Standards für sichere Administration

IV-Sicherheitsteam, Juli 2017

https://www.uni-muenster.de/IV-Sicherheit

Einleitung

Dieses Dokument enthält Best Practices zur sicheren Administration von Servern, Appliances und aktiven Netzwerkkomponenten, die vom IV-Sicherheitsteam in Zusammenarbeit mit dem Zentrum für Informationsverarbeitung (ZIV) und den Informationsversorgungseinheiten (IVVen) zusammengestellt wurden. Deren Umsetzung ist allen Mitglieder und Angehörige der Westfälischen Wilhelms-Universität Münster (WWU), die im Rahmen ihrer dienstlichen Tätigkeit Server, Appliances oder aktive Netzwerkkomponenten an der WWU betreiben, empfohlen. Diese Standards sollen dafür sorgen, dass die Sicherung der Grundziele der IT-Sicherheit, **Integrität**, **Verfügbarkeit** und **Vertraulichkeit**, im notwendigen Maße umgesetzt wird. Eine wiederholte oder massive Missachtung dieser Standards gilt als fahrlässiger Betrieb des Servers. Sollten dem ZIV solche Fälle bekannt werden, wird es geeignete technische und organisatorische Maßnahmen ergreifen, um die gewünschten Standards wiederherzustellen. Weitere Empfehlungen und Regelungen zur Informationsverarbeitung an der WWU, insbesondere zur IV-Sicherheit, finden sich im IV-Sicherheitshandbuch der WWU[1].

Inhaltsverzeichnis

[1] https://www.uni-muenster.de/IV-Sicherheit/handbuch/

Grundempfehlungen für den sicheren Betrieb

In diesem Kapitel werden grundlegende Konzepte für einen sicheren Betrieb von Servern, Appliances und aktiven Netzwerkkomponenten festgelegt. Die nachfolgenden Kapitel ergänzen und präziseren die hier vorgestellten organisatorischen und technischen Sicherheitsmechanismen.

Begriffserläuterungen

Als Dienstrechner, **Server** oder auch Host wird ein in ein Netzwerk eingebundenes Rechnersystem bezeichnet, das Clients bedient oder Server-Software beherbergt[2].

Als **Arbeitsplatzrechner** oder Arbeitsplatzcomputer wird ein Rechnersystem bezeichnet, das am Arbeitsplatz einer Person steht und zur Bildschirmarbeit genutzt wird. Das Gegenteil von Arbeitsplatzrechner sind Dienstrechner (Server) [3] . **Adminarbeitsplätze** sind speziell abzusichernde Arbeitsplatzrechner, die optimalerweise ausschließlich zu Administrationszwecken genutzt werden.

Ein Jumpserver oder **Jumphost** ist ein spezielles Rechnersystem in einem Netzwerk, das typischerweise dafür genutzt wird, Geräte in einer separaten (Netzwerk-)Sicherheitszone zu administrieren.

Als **Appliance** wird ein Ansatz zum Design für ein kombiniertes System aus Rechner-Hardware und speziell auf diese Hardware optimierter Software bezeichnet, welche im Wesentlichen einer oder nur wenigen Anwendungen dient.[4]

Aktive Netzwerkkomponenten sind alle Bestandteile eines Netzwerks, die aktiv Signale verarbeiten bzw. verstärken können. Sie benötigen dazu eine Stromversorgung und haben in der Regel eine Administrationsschnittstelle. Zu dieser Gruppe gehören Hubs und Switches, Router, Firewalls usw.[5]

Grundsätzliches

Servern, Appliances und aktiven Netzwerkkomponenten müssen grundsätzlich von qualifiziertem Fachpersonal betreut werden. Optimaler Weise sollte der Betrieb von einer IVV oder vom ZIV geregelt sein. Sollte die Betreuung durch eine IVV in Einzelfällen nicht praktikabel sein, ist - vor allem in sicherheitsrelevanten Zweifelsfällen - eine enge Zusammenarbeit mit dem ZIV empfohlen.

