Empfehlungen zur Sicherheit des Intranets von Krankenhäusern

AG DGI der GMDS, 27. März 2011

0. Zusammenfassung (Management Summary)

0.1 Zielvorstellungen, Anforderungen und Risiken: Hohe Priorität für ein Krankenhaus hat die Sicherheit der Patienten und der Schutz der Patientendaten und anderer Ressourcen, insbesondere vor Gefahren aus dem Internet. Andererseits erfordern dienstliche Belange und die Unterstützung der Krankenversorgung und Forschung einen möglichst ungehinderten Zugang zum Internet aus dem Bereich des Krankenhauses heraus sowie in umgekehrter Richtung den Zugriff auf das Intranet des Krankenhauses, möglichst von überall in der Welt.

Diese beiden Zielvorstellungen (Sicherheit und ungehinderter Zugriff) *stehen in einem Konflikt miteinander, zu dessen Auflösung nicht zu vernachlässigende Anstrengungen und Ressourcen notwendig sind.*

Der Schutz der Patientendaten einschließlich dem Schutz von Medizingeräten[1] muss dabei höchste Priorität genießen

- wegen der gesetzlichen Anforderungen der ärztlichen Sorgfalts- und Schweigepflicht,
- wegen des Schutzes von Leben und Gesundheit der Patienten,
- wegen des Ansehens und der Glaubwürdigkeit des Krankenhauses in der Öffentlichkeit.

Die letztendliche Verantwortung hierfür liegt beim Vorstand. Damit dieser sie adäquat wahrnehmen kann, sind

- angemessene technische Maßnahmen nach Vorgaben der anerkannten guten Praxis,
- organisatorische Regelungen zum Abdecken verbleibender Sicherheitslücken

notwendig. Dazu muss die Sicherheitslage dem Vorstand nachvollziehbar dargestellt werden.

Daher sind für dringende Sicherheitsprobleme im Netz des Krankenhauses praktikable Lösungen zu entwickeln. Das betrifft die Sicherheit der Patientendaten vor Angriffen aus dem Internet, die Sicherheit des internen Netzes und der Server, Medizingeräte und Arbeitsplatzrechner und ergänzend dazu die abgesicherte Möglichkeit zum Zugriff für Mitarbeiter von außen auf interne Daten und das E-Mail-Konto.

0.2 Grundsätzliche Empfehlungen:

1. Ein IT-Sicherheitskonzept für das Krankenhaus ist dringend nötig. Dazu gehört eine vom Vorstand verabschiedete allgemeine Richtlinie (Policy), ein Grobkonzept (z. B. Anpassung dieser Empfehlung an die lokalen Gegebenheiten) sowie ein Feinkonzept, das auch eine Risikoanalyse einschließt.
2. Als wichtigste konkrete Maßnahme wird eine Trennung des Krankenhausnetzes in ein streng geschütztes klinisches Datennetz und ein allgemeines Krankenhausnetz (KH-Netz) mit erleichtertem Internetzugang, das z. B. in Universitätskliniken auch den Bereich „Forschung und Lehre“ umfasst, empfohlen. Von Arbeitsplatzrechnern aus dem allgemeinen KH-Netz sollte ein Zugriff auf das klinische Datennetz über virtuelle

[1] Nach dem 4. MPG-Novellierungsgesetz ist auch ein erheblicher Teil der Software im KIS rechtlich als Medizinprodukt einzuordnen.

Techniken ermöglicht werden[2]. Für Zugriffe von außen ist eine geeignete sichere Portal-Lösung anzustreben.

3. Eine Risikoabschätzung nach dem Kosten-Nutzen-Modell ist für ein Krankenhausnetz nicht sinnvoll durchführbar; statt dessen sind im Sinne der guten Praxis die Empfehlungen des BSI zu befolgen, wie sie in den IT-Grundschutzkatalogen definiert sind[3]. Wegen des hohen Schutzbedarfs von Patientendaten sind zusätzliche Maßnahmen nötig.
4. Die Gewährleistung der IT-Sicherheit im klinischen Datennetz ist als Serviceleistung der zentralen IT-Abteilung anzusehen; Anwender müssen von eigener Sorge um die Sicherheit dieses Netzes und ihrer Patientendaten so weit möglich durch technische Maßnahmen entlastet werden. Im Gegenzug ist eine weitgehende zentrale Administration der Arbeitsplatzrechner anzustreben.
5. Da technische Maßnahmen nicht ausreichen, um alle Sicherheitsprobleme zu lösen, sind ergänzende organisatorische Maßnahmen unerlässlich.

