beine, wobei das äussere über die Edge Firewall vom Internet her erreichbar ist. Auf der Edge Firewall ist ein NAT *port forwarding* eingerichtet, so dass nur Verbindungen über die benötigten Ports (UDP 500, 4500 und TCP 443) überhaupt zum VPN-Server aufgebaut werden können. Auch der Internetzugang der VPN-Clients läuft über dieses Bein.

Das zweite Bein ist mit dem internen Netz verbunden. Darüber läuft der gesamte interne Netzwerkverkehr (über statische Routen). Die Clients befinden sich dabei logisch im gleichen IP-Netz wie der interne NIC. Mit Regeln auf der internen Firewall kann definiert werden, welche Ressourcen die VPN-Clients nutzen können.

Der VPN-Server kann in die Windows Domäne als Member-Server eingebunden werden, was die Administration erleichtert. Ebenfalls unterstützt ist die Variante *stand alone* Server.

Der VPN-Server steht in einer DMZ, wo er vom Internet her erreichbar ist. Deshalb wird er gehärtet. Am einfachsten erfolgt dies durch die Anwendung der *Microsoft Base Line Security*, welche über vordefinierte GPOs einfach implementiert werden kann. Ebenfalls kommt die Windows Firewall zum Einsatz.

Redundanz

Unter Verwendung des Windows Features *network load balancing* (NLB) kann der VPN-Server redundant ausgelegt werden. Solange beide Server aktiv sind, werden die Clients auf die beiden Server verteilt. Fällt einer der Server aus oder wird er zu Wartungszwecken aus dem Cluster genommen, übernimmt der andere Server dessen Clients. Es können bis 32 Server zu einem Cluster zusammengefasst werden, wodurch eine hohe Skalierung möglich ist.

Optional kann auch ein externer *load balancer* verwendet werden.

Zertifikate

Auf dem VPN-Server wird sowohl für IKEv2 als auf für SSTP ein Server-Zertifikat benötigt. Dasjenige für IKEv2 kann von der internen CA ausgestellt werden. SSTP basiert auf TLS und benötigt ein Zertifikat, für das der VPN-Client die CRL abrufen kann. Daher wird hier ein Zertifikat einer offiziellen CA verwendet. Durch den Einsatz von *Let's Encrypt* Zertifikaten kann die Erneuerung automatisiert werden. Diese Zertifikate sind sicher und kostenlos erhältlich.

RADIUS-Server

Als RADIUS-Server wird ein Windows Server mit NPS-Rolle verwendet. Dieser prüft, ob das vorgelegte Benutzerzertifikat von der internen CA ausgestellt wurde und ob der Benutzer Mitglied der AD-Gruppe der VPN-Benutzer ist.

Da EAP ein Standard ist, kann auch ein anderer RADIUS-Server eingesetzt werden.

Das für EAP benötigte Zertifikat kann von der internen CA ausgestellt werden.

Mobiler Client

Der mobile Client basiert auf Windows 10. Er kann sowohl im Büro als auch im Homeoffice oder unterwegs verwendet werden. Die Mitarbeitenden haben somit nur ein persönliches Gerät, das sie z.B. auch an Sitzungen mitnehmen können.

VPN Client

Der *Always On VPN* Client wird mit einem VPN-Profile (XML-File) konfiguriert. Dieses wird automatisch auf die für VPN zugelassenen Geräte (AD-Gruppe) ausgerollt. Im VPN-

Profile sind alle Informationen, die für den Aufbau der VPN-Verbindung benötigt werden, enthalten.

Es wird ein *user tunnel* im *always on* Modus verwendet. Damit wird die VPN-Verbindung aufgebaut, wenn ein Benutzer angemeldet ist und sobald der Client Internetverbindung hat, bzw. den VPN-Gateway erreichen kann.

Im *force-tunnel* Modus wird sämtlicher Netzwerkverkehr durch den VPN-Tunnel geleitet, sobald dieser steht. Optional könnte der *split-tunnel* Modus verwendet werden, bei dem der Netzwerkverkehr mit Regeln aufgeteilt werden kann. Damit lässt sich z.B. der Zugang zu MS365 ohne Umweg über das Firmennetzwerk realisieren.

Windows Firewall

Die Windows Firewall ist das zentrale Sicherheitselement des mobilen Clients. Sie schützt diesen vor unerlaubten Zugriffen aus dem Internet und verhindert dabei auch direkten *inside out* Netzwerkverkehr.