Planung

Vor der Installation eines Servers sollten einige Punkte bezüglich der Sicherheit bedacht werden. So sollte jeder Dienst nach Möglichkeit auf einem separaten Server untergebracht sein, um die optimale Absicherung für diesen gewährleisten zu können. Darüber hinaus sollte geklärt werden, wie hoch die Ansprüche an die Grundziele der IT-Sicherheit (Integrität, Verfügbarkeit und Vertraulichkeit) für den betriebenen Dienst sind. Abhängig von dieser Risikoabschätzung müssen eventuell weitere Sicherheitsmaßnahmen umgesetzt werden.

Standort

Die Hardware muss an einem sicheren Ort betrieben werden, sodass physikalische Zugriffe nur von autorisierten Personen durchgeführt werden können. Hierfür sollten Servern, Appliances und aktiven Netzwerkkomponenten am besten in einem Raum mit Zugangsschutz und -überwachung untergebracht werden. Ist dies nicht möglich, sollte zumindest ein abschließbarer Raum oder

---

[2] https://de.wikipedia.org/wiki/Host_(Informationstechnik)
[3] https://de.wikipedia.org/wiki/Arbeitsplatzrechner
[4] https://de.wikipedia.org/wiki/Appliance
[5] https://de.wikipedia.org/wiki/Netzwerkkomponente

Serverschrank genutzt werden. Je nach Verfügbarkeit folgen auch Anforderungen an die Stromversorgung, Kühlung und Redundanz eines Systems.

Ergänzende rechtliche Bestimmungen

Unabhängig der hier aufgeführten Standards müssen Serverbetreiber eine Vielzahl rechtlicher Bestimmungen einhalten. Dazu gehören insbesondere Bestimmungen des BDSG, LDSG NRW, TMG, TKG sowie des BGB und StGB, bspw. die so genannte Störerhaftung, Impressumspflicht und gesetzlich vorgeschriebene technische und organisatorische Maßnahmen.

Produktspezifische Sicherheitsmaßnahmen

Je nach eingesetzter Hard- und Software sind weitere produktspezifische Sicherheitsmaßnahmen zu beachten. Administratoren sind in der Pflicht, sich regelmäßig über das Sicherheitsniveau der eingesetzten Produkte zu informieren und müssen ggf. zusätzliche Maßnahmen ergreifen.

Systemseitige Absicherung

Regeln zur Installation und zum Einsatz von Software

Bei der Installation sollte darauf geachtet werden, dass jeder Server optimaler Weise nur einen Dienst bereitstellt. Deshalb sollte nur Software installiert werden, die für den jeweiligen Dienst oder die Administration notwendig ist, um den Softwareumfang gering zu halten und die möglichen Sicherheitslücken zu begrenzen. Dabei sollte sich die Installation auf Distributionssoftware (Unix) oder Software aus vertrauenswürdigen Quellen beschränken. Die Echtheit und Integrität der Software sollte im Zweifelsfall manuell überprüft werden.

Unbedingt empfohlen ist die regelmäßige und zeitnahe Installation von Sicherheitspatches. Dies kann beispielsweise durch automatische Updates geschehen. Sollten automatische Updates nicht möglich sein, z.B. bei kritischen Systemen, sollten regelmäßig manuell Updates durchgeführt werden. Der Updateprozess sollte klar definiert - auch bezüglich Urlaubsvertretungen - und allen Verantwortlichen bekannt sein.

Zur Erhöhung der Integrität entsprechender Systeme sollte der Einsatz von Code-Signing (z.B. für Makros, Powershell-Skripte) in Betracht gezogen werden. Außerdem sollte geprüft werden, ob zusätzliche Sicherheitsmechanismen wie z.B. AppLocker[6] oder EMET[7] unter Windows bzw. SELinux[8], AppArmor oder TrustedBSD unter Unix eingesetzt werden können.

Transportverschlüsselung

Die Verschlüsselung von Daten ist nötig, um die vertrauliche Kommunikation zwischen zwei Systemen sicherzustellen. Sie sollte für jegliche Kommunikation eingesetzt werden, insbes. für die Kommunikation zwischen Nutzer und Server, sowie zwischen Administrator und Server. Eine unverschlüsselte Verbindung sollte nur in begründeten Ausnahmefällen hergestellt werden. Vorher sollte der Einsatz von alternativen Verschlüsselungsverfahren geprüft werden, z.B. durch VPN- oder SSH-Tunnel.

