# Cybersecurity

> ***Kurzfazit***
> - *Es gibt keinen 100%igen technischen Schutz. Es kann jederzeit jeden treffen.*
> - *Betrachten Sie die latenten Herausforderungen der IT-Sicherheit wie die Hygiene im Steri. Ohne geeignete Gegenmaßnahmen geht es nicht.*
> - *Die Anwender müssen immer wieder geschult und unterwiesen werden. Es muss sich ein Sicherheitsbewusstsein entwickeln. Dieser Sicherheitsfaktor ist sehr wichtig.*
> - *Die Sicherheitsmaßnahmen bedürfen hohe Aufwände an personellen und finanziellen Ressourcen. Es ist zu empfehlen jedes Jahr für IT-Security ein festes Budget einzuplanen, um schnell auf Anforderungen reagieren zu können. Anhaltspunkte liefern die Kosten für einen mehrtägigen Ausfall der IT.*
> - *Jedes Klinikum sollte sich im Rahmen des eigenen Risikomanagements auf den Ernstfall vorbereiten und entsprechende Notfallpläne ausarbeiten.*

Die Sicherheitsvorfälle der letzten Wochen haben deutlich gezeigt, dass die latente Bedrohungslage durch Angriffe aus dem Internet sehr real ist. Die Bedrohungen sind nicht temporär sondern waren und werden fortlaufend die Sicherheit der Kliniken bedrohen.
Durch die aktuellen Sicherheitsvorfälle wird ein gewisser Hype bei Herstellern betrieben und die Kliniken werden mit Angeboten überschüttet. Sicherheit ist jedoch nicht durch den Kauf möglichst vieler Einzelprodukte zu erreichen. Die Auswahl von Systemen zur Verbesserung der Sicherheit sollte mit Bedacht und in Abstimmung mit der Sicherheitsstrategie erfolgen. Somit sollte vor dem Ausbau einer genauen Analyse der vorhandenen Maßnahmen erfolgen.
Vergleichbar mit der Wichtigkeit von guten Hygienemaßnahmen im Umfeld der Zentralsterilisation ist auch die Sicherheitshygiene im IT-Netzwerk zu sehen. IT-Sicherheit ist ein strategisches Thema und bedarf der entsprechenden Berücksichtigung bei der Ressourcen sowie Bugdetplanung und der Integration in die Unternehmensstrategie.

Um die heutigen Bedrohungen abzuwehren reichen Einzelmaßnahmen nicht mehr aus. Die Umsetzung muss eine Bündelung von vielen Sicherheitssystemen und Maßnahmen sein, da sich die Bedrohungslage und Angriffsszenarien ständig ändern. Einzelmaßnahmen wie z.B. das Sperren von einzelnen Dateitypen kann die Bedrohung von Morgen schon umgehen. Damit Maßnahmen sich sinnvoll ergänzen, muss ein IT-Sicherheitskonzept erstellt werden.
Die Umsetzung von Sicherheitskonzepten erfordert nicht nur systemspezifisches Knowhow, sondern auch einen hohen Sachverstand bezüglich der komplexen Sicherheitszusammenhänge.
Vergleichbar mit dem Zwiebelschalenmodell, wenn man sich im Winter anzieht, um sich vor Viren zu schützen, erfolgt der Schutz in der IT vor Viren/Malware durch Schutzzonenkonzepte. Die äußeren Schutzzonen sollen hierbei verhindern, dass der Virus überhaupt zu den wichtigen Systemen vordingen kann. Mit Vertrauen in die eigene IT und deren Umsetzungskonzepte, sowie der punktuellen Unterstützung durch externe Spezialisten, ist das Ziel eines guten Schutzes vor Malware umsetzbar.

