hrung.aux

teleinformatik
INNOVATION ERLEBEN

Swiss Medical Clinic
COMPLEMENTARY ONCOLOGY LYME DISEASE MEDICAL CHECK-UP

IT Security Audit
Swiss Medical Clinic

Teleinformatik Services AG
Abteilung Informatik
Schulstrasse 37
CH-8050 Zürich

Vertraulich

Auftraggeber:	Swiss Medical Clinic, Grütstrasse 55, CH-8802 Kilchberg ZH
Autor:	David Meister, Security Engineer, Teleinformatik Services AG
Mitwirkende:	Giorgio Vincenti, Head of IT, Teleinformatik Services AG
	Daniel Luetold, Systems Engineer, Teleinformatik Services AG
	Dr. med. Anwar Giryes, Swiss Medical Clinic
	Tochter von Giryes, Swiss Medical Clinic
Datum:	15. März 2019

Inhaltsverzeichnis

1. Übergreifende Aspekte

1.1 Personal und Organisation

In diesem Bereich werden organisatorische und personelle Aspekte im Zusammenhang mit IT Sicherheit eines Unternehmens beleuchtet. Es werden zuerst mögliche Gefährdungen mit der IST Situation abgeglichen und geeignete Massnahmen abgeleitet.

1.1.1 Gefährdungen

Fehlende oder unzureichende Regelungen Die Wichtigkeit und Notwendigkeit von Regelungen nimmt mit steigender Grösse der Organisation oder dem Schutzbedarf stetig zu. Mitarbeiter einer Unternehmung sind sich häufig der Auswirkungen Ihres Handelns im Bezug auf die Informationssicherheit gar nicht bewusst. Regelungen und Weisungen können dieses Risiko minimieren, da der Mitarbeiter sich nur an die Weisung selbst zu halten hat, die Hintergründe aber nicht im Detail verstehen muss. Beispiele wären z.B. Weisung zur Internetnutzung, ändern von Kennwörtern etc.

Fehlende oder unzureichende Wartung Das bestehende IT System muss regelmässig gewartet werden. Nach erfolgreicher Inbetriebnahme eines Systems oder teile eines Systems muss in periodischen, festzulegenden Abständen Wartungen durchgeführt werden. Dies betrifft zum Einen Betriebssysteme und Software, da durch die Anbindung ans Internet Schwachstellen ausgenutzt werden können, als auch Hardware, welche bei einem Ausfall grosse Teile des Betriebs und wichtige Geschäftsprozesse beeinträchtigt werden können.

Unbefugter Zutritt zu den aktiven Netzkomponenten In einer Unternehmung werden an diversen Stellen im Gebäude aktive Netzwerkkomponenten wie Firewalls, WLAN Access Points, Server oder LAN Switches benötigt. Durch ungenügenden physischen Schutz droht Manipulation oder Ausfall dieser Komponenten. Häufig ist der Zugang zum Haupt-Rack relativ gut geschützt, Zugriffe auf andere aktive Komponenten ausserhalb dieses Racks werden jedoch häufig vergessen.

Gefährdung durch Fremdpersonal Externe Mitarbeiter besitzen häufig ein Client Gerät, welches nicht von der eigenen Unternehmung beschafft und installiert wurde. Somit kann man auch nicht sicherstellen, dass die geforderten Sicherheitsstandards eingehalten werden. Dies kann zum Beispiel auch Datenträger wie USB Sticks beinhalten, welche unter Umständen virenbefallene Daten beinhalten und auf das eigene IT System übertragen werden.

Diebstahl Durch Diebstahl von Geräten oder Zubehör entstehen dem Unternehmen Kosten in Form von der Neubeschaffung der Hardware, der Wiederinbetriebnahmen und eventuellen Datenverlust. Vor allem Letzteres kann ein Unternehmen vor grosse Probleme stellen, wenn Betriebsgeheimnisse oder der Datenschutz verletzt werden.

Fehlerhafte Nutzung von IT Systemen Die Sicherheit eines Systems kann unter Umständen durch unsachgemässe Bedienung der Benutzer oder Administratoren beeinträchtigt werden. Beispielsweise kann von einem Benutzer aus Versehen eine vertrauliche Datei an den falschen Ort gespeichert werden oder eine Arbeitsstation nach gebraucht nicht gesperrt werden. So wäre es beispielsweise möglich, dass vertrauliche Informationen in falsche Hände gerät.

Ungeeigneter Umgang mit Authentisierungsmechanismen Authentisierungsmechanismen dienen zur Überprüfung der Identität eines Benutzers. Aus Bequemlichkeit werden diese häufig aufgeschrieben (z.B. auf einem Zettel unter der Tastatur) oder sie werden mit anderen Personen in der Unternehmung geteilt. Ein Benutzerpasswort darf nur einem einzigen Benutzer bekannt sein, ansonsten droht unbefugter Zugriff und im Falle eines Sicherheitsvorfalls kann nicht verifiziert werden, welche Person mit dem System gearbeitet hat.

Social Engineering Social Engineering ist die mit Abstand erfolgsversprechendste Attacke auf ein IT System. Der Angreifer versucht, unbefugt an sensitive Informationen zu gelangen oder in ein System einzudringen. Das Vorgehen ist denkbar einfach: Es wird versucht, nach diesen Informationen oder Zugängen „zu fragen". Der Angreifer gibt sich dabei z.B. als Mitarbeiter der IT Organisation oder Elektriker aus, der gutgläubige Mitarbeiter verschafft dem Angreifer Zugang zum System.