Zwei-Faktor-Authentifizierung

Der Zugriff auf das Betriebssystem muss ausreichend geschützt sein. Damit die Kompromittierung eines einzelnen Faktors (z.B. Passwort) noch kein kritisches Sicherheitsrisiko darstellt, sollten zwei Faktoren zur erfolgreichen Authentifizierung am System eingesetzt werden. Hier sei vor allem der Einsatz von Security-Tokens (Primär Windows) oder SSH Public Keys (Primär Unix) empfohlen, aber auch der Einsatz von mTAN und OTP können zweite Faktoren darstellen.

Es wird empfohlen den zweiten Faktor erst bei der Anmeldung am zu schützenden System selbst zu verlangen. Falls das System keine Zwei-Faktor-Authentifizierung unterstützt, muss dafür gesorgt werden, dass die Administrationsschnittstellen nur aus besonders geschützten Administrationsnetzen erreichbar sind. Wenn sichergestellt wird, dass jede Zugriffsmöglichkeit auf den Server einen zweiten Faktor verlangt, ist es auch möglich den zweiten Faktor auf einem Jumphost oder den Adminarbeitsplätzen abzufragen und nicht mehr am Server (Letzteres ist jedoch aufwändiger und fehleranfälliger).

Logging und Monitoring

Die Zugriffe auf ein System, darunter auch administrative Zugriffe, sollten protokolliert werden, sodass einerseits Angriffe und Manipulationen erkannt werden können, aber andererseits auch Änderungen durch Administratoren nachvollzogen werden können. Hierbei müssen die Regeln des Datenschutzgesetzes beachtet werden. Es sollte eine im Rahmen der Anwendung angemessene maximale Speicherdauer für Logdaten festgelegt werden (in der Regel 7 Tage).

---

[6] https://msdn.microsoft.com/de-de/library/hh831440(v=ws.11).aspx
[7] https://support.microsoft.com/de-de/kb/2458544
[8] https://selinuxproject.org

Geeignete Software zum Monitoring sollte verwendet werden, um Angriffe oder andere Probleme frühzeitig zu erkennen und gegebenenfalls sofort auf diese zu reagieren. Unter Unix kann z.B. Fail2Ban[9] verwendet werden, um Brute-Force- oder DoS-Angriffe abzuwehren.

Datenschutz

Bei der Verarbeitung von personenbezogenen Daten gelten die Regelungen aus dem Datenschutzgesetz (LDSG-NRW, EU-DS-GVO). Administratoren sollten sich mit dem Datenschutz-Grundwissen vertraut machen, insbesondere die Dokumentation von Verfahren und die Benachrichtigungs- bzw. Auskunftspflichten sind relevant. Außerdem Art.25 "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen".

Backups

Die Einrichtung und Durchführung von regelmäßigen Sicherungen der Systemdaten wird empfohlen. Der Umfang der Sicherungen hängt vor Allem von der gewünschten Verfügbarkeit für die Anwendungsdaten ab. Darauf aufbauend sollte ein passendes Dateisystem und Backup-Verfahren gewählt werden. Für die unmittelbare Wiederherstellung bietet sich die Verwendung von Schattenkopien bzw. Snapshots an. Dazu muss ein Dateisystem verwendet werden, das diese Funktion unterstützt, z.B. Btrfs, GPFS, UFS, ZFS unter Unix oder NTFS unter Windows. Für längerfristige Sicherungen kann eine Bandsicherung, z.B. mittels TSM[10], verwendet werden.

Zu beachten ist, dass Datenträger oder Systeme, die als Ziele für Backups dienen, ebenfalls zugriffsgesichert werden. Hierfür sollten mindestens die gleichen Zugriffsbeschränkungen, wie für die Anwendung selbst, eingerichtet werden. Bei der Nutzung von TSM muss beachtet werden, dass die Wiederherstellung von Dateien allein mit dem Zugangspasswort möglich ist. Daher sollte bei sensiblen Daten über eine zusätzliche Verschlüsselung nachgedacht werden. Optimaler Weise sollten Backup-Systeme getrennt vom eigentlichen Server betrieben werden, sodass z.B. auch im Katastrophenfall die Backups verfügbar sind (siehe auch nächster Punkt).

