Dokumentation

TOM
(technisch organisatorische Maßnahmen)
Anonymisiertes Beispiel
Für Sesam Hannover

Günther Hellberg

08 / 2019

Dokumentation

Inhaltsverzeichnis

1 Ausgangslage / Zielsetzung

In diesem Dokument sollen noch einmal die wichtigsten TOM (technisch-organisatorischen Maßnahmen) im Überblick beschrieben werden. Die detaillierten Ausführungen wurden stets begleitend zur Planung und Realisierung der einzelnen Projekte / Themen erstellt und sind in separaten Dokumenten abgelegt. Dort sind die Einzelheiten für Fachkundige detailliert beschrieben – hier wird bewußt auf eine zu hohe Granularität zugunsten der Verständlichkeit und Lesbarkeit verzichtet (zudem würden ggfls. zu viele Details an Dritte verraten werden). Mit diesem Dokument soll vielmehr ein guter Überblick über die bei Sesam Hannover realisierten und geplanten Verfahren und Maßnahmen mit der speziellen Ausrichtung auf die DSGVO-EU gegeben werden. Dadurch bleibt der Umfang noch einigermaßen in einem überschaubaren Rahmen und führt so zu einer höheren Übersicht. Zudem kann auf diese Weise leichter sichergestellt werden, dass die Inhalte dieses Dokumentes nahe an den aktuellen Gegebenheiten bleiben.

Sesam Hannover betreibt in großen Teilen eine eigene IT-Infrastruktur für ca. 250 Mitarbeiter in einem Hauptgebäude und einer Aussenstelle (Sesam2), die per VPN angebunden ist.

Die interne IT befindet sich überwiegend in einem Serverraum mit diversen Serverschränken, der auch klimatisiert und gegen unbefugten Zutritt geschützt ist. Hier befinden sich alle wesentlichen zentralen IT-Komponenten (für eine detaillierte Aufstellung und Beschreibung siehe extra Dokumente).

Jedoch gibt es derzeit auch noch einige Teile der IT, die ausgelagert sind – wie z.B. Email, Cloud etc. . Auf diese Systeme wird im folgenden auch noch im Detail eingegangen, um auch genau die Schittstellen mit deren Herausforderungen präzise zu beschreiben.

2 TOM (technisch organisatorische Maßnahmen)

2.1 Allgemeines

Die technisch organisatorischen Maßnahmen (im folgenden TOM) werden geplant und umgesetzt, um folgende Schutzziele zu erfüllen / realisieren:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit

In diesem Dokument wird davon ausgegangen, dass die grundlegenden Begrifflichkeiten bekannt sind (bzw. sind sie an anderer Stelle ausführlich definiert und beschrieben). Weiterhin wird in diesem Dokument vorausgesetzt, dass die DSGVO und deren Rahmenbedingungen bekannt sind, so dass an dieser Stelle aus Gründen des Umfanges auf diesbezügliche Erläuterungen verzichtet wird. Vielmehr wird in den folgenden Abschnitten auf die sieben wesentlichen Aspekte im direkten Bezug zu Sesam Hannover eingegangen.

Den einzelnen Aspekten wird im folgenden jeweils ein einzelner Abschnitt gewidmet, der jeweils in extern und intern unterteilt ist.

2.2 Physische Sicherheit

Extern

- Schutz von Rechenzentren
- Redundanz
- Zugang zu Datenverarbeitungsanlagen

Der Serverraum der Sesam ist gegen den Zutritt von Unbefugten mit Transpondern geschützt. In das gesamte Gebäude von Sesam gelangt man auch nur durch vorherige Anmeldung im Empfang oder mit Hilfe eines Transponders / Schlüssels. Selbstverständlich werden dabei alle arbeitsrechtlichen und brandschutztechnischen Aspekte berücksichtigt. Die zentralen IT-Systeme sind zudem gegen Überspannung etc. geschützt, indem diverse unterschiedliche Stromkreise ausgeführt wurden. Die verschiedenen Serversysteme sind weiterhin mit – meist einzelnen – USV-Systemen (unterbrechungsfreie Stromversorgung) gegen einen plötzlichen Stromausfall geschützt. Der gesamte Serverraum ist klimatisiert, so dass das Risiko eines Ausfalls durch Überhitzung als sehr gering eingestuft werden kann (es könnte noch eine Überwachung der Temperatur des Serverraumes mit Meldung per sms nachgerüstet werden). Die zentralen Datenverarbeitungsanlagen sind allesamt gegen den direkten physikalischen Zugriff geschützt – zusätzlich dadurch, dass sich die Serversysteme in eigenen Racks befinden.