1.1.2 IST Situation

Fehlende oder unzureichende Regelungen Todo: nochmals nachfragen!
Zum heutigen Zeitpunkt existieren keinerlei Dokumente, welche Weisungen für die Benutzer des IT Systems der Swiss Medical Clinic enthalten.

Fehlende oder unzureichende Wartung Das bestehende IT System wird regelmässig (halbjährlich) von der Firma Teleinformatik Services AG gewartet (sog. Maintenance Check). Gemäss jahrelang erarbeiteter Standards werden wichtige Updates für Server, Clients und aktive Netzwerkkomponenten eingespielt. Da die IT Infrastruktur der Swiss Medical Clinic in einigen wichtigen Punkten stark von den Teleinformatik Services AG Standards abweicht ist der Maintenance Check betreffend IT Security in vielen Teilen ungenügend. Insbesondere fehlen periodische Update von Servern und Clients, da das Betriebssystem Mac OS verwendet wird. Der letzte durchgeführte Maintenance Check hat im Februar 2018 stattgefunden.

Unbefugter Zutritt zu den aktiven Netzkomponenten In den Räumlichkeiten der Swiss Medical Clinic befinden sich zwei 19 Zoll Racks für aktive Netzwerkkomponenten. Im unteren Stockwerk befinden sich Komponenten wie Server, Switch, Firewall und Internet Router. Im oberen Rack befindet sich lediglich ein LAN Switch. Der Zugang im unteren Rack ist vor Unbefugten geschützt, solange der Raum abgeschlossen ist. Die Racks selbst haben keine verschliessbare Türe. Im oberen Rack besteht keine Sicherung vor Unbefugten. Es existiert keine Videoüberwachung.

Gefährdung durch Fremdpersonal Gemäss Angaben der Swiss Medical Clinic arbeiten gelegentlich externe Ärzte in den eigenen Räumlichkeiten. Diese bringen ihre eigenen Client Geräte mit. Daten werden Teils mit USB Sticks/Festplatten ausgetauscht. Das Reinigungspersonal befindet sich ebenfalls regelmässig in der Räumlichkeiten und hätte potenziell Zutritt zu aktiven Netzwerkkomponenten. Die Sicherheit basiert hier vollständig auf Vertrauen.

Diebstahl Potenziell könnten sämtliche Client Geräte wie PCs, Notebooks und iPads von Diebstahl betroffen sein. Besonders heikel sind sich darauf befindende schützenswerte Daten. Die Festplatten, seien es externe oder client-interne, sind nicht verschlüsselt und somit nicht genügend geschützt im Falle eines Diebstahls. Die Festplatten des Fileservers befinden sich in einem abgeschlossenen Raum und sind deshalb schwieriger zu entwenden.

Fehlerhafte Nutzung von IT Systemen Dieser Punkt ist schwierig zu erheben. Man muss in aller Regel davon ausgehen, dass ungeschulte Benutzer nicht genügend sensibilisiert im Umgang mit IT Sicherheit sind. Es existieren keine technischen Richtlinien für automatisches Ändern des Benutzerkennworts oder Sperren des Bildschirms. Ebenfalls gibt es keine technische Richtlinie für die Komplexität des Benutzerkennworts. Es werden ebenfalls teils sensitive Daten auf den Desktop des PCs oder externe Datenträger gespeichert.

Ungeeigneter Umgang mit Authentisierungsmechanismen In der Swiss Medical Clinic werden gewisse Benutzerpasswörter untereinander geteilt und gar gleiche Benutzeraccounts für unterschiedliche Personen verwendet, Beispiel wäre hier der MPA Account. Unbekannt ist, ob irgendwelche Kennwörter aufgeschrieben sind (z.B. Zettel auf Bildschirm oder unter Tastatur, Ablage in Ordnern), was dringend unterlassen werden sollte.

Social Engineering Bisher wurde noch nicht überprüft, ob eine Social Engineering Attacke funktioniert. Man muss aber davon ausgehen, dass ohne weitere Schulung der Mitarbeiter und Richtlinien im Umgang mit unbekannten Personen eine solche Attacke sehr erfolgsversprechend sein wird.

1.1.3 Massnahmen

Gefährdung	**Massnahme**
Fehlende oder unzureichende Regelungen	- Dokument zur Nutzung der IT Systeme erstellen - Dokument bei Eintritt unterzeichnen lassen.
Fehlende oder unzureichende Wartung	- Wartung häufiger und zuverlässiger durchführen lassen - Standardwartung Teleinformatik auf IT Sicherheits Bedürfnisse der Swiss Medical Clinic anpassen
Unbefugter Zutritt zu den aktiven Netzkomponenten	- Racks mit verschliessbaren Türen beschaffen - Sämtliches sonstiges Material aus Serverraum entfernen - Wichtige Bereiche mit Kameras überwachen - Serverkomponenten in Rechenzentrum auslagern
Gefährdung durch Fremdpersonal	- Fremde Notebooks nicht in produktives Netzwerk zulassen
Diebstahl	- Diebstahlschutz für Notebooks und PCs installieren - Verschlüsselung der Datenträger
Fehlerhafte Nutzung von IT Systemen	- Schulung der Benutzer zur Sensibilisierung von IT Sicherheit durchführen - Technische Richtlinien für Kennwörter und Sperrung einrichten
Ungeeigneter Umgang mit Authentisierungsmechanismen	- Separater Benutzeraccounts pro Person - Sensibilisierung betreffend Aufschreiben von Kennwörtern
Social Engineering	- Sensibilisierung der Mitarbeiter - Ausweiskontrolle unbekannter Personen

1.2 Datensicherungskonzept und Archivierung

In diesem Bereich werden Auswirkungen der Datensicherung und Archivierung thematisiert. Es werden zuerst mögliche Gefährdungen mit der IST Situation abgeglichen und geeignete Massnahmen abgeleitet.

