Der folgende Text ist ein Entwurf und noch nicht als Artikel Bestandteil dieses Wiki!

Vereinsdatenschutzkonzept mit virtuellen Maschinen

Das **Vereinsdatenschutzkonzept mit virtuellen Maschinen** ist ein **experimenteller Ansatz** für ein IT-Datenschutzkonzept bei Vereinen und andere Organisationen, vor allem wenn ehrenamtliche Mitarbeiter auf privater Hardware (Bring your own device) für den Verein tätig sind.

Hier soll durch eine zentral gesteuerte Virtualisierung für einheitliche und sichere Verfahren gesorgt werden und zugleich der Schulungsaufwand gering gehalten werden, indem von den ehrenamtlich Tätigen, die keine Administratoren sind, nur die unter Nutzung aufgeführten Punkte umzusetzen sind.

Die folgenden Überlegungen beziehen sich primär auf den Teil des Datenschutzes der die IT betrifft.

Ausgangslage

Alle ehrenamtlichen Mitarbeiter mit eigener Hardware auszustatten und diese ordnungsgemäß zu administrieren überfordert in aller Regel die finanziellen und personellen Möglichkeiten von Vereinen. Dazu kommt bisweilen auch noch ein Akzeptanzproblem. (Wozu einen weiteren Computer - ich habe doch schon einen?)

Die Folge daraus ist eine für gewöhnlich sehr heterogene Infrastruktur, die entweder gar nicht geregelt ist oder es gibt sehr vage Regelungen, die nur sehr bedingt weiterhelfen, wie zum Beispiel „Virenscanner verwenden“.

Weiterhin werden Daten (im Zweifel auch sensible Personenbezogene Daten) auf unterschiedlichstens Speichermedien und in der Regel auch vielfach redundant gespeichert, was mannigfaltige Gefahren für den Datenschutz nach sich zieht.

Technischer Lösungsansatz und jeweilige Alternativen

Auf einem zentralen Server werden virtuelle Maschinen installiert. Die Ehrenamtler bekommen Zugangsdaten um eine Remote Desktop Verbindung von ihrer privaten Hardware aus aufzubauen. Für die private Hardware gibt es kaum Einschränkungen - heimischer Desktop-PC, Laptop, Tablett etc. sind ebenso wie unterschiedlichste Betriebssysteme[1)] möglich, so lange mindestens ein halbswegs moderner Browser zur Verfügung steht.

Im Testfall sah das so aus, dass auf einem Server Ubuntu (eine Linux-Distribution) als Betriebssystem installiert wurde. Darauf wurde VirtualBox als Virtualisierungslösung installiert und darin Windows 8.1

als Gastbetriebssystem auf das mittels Chrome Remote Desktop zugriffen wird. Zu den Details siehe unten Technische Umsetzung.

Variationen dieser Konfiguration sind natürlich fast nach Belieben möglich:

Server

Der Server muss nicht in der Cloud sein und erst recht nicht bei dem hier gewählten Anbieter. On Premises, also das „Blech“ vor Ort stehen zu haben, wird unter Vollkostenaspekten eher teuerer sein, denn Anschaffung einer geeigneten Maschine ist nicht alles. Es braucht auch einen geeigneten, sicheren Aufstellungsort, Wartung, elektrischen Strom und einen schnellen Internetzugang (geringe Latenz, hohe Bandbreite beim Upload). Das kostet. Bei einer Cloud-Lösung haben gegenwärtig (2019) die deutschen Anbieter gegenüber den amerikanischen Großkonzernen den Nachteil, dass sie eher langfristige Verträge anbieten. In der Einführungsphase mit verschiedenen Serverkonfigurationen testen, wird also sehr schnell teuer.

Ein AV-Vertrag wird in allen Varianten zwischen dem Verein und dem Hoster erforderlich sein, es sei denn, der Verein besitzt eigene Räumlichkeiten, in denen der Server unter eigener Hoheit des Vereins betrieben werden kann. Die Räumlichkeiten müssen auch dazu geeignet sein, dass darin ein Server betrieben wird.

Betriebssystem des Servers

Als Betriebssystem des Servers kann natürlich auch eine andere Linux-Distribution Verwendung finden.

Auf einem leistungsstarken Server und bei einem entsprechenden Budget für eine ordnungsgemäße Lizensierung, kann auch Microsoft Server verwendet werden. Der Vorteil dürfte vor allem in der eher laientauglichen Administration des Servers liegen. Linux ist doch zunehmend wieder eine Welt für Spezialisten.

Virtualisierung

Die Virtualisierungslösung VirtualBox ist nicht zwingend. VMware (korrekte Lizensierung beachten) und QEMU beziehungsweise andere Linuxalternativen sind ebenso denkbar. Von den Lizenzkosten der kommerziellen Varianten abgesehen, wird es auf den Server, sein Betriebssystem und das Gastbetriebssystem ankommen, mit welcher Kombination sich eine vernünftige Performance erreichen lässt.