0.3 Empfehlungen für den Vorstand:

1. In Abstimmung mit dem Datenschutzbeauftragten Erlass einer Leitlinie („Policy“) zum Datenschutz und zur IT-Sicherheit, die für Mitarbeiter verpflichtend ist; hier sollten auch Zugriffsregelungen von extern und mögliche Ausnahmeregelungen bei nachgewiesener dienstlicher Notwendigkeit definiert sein.
2. Anforderung regelmäßiger schriftlicher Berichte der zentralen IT-Abteilung über bestehende Risiken und Schwachstellen.
3. Auftrag an die zentrale IT-Abteilung zur Erstellung eines Feinkonzepts zu den vorgesehenen Maßnahmen für Netzstruktur und Sicherheit der IT-Arbeitsplätze sowie zur Kostenplanung, Priorisierung und Umsetzung.
4. Bereitstellung der dafür notwendigen Ressourcen gemäß der von der zentralen IT-Abteilung vorgelegten Kostenplanung.
5. Auftrag an die zentrale IT-Abteilung zur Formulierung von SOPs für die Mitarbeiter zum Umgang mit Patientendaten, Medizingeräten, Internet, E-Mail und mobilen Geräten; hierzu soll auch der Datenschutzbeauftragte konsultiert werden.
6. Grundsätzlich ist zu empfehlen, die Stelle eines IT-Sicherheitsbeauftragten zu etablieren. Dieser sollte direkt dem Vorstand unterstellt und bezüglich Beratungs- und Weisungsbefugnis ähnlich dem Datenschutzbeauftragten eingeordnet sein. Für kleinere Krankenhäuser kann diese Aufgabe auch an vertrauenswürdige externe Dienstleister vergeben werden.

1. Anforderungen

Die besonderen Schutzanforderungen der klinischen Daten und Prozesse und der Medizingeräte geben sehr enge Rahmenbedingungen für den Betrieb des Intranets eines Krankenhauses und seiner Anbindung an das Internet vor. Ärztliche Sorgfalts- und Schweigepflicht sowie Datenschutz definieren für die Patientendaten aus der Krankenversorgung einen hohen[4] Schutzbedarf. Die ins Intranet eingebundenen Medizingeräte erfordern gleichfalls einen ho-

[2] Der entscheidende Aspekt hierbei ist, dass Daten nicht auf den Arbeitsplatzrechner herunter geladen, sondern nur auf dem Bildschirm dargestellt werden. Diese weitgehende Abschottung der Patientendaten ist Voraussetzung dafür, dass der Umgang mit dem Internet für das allgemeine KH-Netz erleichtert werden kann.
[3] Diese werden auch in der Rechtsprechung und bei Datenschutzprüfungen zu Grunde gelegt.
[4] Gemäß § 3 Abs. 9 i.V.m. § 4a Abs. 3, § 4d Abs.5 und § 28 Abs. 6 BDSG muss bei Patientendaten immer von einem hohen Schutzbedarf ausgegangen werden.

hen Schutz[5]; zu den Medizingeräten muss seit dem 4. MPG-Änderungsgesetz auch ein Teil der KIS-Software gezählt werden. Daneben sind aber auch dienstliche Daten wie Benchmarking- und Forschungsdaten, innerbetriebliche Verwaltungsdaten und Finanzdaten als Betriebskapital des Krankenhauses schützenswert.

Andererseits erfordern die Unterstützung der Forschung und die Optimierung der Versorgung einen möglichst ungehinderten Zugang zu den Ressourcen des Internets aus dem Bereich des Krankenhauses heraus sowie in umgekehrter Richtung den Zugriff auf Ressourcen des Krankenhauses von überall in der Welt. Insbesondere in Universitätskliniken haben die Bereiche „Forschung und Lehre“ und „Krankenversorgung“ sehr unterschiedliche Anforderungen an Informationsoffenheit und den gleichzeitig zu gewährleistenden Schutz klinischer Ressourcen.

Ein Bedarf an Fernzugriffen besteht auch im Bereich der Patientenversorgung, etwa durch den ärztlichen Hintergrunddienst, sowie für Zwecke der Fernwartung von Servern und Medizingeräten.