1.2.1 Gefährdungen

Verlust von Unternehmensdaten Datenverlust ist in Unternehmungen allgegenwärtig. Es gibt viele verschiedene Möglichkeiten, Daten zu verlieren: Benutzer löschen aus Versehen Daten, Daten werden fälschlicherweise überschrieben, technische Ausfälle von Festplatten, Diebstahl etc. Die Folgen von Datenverlust können unterschiedlich gravierend sein. Beispielsweise könnte Arbeitszeit oder wichtige Informationen verloren gehen. Die Auswirkungen reichen von ärgerlichen Nacharbeiten bis zu Reputationsverlust oder gar juristischen Folgen.

Verlust von Systemkonfigurationen Nebst Unternehmensdaten können auch wichtige Systemkonfigurationen verloren gehen. Als Hauptursache kommen hier Defekte in Frage. Fällt beispielsweise ein Serversystem aus, so sind nicht nur die darin enthaltenen Unternehmensdaten wichtig, sondern auch die Konfiguration des Systems selbst. Die Folgen können ebenfalls gravierend sein, beispielsweise kann mehrere Tage nicht gearbeitet werden, da im Falle eines Defekets das System neu aufgesetzt werden müsste.

Datensicherungen unbrauchbar Datensicherungen werden häufig ordnungsgemäss durchgeführt, jedoch wird deren Wiederherstellung nicht getestet. Es besteht die Möglichkeit, dass Daten nicht vollständig sind oder überhaupt nicht lesbar.

1.2.2 IST Situation

Todo: Dani ausfüllen

1.2.3 Massnahmen

Gefährdung	**Massnahme**
Verlust von Unternehmensdaten	- Regelmässige Backups der Daten (Häufigkeit gemäss Bedarf) - Langzeitarchiv der Unternehmensdaten - Richtlinie zum Speichern von Unternehmensdaten (auf gesicherten Orten)
Verlust von Systemkonfigurationen	- Regelmässige Sicherungen von wichtigen Konfigurationsdateien an sicheren Ort - Systembackups von Servern und wichtigen Clients
Datensicherungen unbrauchbar	- Periodisch Restore Tests durchführen

1.3 Datenschutz

In diesem Bereich wird der Datenschutz näher beleuchtet. Da in der Swiss Medical Clinic auch besonders schützenswerte Personendaten verarbeitet werden, ist die Datensicherheit enorm wichtig, um den gesetzlich vorgeschriebenen Datenschutz gewährleisten zu können.

1.3.1 Gefährdungen

Das DSG (Datenschutzgesetz) schreibt gemäss Artikel 7 vor „Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.“. Daraus ergeben sich bei Nichteinhaltung juristische Konsequenzen. In einer Praxis existieren diverse sensitive Personendaten, seien es die besonders schützenswerten Patientendaten, aber auch Personaldaten etc. Existieren auch Daten von EU-Bürgern, so muss die 2018 in Kraft getretene DSGVO (Datenschutz Grundverordnung) ebenfalls umgesetzt werden.

1.3.2 IST Situation

Todo: Patienten aus der EU?
Todo: Auflistung, wo Patientendaten ausserhalb von Simed sich befinden (externe Festplatten, Notebooks/PCs, Ordner im Filesystem, etc.). Wo befinden sich Personaldaten?

1.3.3 Massnahmen

- Verständnis, was Datenschutz bedeutet und welche gesetzlichen Grundlagen einzuhalten sind.
- Wissen, wo sich schützenswerte Daten befinden.
- Schulung der BenutzerInnen betreffend Umgang mit schützenswerten Daten - Durchsetzen von Massnahmen, welche der IT Sicherheit dienen

1.4 Hard- und Softwaremanagement

Um IT Sicherheit im Unternehmen zu gewährleisten, darf man nicht eine Hard- oder Softwarekomponente isoliert betrachten. Vielmehr benötigt man ein umfassendes Bild des gesamten Systems, da heutzutage die Kompoenten miteinander vernetzt sind und zusammenspielen. Ein IT System durchläuft unterschiedliche Phasen in seinem Lebenszyklus. In jeder dieser Phasen (Planung, Beschaffung, Einführung, Betrieb, Abbau) muss zwingend die IT Sicherheit fester Bestandteil sein.

1.4.1 Gefährdungen

Höhere Gewalt Höhere Gewalten beschreiben Gefahren, auf deren Eintritt man keinen Einfluss hat. Dies wären unter anderem Elementarschäden wie Feuer, Wasser oder Erdbeben, aber auch Ausfälle von Hardware oder Fehler in Software. Ebenfalls sind an einem IT System externe Dienstleister und Hoster beteiligt. Probleme sind nicht auszuschliessen, seien es technische Schwierigkeiten und Ausfälle oder Konkurs etc. Als Unternehmen hat man auf die Eintrittswahrscheinlichkeit keinerlei Einfluss, sehr wohl aber auf das Schadensausmass bei tatsächlichem Eintritt.