Gastbetriebssystem

Beim Gastbetriebssystem ist Windows 8.1 keine optimale Lösung. Argumente dafür waren im Wesentlichen: 1. Es funktioniert. 2. Die Lizenzen dafür waren vorhanden.

Windows 7 wäre technisch sicher besser aber der Support endet Anfang 2020.

Damit bleiben als bessere Optionen hauptsächlich Windows 10 und eine Linux-Distribution. (Für weitere eher abseitige Alternativen gelten grundsätzlich die Ausführungen für Linux.)

Der stärkste Pluspunkt von Windows 10 ist die hohe Nutzerakzeptanz - ein (leider) kaum zu unterschätzender Aspekt. Der zweite Pluspunkt ist die umfassende Palette an Standardsoftware, wobei es natürlich gerade die Idee hinter diesem Konzept ist, die Menge an Programmen klein zu halten, die auf dem (virtuellen) Rechner installiert sind. Nachteile von Windows sind der relativ hohe Verbrauch an Ressourcen, die Anfälligkeit für Schadsoftware und natürlich kosten die Lizenzen, zumal im Regelfall Lizenzen für Windows 10 Pro benötigt werden.

Bei Linux ist es genau umgekehrt: Linux ist in aller Regel kostenlos. Das Sicherheitslevel ist von Hause aus sehr hoch. Bei einer geeigneten Einrichtung vor allem der graphischen Benutzeroberfläche ist auch der Ressourcenbedarf überschaubar. Hauptproblem ist zum einen die geringe Nutzerakzeptanz, vor allem wenn die grafische Benutzeroberfläche weit von einem aktuellen Windows entfernt ist, was wiederum für einen geringen Ressourcenbedarf nützlich ist. Zum anderen ist das Angebot an Standardsoftware eher bescheiden, wobei die Hauptproblemfelder hinsichtlich Akzeptanz Email-Client und Office-Lösung sowie bei der Beschaffung eine Vereinsverwaltungssoftware sein dürften. (Weiteres siehe unten Anwendungssoftware.)

Falls Linux einsetzt werden soll, kann mit leichten Abstrichen bei der Sicherheit aber dafür großen Vorteilen bei Performance und Ressourcenbedarf auf die Virtualisierung verzichtet werden: Die Nutzern erhalten Zugriff direkt auf den Server - natürlich mit eingeschränkten Rechten.

Anwendungssoftware

Die Anwendungssoftware sollte zentral vorgegeben werden. Das wird klassischerweise betreffen:

- Eine Office-Lösung. Marktbeherrschend ist hier Microsoft Office. Auch hier ist die nötige korrekte Lizensierung zu beachten. Freie Alternativen wie LibreOffice und Apache OpenOffice sind für normale Anwendungen sicherlich kaum schlechter aber sie erfordern Umstellungsaufwand.
- Ein Email-Client. Auch hier gilt es letztendlich Microsoft Outlook gegen kostenlose Alternativen wie Thunderbird abzuwiegen.
- Ein Webbrowser. Bei der beschriebenen Umsetzung ist Chrome notwendig. Wenn die Remote Desktop Verbindung auf einer anderen technischen Basis erfolgt, besteht natürlich die freie Auswahl. Neben dem Ressourcenbedarf und der Performance sollte beachtet werden, dass auch für den Browser ein möglichst strenges Berechtigungskonzept unterstützen sollte.
- Ein Messenger. An dieser Stelle sich für einen Messenger zu entscheiden, bedeutet sich gegen die verbreitetste Lösung WhatsApp zu entscheiden, weil WhatsApp zunächst immer auf einem Smartphone installiert werden muss. Das ist bei Alternativen wie Threema und Nextcloud anders. Hier können Accounts auch zentral eingerichtet werden und gegebenenfalls werden dann (zusätzlich) Clients auf Smartphones installiert.
- Eine Vereinsverwaltungssoftware. Für Windows 10 als Gastbetriebssystem gibt es fast unüberschaubar viele Lösungen, vom Allrounder bis zur hoch spezialisierten Software für spezielle Typen von Vereinen (z.B. Fördervereine, Kleingartenvereine). Für Linux ist das Angebot wesentlich geringer.[2)]

Backup

Zumindest die wesentlichen Daten sollten redundant gespeichert werden und es sollten regelmäßig

automatisch Backups durchgeführt werden.[3)]

Zukünftige Optionen

Angekündit aber noch nicht erschienen ist Windows 10 Multi User. Damit können mehrere Benutzer gleichzeitig mit einem Windows 10 arbeiten. Es vereint also für die hier geschilderten Zwecke die Funktionalität eines Servers auf dem mehreren virtuellen Maschinen mit Windows 10 instaliert sind. Auch hier dürfte gelten: Durch den Verzicht auf Virtualisierung gibt es Nachteile bei der Sicherheit, deren Umfang unklar ist, und im Gegenzug gibt es Vorteile bei Performance und Ressourcenbedarf.

Organisatorische Umsetzung

Unter der Annahme, dass sich die technische Infrastruktur so darstellt beziehungsweise darstellen soll, wie oben beschrieben, werden die folgenden organisatorischen Ansätze sinnvoll sein.