Solange der VPN Tunnel nicht steht, sind die Netzwerkzugriffe auf lokale DHCP- und DNS-Server erlaubt, ebenso der Zugriff auf den VPN-Gateway über IKEv2 und SSTP.

Die Windows Firewall arbeitet mit sogenannten Profilen, wovon es drei gibt. Solange der Client keinen Kontakt zu einem Domain Controller hat, wird entweder das *public* oder das *private* Profil verwendet. Stellt die Firewall fest, dass der Client seinen Domain Controller sieht, wird das *domain* Profil verwendet. Dies ist der Fall, wenn der Client im Firmennetzwerk betrieben wird und den DC dadurch direkt sieht oder wenn er diesen durch den VPN Tunnel sieht. Zu beachten ist hier, dass gleichzeitig mehrere Firewall Profile aktiv sein können, da diese pro Netzwerkkarte zugeteilt werden. Wenn der Client also im Homeoffice über WLAN mit dem Internet verbunden ist, gilt für das WLAN-Interface das Profil *public* und für das VPN-Interface das Profil *domain*.

Die Firewall Konfiguration wird dem Client über GPO zugewiesen, wobei lokale Regeln nicht angewandt werden. Dadurch wird verhindert, dass automatisch erstellte Firewallregeln weiteren Netzwerkverkehr zulassen.

Zertifikate

Die Authentifizierung des VPN-Tunnels erfolgt über ein Benutzerzertifikat. Dieses wird automatisch erstellt, wenn sich der Benutzer das erste Mal anmeldet. Dazu muss sich der Client im internen Netzwerk befinden. Die Steuerung der automatischen Zertifikatserstellung erfolgt über GPO und eine AD-Gruppe (nur für Mitglieder der Gruppe wird ein Zertifikat erstellt). Die Erneuerung dieses Zertifikats erfolgt ebenfalls automatisch. Dies erfolgt auch durch den VPN-Tunnel.

DNS

Solange der VPN-Tunnel noch nicht steht, werden die über DHCP konfigurierten DNS-Server verwendet. Sobald der Tunnel steht, werden die internen DNS-Server verwendet.

Der Client kann seine aktuelle IP-Adresse im DNS-Server eintragen (*dynamic DNS*). Dadurch sind z.B. Zugriffe zu Wartungszwecken über den DNS-Namen möglich, unabhängig davon, ob der Client mit dem Firmennetzwerk oder über VPN verbunden ist.

Sicherheit

Wenn der Client in den Räumlichkeiten der Firma betrieben wird, ist er vor physischen Angriffen gut geschützt. Wird er aber extern betrieben, ist dies nicht mehr der Fall. Bei der Risikoanalyse zeigte sich, dass insbesondere die Situation, bei der der Client in fremde Hände fällt, besondere Schutzmassnahmen erfordert. Diese müssen gewährleisten, dass die auf dem Client gespeicherten Daten vor Zugriff geschützt sind und dass ein unbefugtes Anmelden verhindert wird. Diese Risiken bestehen aber grundsätzlich bei allen mobilen Geräten.

Ist das Gerät ausgeschaltet oder im Ruhezustand, sind die Daten sehr gut durch die Verschlüsselung der Festplatte mit *Bitlocker* geschützt. Der Verschlüsselungsschlüssel ist dabei auf dem TPM hinterlegt und mit einem PIN geschützt. Ohne Kenntnis des PINs kann das System weder gestartet werden noch kann die Festplatte auf einem anderen System gelesen werden. Da das TPM *tamper resistant* ist, ist der PIN wirkungsvoll gegen *brute force* Angriffe geschützt[1].

Hat ein Angreifer hingegen Zugriff auf ein eingeschaltetes Gerät ist dieses nur noch durch die schwache Authentifizierung mit Benutzername und Passwort geschützt.

Soll dieses Risiko auch noch kompensiert werden, kann eine starke Authentifizierung mit *Windows Hello for Business* verwendet werden. Dabei wird ebenfalls ein Benutzerzertifikat verwendet, dessen privater Schlüssel im TPM liegt und mit einem PIN geschützt ist. Durch die Deaktivierung des *Logon Providers* für Benutzername/Passwort ist die Anmeldung nur noch mit dem PIN möglich.

[1] Nach 32 erfolglosen Versuchen sperrt die TPM den Zugriff auf den *Bitlocker* Schlüssel, die Entsperrung ist nur mit dem im AD hinterlegten Recovery Key möglich.