Organisatorische Mängel Organisatorische Mängel betreffen die gesamte IT Organisation. Das Management muss sicherheitsrelevanten IT Prozessen die notwendige Aufmerksamkeit schenken. Es müssen wichtige Weisungen über die Benutzung des IT Systems erstellt und auf deren Einhaltung bestanden werden. Es muss dafür gesorgt werden, dass die technischen Anlagen vor unbefugtem Zutritt geschützt werden und im Allgemeinen Berechtigungen für sensitive Einsichten und Veränderungen im System nur an vertrauenswürdige Personen resp. Organisationen erteilt werden. Finanzielle Mittel für IT Sicherheit resp. notwendige und sinnvolle Massnahmen müssen bereitgestellt werden.

Menschliche Fehlhandlungen Menschliches Fehlverhalten kann nie ausgeschlossen werden. Es wird nie technische Hilfsmittel geben, welche alle möglichen Fehler verhindern können. Beispiele wären das Nich-abschliessen von Räumen, versenden sensitiver E-Mails an falsche Personen, aufschreiben oder weitergeben des Passworts, nicht-sperren des PCs, etc.

Technische Mängel Technische Mängel können jedes einzelne System betreffen. Da heutzutage viele oder alle Komponenten miteinander vernetzt sind, kann ein technischer Mangel eines Systems schnell das gesamte System betreffen. Wenn beispielsweise ein zu schwaches Passwort an einem Ort verwendet wird, kann unter Umständen mit demselben Kennwort an einer anderen Komponente ebenfalls etwas geändert werden. Im Cloud Zeitalter kann bei technischen Schwierigkeiten bei der Internetanbindung nicht nur nicht gesurft werden, sondern auch für Geschäftsprozesse elementare Software nicht gebraucht werden.

1.4.2 Massnahmen

Phase	**Massnahme**
Planung/Beschaffung	- Bei Changes immer gesamtheitliche Sicht der IT im Blick haben - Bei Beschaffungen Security im Blick haben, nicht nur den Preis - Möglichst wenige Partner für IT Beschaffungen - Benötigte Verfügbarkeiten prüfen
Einführung und Betrieb	- Regelmässige Wartungen/Audits mit Checklisten - Schulungen (neuer) Mitarbeiter - Notfallszenarien planen, durchführen und dokumentieren
Abbau	- Bei Hardware Daten sicher zerstören (Festplatten, USB Disks, etc.) - Nicht mehr benötigte Benutzer deaktivieren/löschen - Nachkontrollen durchführen

1.5 Patch- und Änderungsmanagement

Informatiksysteme sind im Laufe ihres Lebenszyklus Änderungen ausgesetzt. Beispielsweise könnten veränderte Anforderungen oder gestiegene Nutzerzahlen Anpassungen notwendig machen. Da wir heute fast ausschliesslich verteilte Systeme mit Internetzugang haben, müssen Betriebssysteme und Software Sicherheitsupdates erhalten, um auf neue Bedrohungen zu reagieren. Dies betrifft nicht nur Notebooks, PCs und Server, sondern auch Aktivkomponenten wie Wireless Access Points und Firewalls. Bei Änderungen, resp. Patches entstehen Risiken sowohl beim Patchen, als auch beim nicht-Patchen.

1.5.1 Gefährdungen

Fehlerhafte Testverfahren Problematisch an Software und Betriebssystemen ist die Tatsache, dass die Entwicklerfirma nicht selbst die Änderungen vornimmt. Als Systemadministrator muss man sich darauf verlassen können, dass freigegebene Software oder Patches funktionieren. Da keine Entwicklungsfirma alle möglichen Konstellationen der IT-Systeme ihrer Kunden kennen können, kann- und wird man sich nie mit Sicherheit darauf verlassen können, dass durch Patches und Updates Probleme auftreten werden. Funktionschecks nach Änderungen am System sollten deshalb eingeführt und laufend angepasst werden, um bestmöglich Funktionalität und Sicherheit am System gewährleisten zu können.

Mangelhafte Kommunikation An einem IT-System sind immer mehrere Personen, teils aus unterschiedlichen Firmen, beteiligt. Da Änderungen an einem System auch immer die Umsysteme beeinträchtigen könnten, ist es notwendig, dass alle Änderungen an einer zentralen Stelle gemeldet und koordiniert werden.

Fehlende Wiederherstellungsmöglichkeiten Bei sämtlichen Changes und Patches muss immer in Betracht gezogen werden, dass etwas nicht wie geplant funktioniert. Bei fehlenden Wiederherstellungsmöglichkeiten drohen Datenverlust oder erhebliche Aufwände/Kosten, um das System wieder in den gewünschten Zustand zu bringen. Dies betrifft Daten, aber auch Konfigurationen von Aktivkomponenten und Betriebssystemen/Servern.

1.5.2 IST Situation

Fehlerhafte Testverfahren Es existieren keine standardisierten Testverfahren nach Updates und Änderungen. Einzig werden periodisch (1/2-jährlich) Maintenance Checks durchgeführt, was aber nicht sofort auftretende Probleme nach Änderungen verhindert.