Intern

- Gilt nur für die Infrastruktur von Sesam
- Zutrittskontrolle
- Schutz von Rechenzentren und Redundanz an Standards orientiert

Die Betrachtung Intern ist bezogen auf diesen Aspekt identisch.

2.3 Server Sicherheit

Extern

- Firewalls und Intrusion Detection Systeme
- Unnötige Dienste deaktiviert / deinstalliert

Die zentralen Server-Systeme von Sesam sind gegen den unberechtigten Zugriff von außen (und teilweise von innen) auch aus logischer Sicht sehr gut geschützt. Dazu wurde Anfang 2017 ein völlig neues Firewallsystem der Firma Securepoint angeschafft und eingerichtet. Dieses System wurde sogar zusätzlich redundant in Form eines Fail-over-Clusters ausgeführt, so dass im Falles eines totalen Ausfalls der primären Firewall die sogenannte „Spare"-Firewall die Funktionalität automatisch übernimmt und somit einen fast unterbrechungsfreien Betrieb ermöglicht. Das gesamte Firewall-Konzept wurde völlig neu ausgearbeitet und an die aktuellen Anforderungen angepasst. Dabei wurden im wesentlichen drei verschiedene Zonen realisiert:

- Die externe Zone zur Anbindung an den Provider Internetti
- Die interne Zone zur Anbindung der Clients von Sesam
- Eine DMZ Zone zur Anbindung der Aussenstelle (Sesam2) via VPN

Als wesentliche Funktionalitäten wurden Antivirenschutz, Content-Filterung, sehr restriktive Beschränkungen des eingehenden und ausgehenden Netzwerkverkehrs und ein http-Proxy für das Surfen im Internet eingerichtet. Weiterhin wird die Firewall kontinuierlich durch die IT-Administratoren gepflegt, überwacht und angepasst.

Als eine weitere wesentliche Verbesserung / Optimierung wurden im Rahmen der Planung und Umstellung fast aller Services und Dienste alle unnötigen Dienste / Server abgeschaltet bzw. deaktiviert. Somit ist weitestgehend sichergestellt, dass Angreifer nicht auf Systeme zugreifen können, die gar nicht mehr benötigt werden. Die Überprüfung auf nicht mehr benötigte Systeme / Dienste wird in regelmäßigen Abständen wieder vorgenommen (spätestens alle drei Monate).

Intern

- Unnötige Dienste deaktiviert / deinstalliert
- Härtungsstandard für jedes System -> Firewall-Einstellungen

Der Aspekt unnötige Dienste ist analog zu extern zu betrachten.
Die einzelnen Systeme wurden im Rahmen der Migration auf die neuen Serversysteme mit Hilfe einer Checkliste einheitlich optimiert und sicherer gemacht. Die älteren Systeme konnten nur in Rahmen der Möglichkeiten gehärtet werden, was jedoch nicht so sehr ins Gewicht fällt, da alle Systeme durch die Firewall abgesichert sind und die älteren bereits entweder in bälde abgeschaltet oder ersetzt werden.

2.4 Netz Sicherheit

Extern

- Virenschutz
- Netzsegmentierung
- Verschlüsselte Kommunikation

Das gesamte Netzwerk von Sesam wird durch den Firewall-Cluster gegen Virenbefall von aussen geschützt. Als zusätzliche Maßnahme gegen Virenbefall oder Malware wird bei Sesam ein Antiviren-Server der Firma MCAffee betrieben, über den die Clients mit einem zusätzlichen Virenschutz versehen sind. Die aktuellen Virensignaturen werden automatisch verteilt bzw. aktualisiert.

Das Netzwerk von Sesam ist zwecks besserer Administration und Wartbarkeit in diverse Segmente unterteilt (siehe auch 2.3 die Zonen des Firewall-Clusters). Dieses findet jedoch derzeit nur auf logischer Ebene statt. Als eine weitere Optimierung ist eine Unterteilung des Netzwerkes in

mehrere physikalische Segmente bereits konzipiert und geplant. Damit ist eine Erhöhung des Sicherheitsniveaus und der Performance zu erwarten. Im Zuge dieser Umstellung werden auch bereits Anfang 2018 angeschaffte GBit-Switche und Mini-Gbics ausgetauscht. Damit wird die Bandbreite für die Clientsysteme deutlich erhöht.