Redundanz

Im Rahmen einer hohen Verfügbarkeit sollten ganze Server oder Teilsysteme redundant betrieben werden. Der Umfang hängt stark von der notwendigen Verfügbarkeit der Anwendung ab. Im Idealfall sollten redundante Systeme so umgesetzt werden, dass diese sofort einspringen können, sollte ein anderes System ausfallen.

Management-Schnittstellen

In der Regel stellen Server-Systeme dedizierte Management-Schnittstellen zur Verfügung, um Server aus der Ferne konfigurieren und steuern zu können. Diese Schnittstellen dürfen bei der Absicherung des Servers nicht außer Acht gelassen werden.

Bestenfalls steht hierfür eine zusätzliche Netzwerkschnittstelle zur Verfügung, welche nur für den Zugriff auf die Management-Schnittstelle genutzt wird. Dies ermöglicht eine strikte Trennung von Nutzer-Zugriffen und Management-Zugriffen. Ist die Verwendung einer zusätzlichen Netzwerkschnittstelle nicht möglich, sollte ein VLAN genutzt werden, um die Zugriffe getrennt verarbeiten zu können.

Auch bei der Nutzung von Management-Schnittstellen sollte möglichst Zwei-Faktor-Authentifizierung genutzt werden. Wird dies nicht von der Management-Software selbst unterstützt, sollte diese nur über einen Terminalserver oder Adminarbeitsplätze mit Zwei-Faktor-Authentifizierung zugänglich gemacht werden.

Datenverschlüsselung

Werden auf dem **Server** sensible Daten gespeichert, sollte eine Verschlüsselung der Daten auf dem Server selbst in Betracht gezogen werden. Dies kann dabei helfen, die sensiblen Daten auch

[9] http://www.fail2ban.org
[10] ZIV TSM Link einfügen

bei erfolgreichen Angriffen auf das System weiterhin sicher zu halten. Es sollte bereits im Voraus geklärt werden, welche Daten mit welchen Methoden verschlüsselt werden.

Die Daten auf **Arbeitsplätzen** von Administratoren sollten verschlüsselt sein. Bei Windows-Systemen sollte dafür BitLocker[11] eingesetzt werden. Alternativ gibt es auch das Open-Source-Produkt VeraCrypt[12]. Diese Regelung gilt insbesondere für mobile Geräte, die zur Administration eingesetzt werden, da hier neben der Integrität auch das Risiko eines Geräteverlusts noch wesentlich höher ist.

Accounts

Der Zugriff auf den Server sollte nur über eigens eingerichtete Zugänge möglich sein. Alle nicht benötigten Accounts sollte gesperrt oder gelöscht werden. Ebenso sollten Standardpasswörter für Accounts oder Anwendungen sofort geändert werden, da diese sonst missbraucht werden könnten. Für Nutzer sollten keine lokalen Kennungen eingerichtet werden, sondern die zentrale Unikennung verwendet werden. Windows-Systeme können dafür in die wwu.de-Domäne aufgenommen werden. Unix-Systeme können mit Samba/Winbind ebenfalls ans Active-Directory und die zentrale Nutzerverwaltung angebunden werden.

Netzseitige Absicherung

Von großer Wichtigkeit ist die netzseitige Absicherung von Servern, Appliances und aktiven Netzwerkkomponenten. Was dabei zu beachten ist, folgt in diesem Kapitel.

Erreichbarkeit von Servern und Adminarbeitsplätzen

Das ZIV setzt eine Firewall ein, die grundsätzlich Verbindungsversuche aus dem Internet unterbindet. Ist der Nutzerkreis eines Servers oder Dienstes auf eine kleinere Gruppe beschränkt, sollte die Möglichkeit in Betracht gezogen zu werden, den Server nur in einem Subnetz für die Arbeitsgruppe oder im internen Netz der Uni erreichbar zu machen. Soll das System auch aus dem Internet erreichbar sein, kann über die zuständige IVV beim ZIV die Freischaltung für die zugehörige Whitelist beantragt werden.