Diese beiden Anforderungen (Sicherheit und ungehinderter Zugriff) stehen in einem Zielkonflikt miteinander, zu dessen Auflösung erhebliche Anstrengungen notwendig sind. Die Sicherheit von Daten, Prozessen und Medizingeräten im Intranet und der freie Informationsaustausch im Internet können nicht gleichermaßen in einem gemeinsamen Netz ohne zusätzliche technische und organisatorische Maßnahmen garantiert werden.

2. Bisherige Empfehlungen

Bisherige Sicherheitsempfehlungen, auch dieser AG, beruhten auf der Annahme, dass das Intranet sicher ist und Gefährdungen im wesentlichen vom Internet ausgehen. Durch die Parallelität der Nutzung des Arbeitsplatzrechners für das Arbeiten im Intranet und im Internet hat sich die Problemlage für die Sicherheit der Daten im Intranet aber in den letzten Jahren zunehmend verschärft.

Die physikalische Trennung von Intranet und Internet mithilfe eines Sicherheitsgateways („Firewall“) und der Einsatz eines Remote-Controlled Browsers Systems (ReCoBS[6]) für den Zugriff auf das Internet – entsprechend dem Konzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – wurden bislang als wesentlicher Beitrag zur Wahrung des notwendigen Sicherheitsniveaus für die im Intranet vorhandenen Ressourcen angesehen.

Die Verfügbarkeit neuer Techniken und deren unkontrollierter Einsatz haben deutliche Auswirkungen auf das Sicherheitsniveau des Intranets und zeigen die Unzulänglichkeit der bisherigen Empfehlungen. Hierzu gehören z. B. UMTS-Sticks, die den Internetzugriff aus dem Intranet des Krankenhauses heraus unter Umgehung des Sicherheitsgateways erlauben, mobile Speicher mit großem Speichervolumen zum Import und Export von Daten, unkontrollierter

[5] vgl. Norm E IEC / DIN EN 80001

[6] Unter einem Remote-Controlled Browsers System (ReCoBS) versteht das BSI den Web-Zugang mit Hilfe von speziell gesicherten Terminalserver-Systemen. Dabei laufen die Browser nicht auf den Arbeitsplatz-PC’s, sondern auf einem Terminalserver außerhalb des LAN und werden von den Arbeitsplätzen aus ferngesteuert. Im Browser auf dem Terminalserver werden alle Webinhalte ausgeführt, so dass bei Einhaltung entsprechender Sicherheitsanforderungen Aktive Inhalte nicht ins LAN gelangen können. Statt dessen werden grafische Informationen an die Arbeitsplätze übermittelt und dargestellt. Damit sind Ausführung und Darstellung Aktiver Inhalte voneinander getrennt. (Quelle: Remote-Controlled Browsers System (ReCoBS) - Grundlagen und Anforderungen, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/cae/servlet/contentblob/478364/publicationFile/30920/recobslanginfo_pdf.pdf)

Einsatz von WLAN, unkontrollierte getunnelte VPN-Verbindungen mit Laufwerkzugriff, die Nutzung von Skype und Instant-Messaging, Teamviewer und ähnlicher Werkzeuge, die den Zugriff von außen über Tunnel durch das Sicherheitsgateway hindurch auf Rechner im Intranet erlauben. Dazu kommt ein stark verändertes und oft wenig sicherheitsbewusstes Nutzerverhalten, uneinheitlich gestaltete Vergabe der Administrationsrechte für die am Intranet angeschlossenen Rechner, der Einsatz privater Rechner im Intranet und insbesondere auch die mobilen Rechner (Laptops), die innerhalb und außerhalb des Intranets des Krankenhauses betrieben werden.

3. Sollkonzept

Aus den genannten Gründen muss ein auf den bisherigen Empfehlungen beruhendes Sicherheits- und Netzkonzept dringend überdacht und geändert werden. Ziel dabei ist es, das nicht verhinderbare Risiko für die Sicherheit der Daten auf ein vertretbares Maß zu reduzieren und gleichzeitig eine größere Freiheit für den Internetzugriff zu ermöglichen.