Folgende Grundanforderungen / -regeln sollen als Anhaltspunkt dienen für eine möglichst gute technische Sicherheitsinfrastruktur:

- Alle Sicherheitsmaßnahmen sollten frühestmöglich greifen. Nach dem Zwiebelschalenprinzip ist das interne Netz durch Verteidigungswälle / Schutzzonen zu schützen. Ist der Virus erst im Rechenzentrum ist es zu spät. D.h. möglichst bevor der Schadcode das interne Netzwerk erreichen kann. Die Architekturen sind dahingehend zu prüfen und anzupassen.
- Sollte ein Angriff einmal erfolgreich sein und Unternehmensdaten von einer Malware verseucht sein, ist die letzte Rettung das Unternehmensdatenbackup. Auf dieses sollte ein besonderes Augenmerk gelegt werden. Ein Backup sollte zudem offline gehalten werden. Der Restoreprozess muss auch bewertet werden. Lange Wiederherstellzeiten führen auch zu längeren Ausfallzeiten. Häufige und schnelle Backups sowie Wiederherstellzeiten erfordern einen hohen technischen Aufwand und Kosten. Eine Abwägung von Risiko und Nutzen sollte bewusst erfolgen.
- Es sollte die Möglichkeit geben, Inhalte je nach Bedrohungslage möglichst flexibel mit sogenannten Content-Filtern für Web-, Mail- und sonstige Daten zu filtern. Diese sind im Idealfall in der Lage, nur den gefährlichen Inhalt herauszufiltern und die Nutzdaten dem Anwender zuzustellen.
- Installation der verfügbaren Sicherheitsupdates auf Servern und Clients. Wenn dies nicht möglich ist (Medizinprodukte, keine Herstellerfreigabe) sind die Systeme auf andere Weise zu schützen (z.B. Schutzzonen mittels eigener VLANs, Sperren von gefährlichen Diensten wie Internet usw.).

- Virenschutz nach Möglichkeit mindestens zweistufig. Die sogenannten Pattern/Sicherheitsupdate sind mehrfach täglich durchzuführen. Der Virenschutz sollte nicht nur auf Signaturbasis, sondern auch auf heuristischer Ebene und durch Isolierung und Beobachtung (Sandbox) betrieben werden.
- Überwachung auch von verschlüsselter Kommunikation (z.B. verschlüsselten Mails und verschlüsseltem Webtraffic). Sonst kann der Schadcode alle Sicherheitsmaßnahmen umgehen.
- Sensibler Umgang mit Internetdiensten aller Art (Webmailer, Cloudspeicher usw.). Absicherung und Eingrenzung dieser Dienste mit Sicherheitssystemen.

Die Sicherheit kann nicht nur durch technische Maßnahmen erreicht werden. Organisatorische Maßnahmen haben einen genauso hohen Stellenwert. Sicherheit entsteht aus der Lust zur Anwendung. Ein Umdenken bei den Anwendern ist somit unbedingt von Nöten, damit die Anwender keinen Einfallsreichtum zur Umgehung von Sicherheitsmaßnahmen mehr aufbringen.

- Die Awareness und das Sicherheitsbewusstsein der Anwender muss deutlich verbessert werden. Das Verständnis und die Problematiken sind den Nutzern oft nicht klar oder werden als überflüssig abgetan.
- Unterbindung der Nutzungsmöglichkeiten von privaten Geräten im Unternehmensumfeld, da diese nicht zentral überwacht und verwaltet werden können. Dies gilt auch für die Anbindung von IT-Equipment von Partnern (Wartungsrechner usw.).
- Definition klarer Regelungen zur Nutzung von mobilen Unternehmensgeräten (Notebooks, USB-Sticks usw.) im externen Umfeld. Z.B. verpflichtende Virenprüfung vor Anbindung ans Unternehmensnetzwerk usw.
- Wichtig ist es auch keine Hintertüren zuzulassen. D.h. ISDN und DSL-Zugänge für Fernwartung die an allen Sicherheitssystemen vorbei einen Zugriff auf das Netzwerk erlauben. Jeglicher Datenverkehr im Unternehmen muss über die zentrale Sicherheitsinfrastruktur laufen.
- Schatten-IT in Bereichen/Kliniken ist unbedingt zu vermeiden. Insbesondere im Sicherheitsumfeld müssen alle Maßnahmen zentral durch die IT verwaltet und überwacht werden.
- Die Embedded-IT wie z.B. bei Medizinprodukten, wird in den kommenden Jahren ein immer größeres Thema werden. Hier können viele technische Maßnahmen nicht sinnvoll angewendet werden und es müssen Schutzzonenkonzepte etabliert werden. Die hierzu erforderlichen technischen Maßnahmen bedürfen einer strategischen Integration in die Unternehmensausrichtung.
- Ein höheres Maß an Sicherheit erfordert mehr Ressourceneinsatz. Insbesondere mehr Überwachung und Konzeption durch Fachpersonal, welches in den Sicherheitssystemen geschult ist und Zeit für die oft aufwendigen Prüfungen erhält.
- Fortgeschrittene Sicherheitskonzepte bedürfen eine strategische Bewertung und können oft nur langfristig erfolgen, da vorhandene IT-Strukturkonzepte umgestellt werden müssen. Z.B. der Zugriff auf Internetdienste (Web/Email) nur über eigene Strukturen (Terminalserver) zuzulassen, um das Sicherheitsniveau nochmals zu verbessern. Solche Konzepte detaillieren den Ansatz der Sicherheitszonen weiter, da kein PC oder medizinisches Gerät einen direkten Internetzugriff erhält.