Bei der Migration der alten Serversysteme auf die neuen im 4.Quartal 2017 und 1. Quartal 2018 wurde die Anbindung dieser Systeme an die Clients völlig neu konzipiert und realisiert. So ist beispielsweise der Storage-Cluster in einem eigens realisierten, separaten physikalischem 10GB Netzwerk mit den ausführenden Servern (ESXi von VMware) mit separaten 10GB-Switchen angebunden. Somit ist ein Zugriff auf diese Systeme von aussen als fast unmöglich einzustufen.

Die Kommunikation bei Sesam findet in den relavanten Bereichen verschlüsselt statt. Das betrifft z.B. das externe Email-System beim Provider 2&2, die externe Cloud-Lösung etc.
Bei dem separaten, internen Storage-Netzwerk wurde auf die Verschlüsselung komplett verzichtet, da sie an dieser Stelle nicht notwendig ist, sondern nur die Performance beeinträchtigen würde.

Weiterhin wurde bereits im Jahr 2017 eine Konzeption für die Verschlüsselung der Daten auf den Clientsystemen – insbesondere von Notebooks – besprochen, konzeptioniert und geplant. Die ersten Systeme sind bereits im 2. Quartal 2018 mit Hilfe der Lösung Bitlocker von Microsoft verschlüsselt worden. Dabei werden die Systeme mit Hilfe der IT-Administratoren verschlüsselt, der Wiederherstellungsschlüssel wird dabei in Papierform sicher verwahrt. Der Anwender schützt das System durch einen mindestens sechstelligen PIN.

Intern

- Vorgaben an Virenschutz-Software
- Gesicherte Verbindung durch
    - Netzsegmentierung
    - Verschlüsselung
    - Andere geeignete Technologien

2.5 Anwendungs- und Plattform-Sicherheit

Extern

- Vorgaben zu sicherer Softwareentwicklung
- Trennung verschiedener Anwendungen

Bei Sesam werden im Verwaltungsbereich überwiegend gekaufte Softwarelösungen eingesetzt, so dass hier gar keine Software selber entwickelt wird. Im Forschungsbereich findet vereinzelt jedoch Softwareentwicklung statt, die jedoch nur auf separaten Insellösungen eingesetzt wird, so dass immer noch ein angemessenes Sicherheitsniveau gewährleistet ist.

Die einzelnen benötigten Services/ Dienste/ Anwendungen bei Sesam sind in optimaler Weise getrennt. Das ist dadurch perfekt realisiert, weil bei Sesam die Infrastruktur durch virtuelle Systeme auf separaten virtuellen Server-Systemen (vms) aufgebaut wurde. Auf diese Weise sind Wechselwirkungen von Anwendungen auf einem Server-System so gut wie ausgeschlossen. Der einzige Nachteil ist die etwas höhere Anzahl an zu verwaltenden virtuellen Systemen (diese sind wie in der Einleitung beschrieben in einer seperaten Dokumentation aufgelistet und beschrieben).

Intern

- Vorgaben zu sicherer Softwareentwicklung
- Bewertung von fremdentwickelter Software
- Patch Management für Plattformsicherheit

Vorgaben zu sicherer SWE sollten bei Sesam noch weiter ausgearbeitet werden, es betrifft jedoch fast ausschließlich den Forschungsbereich.

Fremdentwickelte Software wird bereits schon seit längerer Zeit im Rahmen von Ausschreibungen, Pflichtenheften, Anforderungskatalogen und Tests bewertet. Es gibt keinen Grund, die Vorgehensweise zu ändern.

Das Patchmanagement bei Sesam erfolgt mit Hilfe verschiedener Verfahren. Die Clients werden über die Firewall / über das Internet mit aktuellen Sicherheitsupdates versorgt. Die Virensignaturen werden ebenso auf dem aktuellen Stand gehalten.

Die Serversysteme werden jedoch in regelmäßigen Abständen durch die IT-Administratoren manuell vorgenommen, um Fehlfunktionen aufgrund von Updates möglichst ausschließen zu können. Dies ist sehr effizient, da mit Hilfe der virtuellen Maschinen ein vorheriger Test der Updates ohne Risiko möglich ist. Außerdem können die Administratoren auch erst abwarten, ob ein Update eventuell Schwierigkeiten macht (z.B. Meltdown und Spectre, etc.).

Weitere Funktionalitäten und Einstellungen werden auch mit Hilfe von Gruppenrichtlinien über das AD (Microsoft Active Directory) auf die Clients verteilt.