Mangelhafte Kommunikation Sämtliche Änderungen am System werden der Teleinformatik gemeldet und dort, wenn notwenig, koordiniert.

Fehlende Wiederherstellungsmöglichkeiten Todo: Dani (Backupkonzept etc)

1.5.3 Massnahmen

Gefährdung	**Massnahme**
Fehlerhafte Testverfahren	- Standardisierte Funktionschecks entwickeln - Periodisch Funktionschecks anpassen/verbessern
Mangelhafte Kommunikation	- Dienstweg für Anpassungen definieren - Definierten Dienstweg allen Beteiligten kommunizieren
Fehlende Wiederherstellungsmöglichkeiten	- todo: dani ausfüllen

1.6 Identitäts- und Berechtigungsmanagement

Das Thema Idenitäts- und Berechtigungsmanagement beinhaltet die Verwaltung der Personen, IT-Komponenten und Benutzer und die entsprechende Authentisierung auf die Informationen. Dabei ist vorgängig sicherzustellen, dass die Benutzer nur auf IT-Ressourcen und Informationen zugreifen dürfen, die sie für ihre Arbeit benötigen. Idenitäts- und Berechtigungsmanagement wird aus dem organisatorischen sowie technischen Verfahren zusammengesetzt. Wichtig ist, dass die Berechtigungen möglichst gering, eingeschränkt und aufgabenbezogen gesetzt werden. Schlussendlich braucht es dafür eine dokumentierte Vorgehensweise der Zuweisung, Veränderung und Entzug von Berechtigungen auf den jeweiligen Zutritt, Zugriff und Zugang zu Informationen um dies kontrolliert zu steuern. Die Sicherung der Räumlichkeiten und mittlerweilen insbesonders der IT-System und des darin befindenden geistlichen Eigentums wird damit gewährleistet.

1.6.1 Gefährdungen

Fehlende oder unzureichnende Regelungen Unklare Zuständigkeiten, falsche Verteilungen von Kontrollaufgaben oder auch unverständliche und zusammenhangslose Regelungen können zu missverständnisen führen. Folgeproblem ist ein störungsbehafteter Betrieb. Dies hat einen wesentlichen Einfluss auf die Informationssicherheit.

Unzureichende Kontrolle der Sicherheitsmassnahmen Bereits eingeführte Sicherheitsmassnahmen müssen konsequent und regelmässig kontrolliert werden. Mängel können dabei meist ohne grösseren Schaden behoben werden. Falls Verstösse erst bei einem Schadenfall erkannt werden, kann oft nicht mehr angemessen auf die Situation reagiert werden.

Ungeeigneter Umgang mit Passwörtern oder anderen Authentifikationsmechanismen Für die Authentifizierung müssen die Benutzer entsprechend geschult werden. Es nützt nichts wenn diverse technische Möglichkeiten vorhanden sind, diese aber falsch benutzt werden.

1.6.2 IST Situation

Fehlende oder unzureichnende Regelungen Berechtigung auf IT-System werden bis anhin von der Teleinformatik Services AG vergeben und dokumentiert. Schriftliche organisatorische Regelungen fehlen komplett.

Unzureichende Kontrolle der Sicherheitsmassnahmen Es wurden keine Kontrollen getätigt. Wenn etwas geändert werden musst, dann anhand einer unbefriedigenden Situation sowie Veränderungen und Anpassungen innerhalb von Swiss Medical Clinic.

Ungeeigneter Umgang mit Passwörtern oder anderen Authentifikationsmechanismen Konkrete Schulungen, Hinweise sowie Social Engineering wurden nicht durchgeführt. Daher besteht ein unterschiedlicher Wissenstands sowie Handhabungen zu den bestehnden Authentifikationsmechanismen.

1.6.3 Massnahmen

Gefährdung	Massnahme
Fehlende oder unzureichnende Regelungen	- Kontrollaufgaben und Zuständigkeiten definieren - Klare Verteilung der Regelungen
Unzureichende Kontrolle der Sicherheitsmassnahmen	- Sicherheitsmassnahmen konsequent überprüfen
Ungeeigneter Umgang mit Passwörtern oder anderen Authentifikationsmechanismen	- Benutzerschulung zur korrekten Handhabung der Authentifikationsmechanismen

1.7 Infrastruktur

1.7.1 Allgemeines Gebäude

In diesem Bereich wird beschrieben wie die stationären Arbeitsplätze, die verarbeitenden Informationen sowie die aufgestellten Informationstechniken durch das Gebäude geschützt wird. Die Infrastruktureinrichtung ist ein wichtiger Teil damit die Geschäftsprozesse sowie der IT-Betrieb korrekt durchgeführt werden kann. Zubeachten gibt es, dass das Gebäude von einer oder mehreren Organisationseinheiten wie auch Organisationsfremden (Kunden, Lieferanten, etc.) genutzt werden. Hierzu können durchaus unterschiedliche Sicherheitsansprüche geltend gemacht werden. Es ist von Vorteil ein Nutzungskonzept für das Gebäude mit Ausstattung und Gestaltung zu erstellen, die zueinander passen. Dabei erhalten Unberechtigte keinen Zutritt, wo die Sicherheit der tätigen Menschen beeinträchtigt wird. Des weiteren soll sichergestellt werden, dass die stationäre Techniken sicher und effizient betrieben werden.