Die AKG-IT macht den Vorschlag, dass innerhalb der AKG-IT in diesem Jahr das Thema Notfallkonzept für Cybersecurityangriffe aufgenommen wird. An dieser Stelle will die AKG-IT nochmals auf die Bedeutung der Bestellung eines IT-Sicherheitsbeauftragten hinweisen und auf die Wichtigkeit der Einführung eines Informationssicherheitsmanagements. Beide Themen bedürfen der strategischen Aufnahme in die Unternehmensziele, da die Aufwände hierfür nicht unerheblich und sehr zeitaufwendig sind.
Auf die Wichtigkeit der allgemeinen Notfallkonzepte hat die Arbeitsgruppe schon im Rahmen des IT-Sicherheitsgesetzes 10/2013 und 10/2015 hingewiesen. Die AKG-IT rät den Kliniken dringend die unternehmenskritischen Prozesse ihrer Krankenhäuser und auch die manuellen Ausfallkonzepte der betroffenen Prozesse zu überprüfen. Sie bilden die Überlebensgrundlage für die Anwender, solange die IT oder IT-Services wie Internetdienste nicht zur Verfügung stehen.

IT-Hygiene im Rahmen der IT-Sicherheit ist wie klinische Hygiene zu sehen. Gefährliche Viren und Keime verbreiten sich in der IT oft noch schneller als in der Medizin und gefährden den klinischen Betrieb und die Patienten. In Anbetracht der aufgeführten Herausforderungen im Bereich IT-Security, empfehlen wir dringend dieses Thema als festen Bestandteil in den Jahresprojektplänen vorzusehen. Der Aufwand bezüglich Personal und Kosten entspricht dem normaler Projekte und darf nicht vernachlässigt werden.

Die AKG-IT hat eine Abfrage zu den getroffenen Sicherheitsmaßnahmen in den Häusern durchgeführt.
Es haben 50% der AKG-Häuser an der AdHoc-Abfrage zur Cybersicherheit teilgenommen.
Anbei die wichtigsten Ergebnisse