Adminstration

- Das gesamte System wie oben beschrieben, wird durch einen oder mehrere ausdrücklich dazu beauftragte Administratoren betreut.
- Wenn es nur einen Adminstrator gibt, sollte es für den Ausfall des Admins einen **Notfall-Plan** geben. Dazu muss geregelt werden,
  - wer,
  - unter welchen Voraussetzungen,
  - wie die nötigen Zugangsdaten erlangen kann.
- Wenn das nötige Wissen zur Administration fehlt, ist auch eine (allerdings kostenträchtige) externe Vergabe möglich. Wesentliche Punkte hier:
  - Zuverlässiger Auftragnehmer,
  - Abschluss eines AV-Vertrages.
- Administration und Benutzung des Systems sind technisch zu trennen. Wenn beide Rollen in einer Person zusammenfallen, sind für diese Person zwei getrennte Konten anzulegen.
- Die Administration sollte auf externen Datenträgern (externe Festplatten im Wechsel oder DVD) regelmäßig Backups zusätzlich zu den automatischen Backups des Servers durchführen. Das Intervall ist nach den Gegebenheiten des Vereins festzulegen. (Schutz vor Ransomware[4)])
- Das Einspielen eines Backups sollte regelmäßig, wenigstens jährlich getestet werden.
- Accounts für Nutzer sollten
  - mit nicht-trivialen Accountnamen angelegt werden (siehe unten zum Adminaccount),
  - zumindest bei Zugriff auf etwas sensiblere Daten personengebunden sein (keine Sammelaccounts für z.B. eine Abteilung des Vereins; individuelle VM für jeden Benutzer ist nicht notwendig).

Nutzung

Die folgenden Punkte sind der Teil, der von den ehrenamtlich Tätigen umzusetzen ist, was sich der Verein schriftlich bestätigen lassen sollte.

Virtuelle Maschine

- Zugangsdaten (Passwort aber auch Accountname) geheim halten
- Ausschließliche Nutzung für die ehrenamtliche Tätigkeit
- keine private Nutzung
- Email-Client nur für den Vereins-Emailaccount
- Installation von zusätzlicher Software nur durch Administrator

(Privates) Hostsystem

Hier können und sollten tatsächlich die „üblichen“ Empfehlungen gegeben werden.

- Regelmäßige Updates
- wo nötig Virenscanner
- keine illegale Software
- keine gecrackten Softwareversionen
- kein gerootetes Betriebssystem (mobile Geräte mit Android und iOS; bei Linux nicht als Root standardmäßig arbeiten)
- Anmeldung mit nicht-trivialem Passwort (eher mindestens 12 Stellen aber merkbar)

Technische Umsetzung

Unter azure (andere Anbieter sind grundsätzlich genauso möglich) einen Linux-Server (z.B. B2s Maschine mit 2 vCPU, 4 GiB RAM, 8 GiB Temp Speicher) mit Ubuntu einrichten.

Admin Account mit Passwort einrichten. (Admin Account für SSH wäre auch möglich, dann muss das Passwort aber später manuell eingerichtet werden) Der Accountname sollte nicht ganz trivial sein (zum Beispiel „Admin“), sondern etwas komplexer ausfallen. Das ist zwar keine Zwei-Faktor-Authentifizierung[5] aber etwas mehr Schutz bieten individuelle Accountnamen schon.

Als zusätzlicher Datenträger sollte eine SSD mit mindestens 64 GB genutzt werden. (Abhängig von der Anzahl der VM´s und der Software, die verwendet werden soll aber bei VM´s mit Windows sollten allein dafür 10-20 GB je VM eingeplant werden.)

Anmelden

```
sudo apt-get update
```

XFCE installieren. (XFCE ist eine graphische Benutzeroberfläche, die wenig Ressourcen benötigt.)

```
sudo apt-get install xfce4
```

Remotedesktopserver installieren.

```
sudo apt-get install xrdp
sudo systemctl enable xrdp
```

XFCE in Remote-Session verwenden.

```
echo xfce4-session>~/.xsession
sudo service xrdp restart
```

Remote-Session starten. 2 Warnungen wegclicken. Unter graphischer Benutzeroberfläche anmelden. (Dafür braucht es einen Account mit Passwort-siehe oben.)

Entwurf

1)

Bei der hier vorgestellten Lösung können auf dem Client, also der Hardware, auf der der Ehrenamtler arbeitet, als Betriebssystem Windows, Linux, Chrome OS, OS X, iOS oder Android installiert sein.

2)

Bei einer kurzen Recherche ist eigentlich nur JVerein aufgefallen. Zu Prüfen wäre im Einzelfall, ob unter dem installierten Linux ein Windows-Programm mittels Wine PlayOnLinux sinnvoll genutzt werden kann. Im Regelfall sollten das Programm an sich laufen. Kritisch und daher unbedingt zu testen sind die Performance und vor allem die Schnittstellen zur Office-Lösung und zum Web-Client.

3)

Siehe in der Wikipedia Datensicherung

4)

Siehe in der Wikipedia Ransomware

5)

Vgl. Artikel in der Wikipedia.