1.7.2 Gefährdungen

Unbefugter Zutritt zu schutzbedürftigen Räumen Alle Räume die Archive, Datenträge, Akten und Informationen sowie IT-Komponenten aufbewahren werden als schutzbedürftige Räume bezeichnet. Diese können durch vorsätzliche Manipulationen und Vandalismus aber auch durch mangels Fachkenntinissen beschädigt werden. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann durch die Untersuchungen der Betriebsablauf gestört werden. Ein nicht zu vergessender Aspekt ist dabei der Home Office Arbeitsplatz. Dieser wird meistens weniger stark geschützt als der Büroarbeitsplatz und ist dadurch grösseren Gefahren ausgesetzt.

Verstoss gegen gesetzliche Regelungen und vertragliche Vereinbarungen Unzureichende Absicherung der Informationen, Geschäftsprozesse und IT-Systeme kann dazuführen, dass Verstösse gegen Rechtsvorschriften und Verträge mit Geschäftspartnern führen kann. Ungenügende Kenntnisse zu nationale wie auch internationalen Gesetztsvorgaben, u.a. Datenschutz, Informationspflicht, Insolvenzrecht, Haftung und Informationszugriff für Dritte erhöhen zusätzlich das Risiko und rechtliche Konsequenzen drohen.

Ausfall der Stromversorgung Durch Unterbrüche der allgemeinen Stromversorgung können erhebliche Schäden entstehen. Nicht nur dass die IT-Systeme nicht mehr funktionieren sondern auch dass es zu kompletten Ausfällen von Geräten oder inkonsistenzen der Daten führen kann. Dies hat beachtliche

Konsquenzen für die Firma.

Diebstahl & Vandalismus Bei Diebstahl und Vandalismus können hohe Kosten für die Wiederbeschaffung des Materials, die Wiederherstellung des vorgängigen Zustandes führen. Ausserdem können Verluste aufgrund mangelnder Verfügbarkeit und Schädigung der Vertraulichkeit resultieren. Es muss ins Auge gefasst werden, dass diese Aktionen sowohl von internen als auch fremden Personen getätigt werden können, seis durch unabsichtliches oder durch mutmassliches Verhalten. Nicht zu vergessen sind bei diesem Thema die mobilen Endgeräte (Smartphone, Tablet, Notebook) aber auch externen Speichermeiden (USB, Festplatte, etc.). Unachtsames Verhalten kann zu schwerwiegenden Verlusten führen oder Informationen gelangen direkt in die Hände von unbefugten Personen.

1.7.3 IST Situation

Unbefugter Zutritt zu schutzbedürftigen Räumen Eintrittskontrolle im ersten Stock durch Empfangstisch geregelt. Weiter gelangen Personen ohne Schlüssel in schutzbedürftigte Räume. Der Schrank mit den IT-Komponenten lässt sich nicht schliessen, somit kann direkt auf Server und Netzwerkkomponenten zugegriffen werden. In der oberen Etage besteht freier Zuritt. Schutzbedürftige Räume sind weitgehend für jedermann zugänglich. Die wesentlichen IT-Komponenten befinden sich hier im Putzschrank und könnten entsprechend manipuliert werden. Die jetzige Situation zeigt ein enormes Risikopotenzial auf.

Verstoss gegen gesetzliche Regelungen und vertragliche Vereinbarungen Korrekte Absicherung von Rechtsvorschriften und Verträgen sind teilweise bekannt und werden umgesetzt. Konkreter Umgang mit Daten sowie Austausch mit Dritten sind nicht optimal abgesichert.

Ausfall der Stromversorgung Todo: USV vorhanden?

Diebstahl & Vandalismus Durch Mangels Zurittskontrollen und Sicherheitsmassnahmen können Diebstahl sowie Vandalismus von internen wie auch fremden Personen getätigt werden. Für die Wiederbeschaffung der Geräte/des Materials und Wiederherstellung des aktuellen Zustands entstehen erheblich Kosten. Die Vertraulichkeit gegenüber den Patienten, Mitarbeitern und Geschäfspartnern können sogar komplett verloren gehen, was zu rechtlichen Konsequenzen führen kann.

1.7.4 Massnahmen

Gefährdung	**Massnahme**
Unbefugter Zutritt zu schutzbedürftigen Räumen	- Zutrittskontrolle und technische Sicherheitsmassnahmen
Verstoss gegen gesetzliche Regelungen und vertragliche Vereinbarungen	- Abklärung relevanter Informationen und deren Handhabung
Ausfall der Stromversorgung	- Notstrom installieren zur Wahrung der Konsistenz der Daten
Diebstahl & Vandalismus	- Mechanismen einrichten und nur definierten Personen Zutritt und Zugriff gewähren

1.8 Büroraum / Lokaler Arbeitsplatz

Der Arbeitsplatz ist ein Bereich in dem ein oder mehrere Mitarbeiter sich aufhalten und verschieden Tätigkeiten nachgehen die teilweise oder ganze IT-Unterstützung benötigen. Ein lokaler Arbeitsplatz befindet sich innerhalb der Institution, daher können grundlegende infrastrukturelle Sicherheitsvorkehrungen wie Zugangskontrolle oder Brandschutz eingesetzt werden.