- Im Allgemeinen kann gesagt werden, dass sehr restriktive und präventive (aufwändige) Sicherheitsansätze nur von wenigen Kliniken durchgeführt werden. Dies liegt vermutlich insbesondere am hohen Personalaufwand zur Umsetzung dieser Techniken. Langfristig werden jedoch gerade diese proaktiven Maßnahmen den besten Schutz gegen sich ständig verändernde Angriffsszenarien bieten.
- Es gibt in vielen Häusern noch Sicherheitslücken, weil gepackte und verschlüsselte Inhalte nur sehr begrenzt mit technischen Systemen überwacht werden können. Auch diese Lücken sollten durch strategische Projekte sukzessive geschlossen werden.
- 5 Kliniken haben einen Schaden durch Viren gemeldet. 4 Kliniken seit 02/2016 und eine Klinik vor 02/2016. Der Schäden hielt sich glücklicherweise immer in Grenzen (wenige PCs eine Abteilung) und lag mit <24h Ausfallzeit im unteren Bereich. Allerdings wurden von allen Kliniken, nach dem Vorfall in Neuss, Ad-Hoc Schutzmaßnahmen umgesetzt. Ansonsten wäre die Ausfallrate sicherlich deutlich höher gewesen. Dies macht die latente Bedrohungslage deutlich.
- Awareness Maßnahmen haben fast alle schon vor 02/2016 ausgeführt. Infomails werden meist anlassbezogen versendet. Allgemeine Newsletter zur Sensibilisierung und Schulungen / Infoveranstaltungen werden von wenigen durchgeführt. Die Stärkung der Sensibilität der Benutzer ist jedoch sehr wichtig, da es keine 100%igen technischen Schutz gibt.
- Das Abwehren der Sicherheitslücken von aktuellen Bedrohungen wie Markos, erfolgte schon in vielen Kliniken. Viele Kliniken haben die Makrosicherheit erhöht, sei es am Client oder durch das Löschen von Makros am Internetzugang.
- Methoden zum Themenfeld Intrusion-Protection und Intrusion-Prevention setzen nur 50% der Kliniken ein. Dies muss jedoch im Kontext der sonstigen Schutzmaßnahmen gesehen werden und bildet für sich alleine kein Qualitätsmerkmal.
- Es gibt nur 2 Kliniken welche die erste Sicherheitsschicht zum Internet (Firewall, Mailsysteme) von einem Provider betreiben lassen. Je nach Personalkapazitäten und Know-How ist es ratsam sich hier Unterstützung zu holen. IT-Sicherheitssysteme nutzen nur dann etwas, wenn man über das entsprechende Fachwissen verfügt und die Logs und Einstellungen ständig kontrolliert.
- Cloud-Angebote (Webmailer, Dateidienste usw.) wurden von vielen schon vor 02‘/2016 gesperrt. Aufgrund des hohen Sicherheitsrisikos haben seit den jüngsten Vorfällen 4 Kliniken Clouddienste gesperrt. Das Handling von erlaubten und nicht erlaubten Internetinhalten erfolgt bei den meisten über Webseitenfilter auf Kategoriebasis. Ohne solche Kategorie-Kataloge ist das Sperren und Erlauben von Webseiten aufgrund der hohen Dynamik nicht sinnvoll möglich.
- Sicherheits- und Betriebssystemupdates für Clientsysteme werden in vielen Häusern wöchentlich oder monatlich durchgeführt. Dies ist im Rahmen der proaktiven Maßnahmen dringend anzuraten. Zumindest die Sicherheitspatche sollten mindestens monatlich erfolgen. Der Aufwand ist nicht zu unterschätzen, da nach jedem Update die Systemfunktionen geprüft werden müssen.
- Ein Problem sind immer noch Altsysteme wie Windows-XP, welche aufgrund von Herstellervorgaben nicht aktualisiert werden können. Die meisten Kliniken sperren Internet und Maildienste für diese Systeme oder stellen sie in isolierte Netzwerke. Dies geschieht um die Betriebs-/Patientensicherheit zu gewährleisten und keine Hintertür für das Gesamtnetzwerk zu öffnen.
- Externe Geräte wie USB-Sticks werden in den wenigsten Kliniken derzeit gesondert überwacht. Auch hier besteht ein nicht unerhebliches Sicherheitsrisiko. Wenn keine Überwachungssysteme vorhanden sind, ist mit hohen Kosten und Ersteinrichtungsaufwänden zu rechnen.
- Ein Gefahrenpotential wird auch durch externe Techniker erzeugt. Diese haben deshalb in vielen Kliniken keine oder nur eingeschränkte Rechte. Externe sind sinnvollerweise bei jeder Wartung Vorort über ein Merkblatt an die Sicherheitsregeln zu erinnern. Die allgemeinen Verpflichtungen sollten als Vertragsanlagen erfolgen, damit zumindest die haftungsrechtlichen Fragen bei Vorfällen geklärt sind.