Darüber hinaus sollten alle Dienste soweit wie möglich über Firewall- und Zugriffs-Regeln auf den Nutzerkreis eingeschränkt werden. Administrative Zugänge sollten aus dem Internet grundsätzlich nicht erreichbar sein.

Jumphosts

Die administrativen Zugänge der Server sollten nur über definierte Rechner erreichbar sein. Dementsprechend ist es empfohlen Adminarbeitsplätze und/oder Einsprungserver (Jumphosts/Proxys) einzurichten, welche diesen definierten Zugangspunkt darstellen. Allerdings sind oft auch auf Adminarbeitsplätzen höchst sensible Informationen gespeichert. Daher sollten diese von außen nicht oder nur über Jumphosts erreichbar sein.

Für **Windows** wird ein entsprechender RDP-Proxy vom ZIV angeboten. Bislang kann man sich auf REMOTEDESKTOP.UNI-MUENSTER.DE über RDP verbinden und von dort aus per RDP auf Rechner innerhalb der Uni Münster weiterverbinden. Aktuelle RDP-Clients unterstützen Remotedesktop-Gateways. Dazu muss beim Aufbau der Remotdesktopverbindung „Optionen einblenden“ angeklickt, dann der Reiter „Erweitert“ ausgewählt und auf den Knopf „Einstellungen...“ geklickt werden. Der Gatewayserver ist REMOTEDESKTOPGATEWAY.UNI-MUENSTER.DE (oder kurz RDG.UNI-MUENSTER.DE). Technisch wird die Verbindung über das Gateway aufgebaut, wo auch eine Authentifizierung verlangt wird. Sicherheitstechnisch ist dieses Vorgehen vergleichbar mit der Einwahl über REMOTEDESKTOP.UNI-MUENSTER.DE, es ist allerdings bequemer.

---

[11] https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-device-encryption-overview-windows-10

[12] https://www.veracrypt.fr/

Unter **Linux** besteht eine Möglichkeit darin, eine eigene ssh-config (~/.ssh/config) zu erstellen und einen SSH-Proxy einzutragen. Dabei handelt es sich um eine Textdatei, in die z.B. folgende Zeilen geschrieben werden:

```
# Direkte Verbindung zum ZIVLTS.UNI-MUENSTER.DE Server
HOST ZIVLTS.UNI-MUENSTER.DE # oder ZIVLTS1/ZIVLTS2/ZIVLTS3/ZIVLTS4
  User NUTZERKENNUNG        # normale Uni-Kennung
  ProxyCommand none
# Für alle anderen Server in der Uni, den Weg über ZIVLTS nehmen
HOST *.uni-muenster.de
  User NUTZERKENNUNG
  ProxyCommand ssh -q NUTZERKENNUNG@ZIVLTS.UNI-MUENSTER.DE -W %h:%p
```

Achten Sie auf die Reihenfolge der Einträge. Das SSH-Kommando nutzt den ersten passenden Eintrag zum Aufbau der Verbindung. Es wird dann automatisch durch den SSH-Client eine Verbindung über den gewählten Proxy-Server aufgebaut. Dabei kann es notwendig sein, dass Sie sich authentifizieren müssen.

VPN

Zum Zeitpunkt des Verfassens dieses Dokument wird davon ausgegangen, dass VPN-Verwaltungsnetze einen unzureichenden Schutz darstellen, da ein zweites Passwort („Netzzugangspasswort“) keinen qualifizierten zweiten Faktor darstellt und insbesondere das WLAN-Passwort identisch mit dem VPN-Passwort ist. Es wird geprüft, ob man diesen Umstand auflösen und durch die Möglichkeit von VPN Netzwerken mit zweitem Faktor ersetzen kann.

Weiterhin ist zu beachten, dass sich in solchen Verwaltungsnetzen die VPN-Geräte nicht untereinander erreichen sollten.