Zusätzlich wurde bereits ein Prototyp eines Serversystems für die Softwareverteilung eingerichtet und ein erster Test für die Softwareverteilung damit durchgeführt. Aufgrund der aktuellen hohen Arbeitsbelastung der IT-Abteilung wird dieses System allerdings derzeit noch nicht in den Produktivbetrieb geschaltet, da auch derzeit durch die oben beschriebenen anderen Verfahren eine hinreichend gute Verteilung gewährleistet ist. Für die zukünftige Optimierung der Arbeitsbelastung ist der Einsatz jedoch vorgesehen.

2.6 Datensicherheit

Extern

- Trennung von Kundendaten
- Regelmäßige Backups
- Informationen über Backups

Bei Sesam werden die Daten – wie bereits in den obigen Abschnitten beschrieben – in separaten virtuellen Systemen gespeichert, so dass ein maximales Maß an Trennung bereits dadurch gewährleistet ist. Z.B. existiert ein eigenes ERP-System, ein eigenes System für die internen Emails, etc.
Aufgrund der stets wachsenden Anforderungen an den Schutz von Kundendaten wurde bereits im Jahr 2017 eine neue Konzeption für die Ablage von Dateien begonnen. Dazu wurden verschiedene Lösungsansätze in Betracht gezogen und die Anforderungen der Fachabteilungen aufgenommen. Da bei Sesam ein Microsoft AD Verzeichnisdienst Verwendung findet, fiel die Entscheidung darauf, auch das neue Berechtigungskonzept mit Hilfe des Active Directory (AD) umzusetzen.
Da jedoch das alte, bestehende AD historisch lange gewachsen und schlecht bis gar nicht dokumentiert ist, fiel der Entschluß auf die Neuimplementation eine AD. Das ausgearbeitete Konzept liegt derzeit noch zur Prüfung bei den Abteilungsleitern der Fachabteilungen und der Geschäftsführung. Die Umsetzung erfolgt gerade prototypisch im „Kleinen“. Der komplette Neuaufbau und die Inbetriebnahme des neuen AD ist für das 3. Quartal 2018 vorgesehen.

Das Backupverfahren der zentralen Serverssysteme ist in einer seperaten Dokumentation detailliert beschrieben. An dieser Stelle sollen nur die wesentlichen Grundzüge dargestellt werden. Die Datensicherung erfolgt derzeit täglich in Form von Snapshots auf den vorhandenen Filersystemen. Es existieren zwei Filer-Systeme, die jeweils als RAID-Systeme mit Spare-

Festplatten ausgeführt sind. Die beiden Filer-Systeme replizieren sich „über Kreuz“, so dass alle derzeitigen Bewegtdaten stets auf zwei verschiedenen physikalischen Systemen, die jeweils noch lokal Redundanzen besitzen, vorliegen. Wie oben ausgeführt, sind die Filer-Systeme durch USVs abgesichert und befinden sich in dem klimatisierten Serverraum.
Hinzu kommt, dass von dem Filer-System einmal pro Woche (Freitags) eine komplette Sicherung (Fullbackup) auf eine Tape-Library vorgenommen wird. Die Bänder der Tape-Library werden monatlich manuell ausgetauscht und in einem feuerfesten Tresor gelagert (Das Tauschen wird protokolliert). Zusätzlich wird ein Satz Bänder in einem weiteren feuerfesten Tresor in einem anderen Gebäudetrakt gelagert. Somit ist ein hohes Maß an Redundanz (auch bezogen auf den Aufbewahrungsort) gegeben.
Bis auf das Tauschen der Bänder, erfolgen die Verfahren automatisch und bedürfen keines manuellen Eingriffs. Die Datensicherungen werden durch die Software mitprotokolliert / geloggt.

Weiterhin werden von einigen Clients (auch im Verwaltungsbereich) werden zusätzlich Backups mit Hilfe von Acronis bei Bedarf erstellt, um diese Systeme im Falle einer Störung schnell wieder funktionsfähig machen zu können.

Derzeit wird an einer Konzeptionierung für das Backup der Emails und der Emailsysteme gearbeitet. Eine Umsetzung ist noch für Ende diesen oder Anfang des nächsten Jahres angedacht. Allerdings spielen die Aspekte Spam und Archivierung noch eine Rolle.

Intern

- Regelmäßige Backups
- Räumliche Trennung von Datenhaltung

Siehe oben extern.