1.8.1 Gefährdungen

Unbefugter Zutritt zu schutzbedürftigen Räumen

Manipulation oder Zerstörung von Geräten oder Zubehör

Manipulation an Informationen oder Software

1.8.2 IST Situation

Unbefugter Zutritt zu schutzbedürftigen Räumen

Manipulation oder Zerstörung von Geräten oder Zubehör

Manipulation an Informationen oder Software

1.8.3 Massnahmen

1.9 Serverraum

Im Serverraum werden die Server, TK-Anlage und serverspezifische Unterlagen eingeschlossen. Darin werden nur kurzfristige oder sporadische Arbeite erledigt wie z.B. Maintenance oder Änderungen am System. Trotzdem gilt zu beachten, dass der Schaden deutlich höher ist als in einem Bürorraum, da er den Grossteil der IT Infrastruktur beinhaltet.

1.9.1 Gefährdungen

1.9.2 IST Situation

1.9.3 Massnahmen

1.10 Datenträgerarchiv

Die zentrale Datenträgerarchive und Datensicherungsarchvie dienen zur Lagerung der Datenträger jeder Art. Es empfiehlt sich Datensicherungsschränke zu verwenden um den Brandschutz, den Schutz vor

unbefugtem Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

1.10.1 Gefährdungen

1.10.2 IST Situation

1.10.3 Massnahmen

1.11 Häuslicher Arbeitsplatz

1.11.1 Gefährdungen

1.11.2 IST Situation

1.11.3 Massnahmen

1.12 Mobiler Arbeitsplatz

1.12.1 Gefährdungen

1.12.2 IST Situation

1.12.3 Massnahmen

Systeme

2. Netze

2.1 LAN

Ein Local Area Network (LAN) stellt die übliche Vernetzung von Clients, Servern und anderen IT Systemen innerhalb eines Gebäudes dar. Meistens werden die Gerätschaften über Kupfer- oder Glasfaserkabel miteinander verbunden. Ohne besondere Sicherheitsvorkehrungen sind innerhalb eines LANs sämtliche Gerätschaften untereinander netzwerkmässig sichtbar. Die zugrundeliegende Technologie Ethernet funktioniert broadcast basiert. Broadcasts dienen, damit sich Gerätschaften automatisiert untereinander finden. Dies kann nützlich, aber sicherheitstechnisch bedenklich sein. Die Architektur, respektive die LAN Topologie kann einen erheblichen Einfluss auf die Sicherheit haben.

2.1.1 Gefährdungen

Unautorisierter Netzzugriff Sobald eine Person physischen Zugang zu einem Netzwerkkabel oder einem Netzwerkswitch hat sind ohne weitere Vorkehrungen Zugriffe auf Gerätschaften im LAN möglich. Denkbare Beispiele wären Netzwerkkabel in einem Sitzungs- oder Warteraum oder einen unbesetzten Empfang. Nicht-abgeschlossene und gut zugängliche Netzwerkswitches trifft man ebenfalls sehr häufig an. Sobald man sich im internen Netzsegment befindet sind weitere Angriffsvektoren vorhanden. Es ist zum Beispiel sehr viel leichter ein Client Betriebssystem zu härten, dass es vor Zugriffen im Internet besser geschützt ist als im internen LAN.

Manipulation an Aktivkomponenten Durch unberechtigen Administrationszugriff auf Aktivkomponenten könnte die Kommunikation im Netzwerk mitgeschnitten oder manipuliert werden. Mit administrativem Zugriff auf den LAN Switch könnte relativ einfach Voice over IP Verkehr aufgezeichnet werden. Häufig findet man unsichere Default-Konfigurationen. Dadurch ist administrativer Zugriff sehr leicht da das Standardpasswort sehr leicht nachgeschlagen werden kann.

Ausfall des Netzwerks Das Netzwerk ist ein kritischer Dienst. Fällt das Netzwerk aus, kann in aller Regel nicht mehr, oder nur mit riesigen Einschränkungen, gearbeitet werden. Bei der Betrachtung von möglichen Ausfällen erfordert sowohl eine Einschätzung der technischen Konsequenzen, als auch den Business Impact.

Je nach Topologie des Netzwerks sind nicht alle Kabel und Komponenten im gleichen Sinne kritisch. Normalerweise sollte ein LAN in einer Baumstruktur aufgebaut sein. Komponenten wie der zentrale Switch und Uplinks zwischen Switches sind kritischer als einzelne Gerätschaften. Mittels Redundanzen können Ausfallwahrscheinlichkeiten miteinander multipliziert und somit die Verfügbarkeit drastisch erhöht werden. Verfügbarkeiten werden immer prozentual angegeben. Erhält man von einem Netzwerkswitch beispielsweise Eine Verfügbarkeit von 99.8% ($P(A_1) = 0.998$), so würde im 24 Stunden Betrieb der Switch jährlich 17.52 Stunden ausfallen. Wenn man nun ein zweites Gerät aus Redundanzzwecken einsetzen würde, so hätte man eine Verfügbarkeit von $P(A_1 \cup A_2) = 1 - \{(1 - P(A_1)) \cdot (1 - P(A_2))\} = 0.999996$. Dies würde eine jährliche Ausfallszeit von etwa 0.035 Stunden, also etwas über 2 Minuten bedeuten.

Um eine Redundanz zu bilden wird ein weiteres (Hardware-) Gerät beschafft und mit geeigneten Technologien eine automatische Funktionsübernahme bei Ausfall konfiguriert. Redundanzen können jedoch

auch Komplexität und erhebliche Kosten bedeuten.