Absicherung von administrativen Zugängen

Beim Umgang mit Zugangsdaten ist besondere Vorsicht geboten. Das gilt insbesondere für Zugangsdaten von Administratoren. Was dabei zu beachten ist, folgt in diesem Kapitel.

Grundsätzliches

Einige Grundsätze sind unabhängig von den eingesetzten Systemen zu beachten. Dazu gehört, dass Zugangsdaten grundsätzlich nur verschlüsselt oder entsprechend analog in verschlossenen Briefumschlägen zu verschicken sind.

Ebenso sollte ein differenziertes Rechtemanagement umgesetzt und mit möglichst niedrigen Privilegien gearbeitet werden. Insbesondere muss es also eine Trennung zwischen „normalem" und Admin-Account geben und dieser sollte nur benutzt werden, wenn es die Arbeit erfordert. Ein restriktives Vorgehen bei der Vergabe von Rechten sollte angestrebt werden und nur für den jeweiligen Zugriff benötigte Rechte vergeben werden. Das Rechtemanagement sollte auch so umgesetzt werden, dass nur berechtigte Personen Admin-Rechte an andere vergeben können. Weiterhin sollten unterschiedliche Admin-Accounts für unterschiedliche Bereiche genutzt werden.

Der Login mit dem Admin-Account darf nur an sicheren Systemen über verschlüsselte Verbindungen mit Zwei-Faktor-Authentifizierung erfolgen. Sollte der Administrations-Zugang nicht direkt auf dem Server mittels Zwei-Faktor-Authentifizierung abgesichert werden können, kann die Zwei-Faktor-Authentifizierung ausgelagert werden auf einen Jumphost, sofern der Administrations-Zugang nur von diesem erreichbar ist.

Windows

Unter Windows wird meistens die verschlüsselte RDP-Verbindung zur Administration genutzt. Es wird als zweiter Faktor ein Security-Token empfohlen. Dieser kann vom ZIV bereitgestellt und auf Wunsch bereits mit einem wwu.de AD-Zertifikat versehen werden, welches zwei Jahre lang gültig ist und dessen Ablauffrist vom Nutzer selbst verlängert werden kann. Es kann auch ein bereits vorhandenes Zertifikat der WWUCA verwendet werden.

Unix

Bei Unix erfolgt die Administration meistens über eine Secure Shell (SSH) Verbindung. Der SSH-Login sollte mit dem Public Key Verfahren geschützt werden und der Schlüssel mit einem Passwort versehen werden. Der private Schlüssel sollte nur bei Gebrauch entschlüsselt werden.

Es wird geprüft, ob es auch unter Unix Möglichkeit zur Verwendung von Security-Tokens und X.509-Zertifikaten als Alternative zu SSH-Keys gibt.

Außerdem sollten zur (De-)Provisionierung von SSH Keys auf der Serverseite Tools wie z.B. CFEngine[13] eingesetzt werden.

Die Verwendung der Security-Tokens ist – zumindest unter Ubuntu – möglich: https://www.uni-muenster.de/ZIVwiki/bin/view/ZIV/Security-TokenUbuntu

OTP und mTAN

Das ZIV betreibt einen OTP-Server, der als zweiter Faktor in Server-Anmeldungen integriert werden kann. Es wird geprüft ob der mTAN-Dienst, der z.B. in MeinZIV zum Einsatz kommt, auch von weiteren Serversystemen genutzt werden kann.

Neben diesen Angeboten gibt es für Unix Systeme die Möglichkeit den Google Authenticator einzusetzen. Entsprechende Anleitungen für Ubuntu und Fedora sind im ZIVwiki[14] verfügbar.

---

[13] https://cfengine.com/product/community

[14] https://www.uni-muenster.de/ZIVwiki/bin/view/ZIV/GoogleAuthenticator

Verwendung von Zertifikaten

An vielen Stellen während der Administration ist ein verantwortungsbewusster Umgang mit Zertifikaten wichtig. Deshalb folgen in diesem Kapitel noch einige Hinweise zum Umgang mit diesen.