2.7 Verschlüsselung und Schlüsselmanagement

Extern

- Verschlüsselung bei Transport und Speicherung
- Schlüsselmanagement: Kunde oder Cloud-Anbieter
- Sicherheit der Schlüssel gewährleisten

Wie bereits im Abschnitt 2.4 beschrieben, erfolgt die Kommunikation bei Sesam in den relavanten Bereichen verschlüsselt. Das betrifft z.B. das externe Email-System bei 2&2, die externe Cloud-Lösung etc.
Die Client-Systeme werden mit Hilfe der IT-Administratoren verschlüsselt, der Wiederherstellungsschlüssel wird dabei in Papierform sicher verwahrt. Der Anwender schützt das System durch einen mindestens sechstelligen PIN. Auf diese Art und Weise kann die Sicherheit der Schlüssel weitestgehend gewährleistet werden.

Intern

- Verschlüsselung bei Transport oder Speicherung außerhalb von Sesam
- Schlüsselmanagement durch IT-Betrieb

Siehe extern.

2.8 Identifikation- und Rechtemanagement

Extern

- Zwei-Faktor-Authentisierung
- Vier-Augen-Kontrolle
- Nur notwendige Berechtigungen
- Protokollierung

Bei Sesam ist der Schutzbedarf (noch) nicht so hoch, dass derzeit eine 2FA oder eine Vier-Augen-Kontrolle benötigt und eingesetzt wird.

Allerdings wird derzeit sehr aktiv an der Umsetzung der neuen Berechtigungsstruktur (siehe 2.6 neues AD) gearbeitet und es ist in einer nächsten Phase geplant, das die normalen Anwender nur mit Benutzerrechten arbeiten und nicht mit „Administrator-Berechtigungen“. Dazu wurde ein Verfahren zum automatischen Setzen / Ändern des Administratorkennwortes ausgewählt und bereits prototypisch getestet (LAPS von Microsoft). Dies soll nach Rücksprache dann im 3. Quartal 2018 umgesetzt werden. Mit Beendigung dieser Projektphase wäre ein großer Schritt in Richtung „nur notwendige Berechtigungen“ getan und erfüllt.

Die Protokollierung wird seit dem Januar 2017 sehr detailliert und akribisch für die Änderungen und Vorfälle der Systeme durch die IT-Administratoren durchgeführt. Das erfolgt mit Hilfe von Screenshots (Werkzeug Irfanview, mit Datum, Uhrzeit des Screenshots) begleitend zu administrativen Tätigkeiten und Eintragungen in sog. „Ereignisslisten“ (Werkzeug Excel) einmal für alle Serversysteme und eine extra Ereignissliste für Vorfälle beim Firewall-Cluster. Natürlich werden auch die normalen Protokollierungen der Systeme verwendet (FW-Logging, Microsoft-Ereignisanzeige, Unix/Linux /var/log/messages etc.).

Intern

- Zugriff über Benutzerkennung und Passwort
- Hochsensible Daten: Zwei-Faktor-Authentisierung
- Nur notwendige Berechtigungen
- Jährliche Prüfung
- Protokollierung

Zum Abschnitt intern kann nur noch ergänzt werden, dass die normale Authentifizierung über Benutzername und Passwort erfolgt, welches dann per Gruppenrichtline im AD in regelmäßigen zeitlichen Abständen geändert werden muss und eine minimale Komplexität aufweist.

Dadurch, dass seit 2016 eine ständige Planung und Konzeption der verschiedenen Tätigkeiten und Aktivitäten innerhalb der IT vorgenommen wird (mindestens einmal pro Monat im Team!), werden alle diese Aspekte regelmäßig überprüft und protokolliert.

Die wesentlichen Bereiche werden also bei Sesam wohl eher spätestens alle sechs Monate überprüft und stets begleitend dokumentiert / protokolliert.

3 Weitere Informationen / Quellen

Die weiteren, detaillierten Informationen finden sich in den einzelnen Dokumentationen für die einzelnen Systeme. Sie liegen in den entsprechenden Ordnern auf dem Fileserver in der Abteilung IT in Unterordnern. Dort befinden sich die Ereignislisten, Schaubilder, Screenshots, Dokumentationen. Weitere Informationen – wie bespielsweise der Gebäudeplan, Eplan, Netzwerkplan etc. – befinden sich in „Leitz-Ordnern“ in Papierform in der Abteilung TD / IT. Diese Informationen würden den Rahmen dieser TOM sprengen und auch unnötig viele Details an Dritte verraten.

Zusätzlich existieren für Sesam natürlich bereits seit längerem noch Mitarbeiterhandbuch, Vereinbarungen etc., in denen Prozesse, Anweisungen, Abläufe etc. präzise dargestellt sind.

Hannover, Juli 2019

G. Hellberg