Zur grundsätzlichen Lösung der Problematik ist das gängige Verfahren[7] die Aufteilung des Intranets in zwei Ebenen mit unterschiedlichen Schutzprofilen – hier „**klinisches Datennetz**“ und „**allgemeines KH-Netz“** genannt[8]. Der Einsatz eines Netzwerkzugangskontrollsystems und die zentrale Administration aller Rechner sind dabei wesentliche Beiträge zur Netzsicherheit; die zentrale Administration sollte aber auch in Erwägung gezogen werden, um personelle Ressourcen wirtschaftlich einzusetzen. Eine weitere Segmentierung der beiden Teilnetze – wie im folgenden vorgeschlagen – ist notwendig und erhöht die Sicherheit in entscheidendem Ausmaß.

Das **klinische Datennetz** ist ein besonders geschützter innerer Netzbereich, in dem die Medizinprodukte und Daten mit besonderem Schutzwert (Patientendaten, Mitarbeiterdaten, Daten klinischer Studien, Wirtschaftsdaten) liegen. Dieses Netz untergliedert sich in einen *Kernbereich* und einen *erweiterten Bereich*. Der Kernbereich ist räumlich eng lokalisiert und durch physische Zugangskontrolle geschützt, umfasst die Serverräume, insbesondere der zentralen IT-Abteilung und möglicherweise anderer zentraler Leistungserbringer, und erfüllt hohe Sicherheitsanforderungen. Zum erweiterten Bereich gehören alle dezentralen Geräte, auf denen Patientendaten liegen bzw. akquiriert werden, z. B. PDMS, POCT, auch reine klinische Arbeitsplatzrechner mit gar keinem oder sehr eingeschränkten Zugang zum Internet. Zur Absicherung des erweiterten Bereiches wird die Umsetzung folgender Maßnahmen (nach sorgfältiger Prüfung und Detailplanung) empfohlen:

- zentrale Administration der Rechner mit Sperren von CD/DVD-Laufwerken und USB-Schnittstellen,
- Einführung von zentralen Lese- und Brennstationen für den Austausch von Daten, dort auch Virenprüfung der eingelesenen Daten,
- ergänzende organisatorische Regelungen.

Im erweiterten Bereich sollten Subnetze

- für evtl. vorhandene Server für klinische Studien mit Patientendaten,
- für nicht im Kernbereich betriebene Medizingeräte,
- für WLAN-Zugänge für klinische Applikationen

[7] vgl. auch DIN EN 60601-1 3rd

[8] Diese Teilnetze entsprechen den Sicherheitsklassen B und A nach DIN EN 60601-1 3rd sowie den Schutzklassen B und A der neuen Norm E IEC / DIN EN 80001 für Medizinprodukte.

geeignet abgegrenzt werden. Separate Netze für Medizingeräte mit höchstem Schutzbedarf nach DIN EN 60601-1 (3rd Ed.) oder DIN EN 80001, Klasse C, gehören auch zum klinischen Datennetz, sind aber bis auf eventuelle Wartungszugänge nicht mit diesem verbunden[9]. Erforderliche Datenexporte aus dem klinischen Datennetz zu bestimmten, explizit definierten und besonders geregelten Zwecken, müssen auf kontrollierte Weise möglich sein.

Im **allgemeinen KH-Netz** stehen die Arbeitsplatzrechner, die einerseits als Zugangsrechner zum klinischen Datennetz und andererseits als allgemeine Arbeitsplatzrechner dienen. Dieser Bereich kann weniger restriktiv gehandhabt werden. Datensicherheit bedeutet aber auch die Sicherstellung der Verfügbarkeit der Zugangsrechner. Daraus resultiert, dass ein zentraler Schutz durch ein Sicherheitsgateway auch für das allgemeine KH-Netz vorhanden sein muss, jedoch kann dieses Sicherheitsgateway weniger restriktiv betrieben werden bzgl. der Filterung aktiver Inhalte. WLAN-Zugänge (z. B. für Patienten, Gäste, in Universitätskliniken auch für Studenten) sollen in abgetrennten Bereichen des allgemeinen KH-Netzes angesiedelt sein, die keine unkontrollierte Verbindung mit den übrigen Bereichen des allgemeinen KH-Netzes, aber eine ungehinderte Nutzung der nötigen Ressourcen im Internet erlauben.

Die physikalische Trennung dieser beiden Netze durch den Einsatz von Sicherheitsgateways und der Einsatz von virtuellen Zugängen (Remote Controlled Applications, virtuellen Desktops und ähnlichen Techniken) analog zum ReCoBS-Ansatz für die Nutzung von Ressourcen des klinischen Datennetzes aus dem allgemeinen KH-Netz heraus erfolgt in analoger Weise wie bei der vom BSI empfohlenen Internetnutzung. Als Systeme dafür denkbar sind neben Microsoft Terminalserver auch Citrix XEN-Server und VMWare-Lösungen, gegebenenfalls in Kombination. Eine für den Nutzer einfache und praktikable Lösung sollte bevorzugt werden.