Mögliche Ausfallszenarien wären z.B.:

- Geräteausfall (Defekt, Stromausfall)
- Kabelfehler/Defekt
- Netzüberlast
- Denial of Service
- Loop
- Fehlkonfigurationen

Fehlende Segmentierung Grundsätzlich könnte man das gesamte LAN im selben Netzwerksegment betreiben. Ein Netzwerksegment ist eine sogenannte (Layer 2) Broadcast Domäne. Innerhalb dieser Broadcastdomäne können sämtliche Gerätschaften frei miteinander kommunizieren. In grösseren Netzwerken ist es notwendig, dass man einzelne Netzwerkbereiche in unterschiedliche Broadcast Domänen segmentiert. Dies dient unter anderem auch der Vorbeugung von Überlast im LAN (es kann nicht mehr einfach jeder mit jedem kommunizieren), aber es kann auch Denial of Service Attacken wie Duplicate IP Address oder ARP Poisoning vermeiden.

2.1.2 IST Situation

Das LAN der Swiss Medical Clinic ist flach organisiert und nicht segmentiert (Stockwerke oder Client/Server). Sämtliche Aktivkomponenten, Laborgeräte, Drucker, Server und Clients sind in der gleichen Broadcastdomäne. Dies ist nicht untypisch wenn man die Grösse der Organisation betrachtet.

Unauthorisierter Netzzugriff Der LAN Zugriff mittels Netzwerkkabel wird nicht mittels 802.1x (Authentifizierung in Netzen) geschützt. Erhält eine nicht autorisierte Person Zugriff auf ein Netzwerkkabel oder den Netzwerkswitch, ist ein Netzzugriff ohne Spezialkenntnisse leicht möglich. Der Netzwerkswitch im oberen Stockwerk ist sehr leicht zugänglich. Mit einem Netzwerkkabel kann jedes beliebige Endgerät angeschlossen werden. Die Büroräume sind manchmal nicht abgeschlossen. Netzwerkkabel der Drucker könnten ebenfalls leicht verwendet werden für den Netzzugriff.

Manipulation an Aktivkomponenten Alle Aktivkomponenten sind von derselben Organisation konfiguriert und in Betrieb genommen worden (Teleinformatik). Es existieren keine Default Kennwörter. Trotzdem sollten an regelmässigen Wartungen wichtige Sicherheitschecks und Updates vorgenommen werden.

Ausfall des Netzwerks Ausfälle des Netzwerks würden bedeuten, dass Filezugriffe, SiMed, Internetzugriffe allgemein etc. nicht mehr funktionieren würden. Im Falle eines Defekts (Ausfall eines Geräts wie z.B. Switch) könnten voraussichtlich in 1-2 Tagen die Services wiederhergestellt werden. Als besonders kritisch können die Netzwerkswitches und die Firewall angesehen werden. Fällt eines dieser Geräte aus, bedeutet dies einen erheblichen Business Impact. Kabelfehler sind eher unwahrscheinlich und könnten im Falle schnell und leicht ausgetauscht werden.

Die verwendeten Aktivkomponenten und die Netzwerkarchitektur genügen den heutigen Anforderungen bezüglich Performance, eine akute Gefahr von Überlast besteht zur Zeit nicht. Die Gerätschaften sind alle in einem betriebsbereiten Zustand bezüglich Alter und Wartung.

Fehlende Segmentierung Das Netzwerk ist derzeit nicht segmentiert. Sämtliche Geräte im LAN sind sichtbar. Dadurch sind oben erwähnte Angriffsvektoren vorhanden. Mit entsprechenden Kenntnissen und Schadprogrammen könnten bekannte Attacken im LAN ausgeführt werden (z.B. Denial of Service, Ausnutzung von Betriebssystemschwächen, etc.).

2.1.3 Massnahmen

Gefährdung	**Massnahme**
Unautorisierter Netzzugriff	- Serverraum grundsätzlich abschliessen. Server in Rack einschliessen. Putzmaterial in einem anderen Raum verstauen.
Manipulation von Aktivkomponenten	- Vorhandene Berechtigungsstruktur überprüfen und gegebenenfalls anpassen. Wiederkehrende Kontrolle zur Sicherheit der Daten und Dienste einführen
Ausfall des Netzwerks	- Regelmässig Updates einspielen. Upgrade durchführen sobald Kompatibilität gewährleistet ist. Software durch Hersteller warten lassen.
Fehlende Segmentierung	- Regelmässig Updates einspielen. Upgrade durchführen sobald Kompatibilität gewährleistet ist. Software durch Hersteller warten lassen.

2.2 WLAN

2.2.1 Gefährdungen

2.2.2 IST Situation

2.2.3 Massnahmen

2.3 Internet

2.3.1 Gefährdungen

2.3.2 IST Situation

2.3.3 Massnahmen

2.3.4 VPN

2.3.5 Gefährdungen

2.3.6 IST Situation

2.3.7 Massnahmen

2.4 Netz- und Systemmanagement

2.4.1 Gefährdungen

2.4.2 IST Situation

2.4.3 Massnahmen

3. Anwendungen

3.1 SiMed

3.2 E-Mail

3.3 Fileablage

3.4 Internetbrowser

3.5 Laborsoftware

4. Risikoanalyse

4.1 Risiken

4.2 Risikobewertung

4.3 Risikotabelle

5. Abbildungsverzeichnis