Grundsätzliches

Persönliche Zertifikate sind bei verantwortungsvollem Umgang eine gute Alternative zum herkömmlichen Passwort. Ein verantwortungsvoller Umgang ist gekennzeichnet durch die folgenden Punkte:

- Der private Schlüssel zu einem persönlichen Zertifikat darf nur dem Inhaber zugänglich sein. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem ein privater Schlüssel gespeichert bzw. eingesetzt wird, muss angemessen geschützt sein, also z. B. regelmäßig mit Sicherheits-Patches versehen werden, um möglichst frei von Schadsoftware zu sein.
- Wenn der private Schlüssel auf einem Security-Token gespeichert ist, so muss das Token mit einer Passphrase/PIN geschützt sein.
- Wenn der private Schlüssel nicht auf einem Security-Token gespeichert ist, sondern z. B. im Zertifikatsspeicher Ihres Betriebssystems, Ihres Browsers oder als Datei, so muss der Zertifikatsspeicher mit einer Passphrase geschützt sein.

Server-Zertifikate sollten mit gleicher Sorgfalt behandelt werden, um einen Verlust und Kompromittierung zu vermeiden.

Zertifikate der WWUCA

Bei der Verwendung der Zertifikate gelten die Nutzungsbedingungen des DFN: https://www.pki.dfn.de/fileadmin/PKI/Info_Zertifikatinhaber.pdf

Windows AD-Zertifikate

Entsprechende Windows Zertifikate kann aktuell jeder angemeldete Nutzer erzeugen. Die zugehörigen Berechtigungen können über eine Gruppe erlaubt werden. Eine Einschränkung wäre über die Windows-Richtlinien auch für einzelne Nutzer möglich.

Einrichtung von Wartungszugängen

Im Rahmen von Serviceverträgen bei Appliances (z.B. bei Labor- oder medizintechnischen Geräten) wird oft ein entfernter Zugriff auf das Gerät benötigt um Wartungen durchzuführen. Ein Techniker des Herstellers verbindet sich dabei über das Internet mit dem Gerät um bspw. neue Software aufzuspielen. In manchen Fällen sind solche Geräte im Internet auffindbar, direkt erreichbar oder mit Standardkennwörtern gesichert.

Um Missbrauch, technische Defekte und insbes. im medizinischen Bereich Gefahren für Leib und Leben auszuschließen, wird empfohlen die Geräte nicht mehr öffentlich zugänglich zu machen. Insbesondere, wenn die Geräte nur Zugriff mit einer Kennung (Nutzername/Passwort) zulassen, dürfen die Wartungsschnittstellen nicht von außerhalb der Universität erreichbar sein.

Eine Abschottung der Geräte kann darüber geschehen, dass die Geräte in jeweilige spezielle interne Netzbereiche verschoben werden. Um Wartungen durchführen zu können, müssen die Dienstleister dann eine VPN-Verbindung zu diesem internen Netz aufbauen.

Da die VPN-Zugänge auf das jeweilige Wartungsnetz begrenzt sind und keine weiteren/höheren Dienste der WWU verwendet werden, die eine zentrale Nutzerkennung erfordern, ist es für den Dienstleister nicht nötig, der Nutzungsordnung des ZIV und der IVVen in allen Punkten zuzustimmen. Es reicht eine fallbezogene Nutzungsvereinbarung. Die Wartungskennung muss nicht personenbezogen sein, was dem Dienstleister ermöglicht die Kennung frei für seine Techniker zu Wartungszwecken zu verwenden. Die Kennung sollte jedoch nicht an Dritte (bspw. weitere Dienstleister) weitergegeben werden. Wartungskennungen sollten mit einem Ablaufdatum versehen werden. Es ist sinnvoll das Ablaufdatum passend zur Dauer des Wartungsvertrages zu wählen.

Abkürzungsverzeichnis

Abk.	Abkürzung
AD	Active Directory
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
LDSG NRW	Landesdatenschutzgesetz Nordrhein-Westfalen
mTAN	Mobile Transaktionsnummer
OTP	One Time Password
RDP	Remote Desktop Protokoll
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
VPN	Virtuelles privates Netzwerk
W-LAN	Wireless Local Area Network (kabelloses lokales Netzwerk)
WWUCA	Zertifizierungsstelle der WWU
ZIV	Zentrum für Informationsverarbeitung