Der Zugriff von außen kann liberaler gestattet werden, wenn die Möglichkeit eines Durchgriffs (außen → allgemeines KH-Netz → klinisches Datennetz) kontrolliert werden kann. Die Empfehlungen des BSI sollten bei der VPN-Implementierung für das Erreichen des notwendigen Sicherheitsniveaus berücksichtigt werden. Über VPN in das Kliniknetz eingebundene Remote-Rechner (z. B. für den ärztlichen Hintergrunddienst) sollten als Rechner in ein separat abgetrenntes Segment des allgemeinen KH-Netzes eingehängt werden; der Zugriff auf die Daten erfolgt dabei in gleicher Weise wie bei den lokalen Rechnern über Remote Controlled Applications. Für manche Anwendungen (z. B. radiologische Befundung) ist gegebenenfalls aus Performanzgründen eine dedizierte Lösung einzurichten. Die aktuelle Marktentwicklung im Bereich von Zugriffsportalen ist eng zu beobachten; hier sind künftig möglicherweise kostengünstige und sichere Lösungen verfügbar. Unabdingbar für den Einsatz einer solchen Lösung ist, dass beim externen Zugriff Daten aus dem klinischen Datennetz nur auf dem Bildschirm dargestellt, nicht aber auf den externen Rechner heruntergeladen werden. Für Fernwartungsarbeiten, z. B. an Medizingeräten, sollte ein ähnlicher Zugang vorgesehen werden, der kontrolliert freigeschaltet und überwacht werden kann.

Für den Mail-Zugriff wird die Einrichtung eines E-Mail-Kontos empfohlen, auf das auch von außen, evtl. mit Einschränkungen oder nur für gewisse Nutzer, Zugriff möglich ist und das im allgemeinen KH-Netz angesiedelt ist. Als Voraussetzung hierfür sollte der Versand von Patientendaten per E-Mail, auch klinikintern, unterbunden oder untersagt werden. Das wiederum setzt voraus, dass dafür andere geeignete Kommunikationsmöglichkeiten zur Verfügung stehen.

[9] Hierzu gehören z. B. Netze von Intensivstationen. Die Notwendigkeit einer Fernwartung impliziert, dass auch diese Geräte einen Netzzugang benötigen, der aber dann dediziert sein muss.

Die Sicherheit des Intranets des Krankenhauses, sowohl des klinischen Datennetzes als auch des allgemeinen KH-Netzes, ist als Service-Leistung der zentralen IT-Abteilung zu verstehen. Die IT-Nutzer des Krankenhauses sollten soweit wie möglich von eigener Sorge um die Sicherheit ihrer Geräte entlastet werden. Umgekehrt dürfen sie nicht durch unterschiedliches oder mangelndes Sicherheitsverständnis einzelner Kollegen gefährdet werden.

Die Sicherheit des Intranets eines Krankenhauses ist nicht durch technische Maßnahmen allein zu gewährleisten; ergänzend müssen organisatorische Maßnahmen vorgesehen werden. Diese umfassen eine vom Vorstand zu erlassende Policy, Betriebsvereinbarungen und Betriebsanweisungen, SOPs für sicherheitskritische Prozesse sowie ein etabliertes Risikomanagement[10]. Dazu gehört auch die Vereinbarung von Kontrollmaßmaßnahmen sowie dienst- und arbeitsrechtlicher Maßnahmen bei Verstößen.

4. Status dieser Empfehlung

Diese Empfehlung gilt zunächst bis Ende 2014 und soll spätestens dann auf Aktualität überprüft werden.

Obsolet werden mit dieser Empfehlung die Empfehlungen der AG DGI

- zum Internet-Anschluss von Krankenhäusern und Gesundheitsnetzen (überarbeitet Mai 2001),
- zu Modem-Verbindungen im Krankenhaus (Oktober 1998).

Danksagung

Wesentlicher Input zu dieser Empfehlung kam von der AG IT-Sicherheit der Universitätsmedizin Mainz sowie von den IT-Abteilungen und Datenschutzbeauftragten der Universitätskliniken Marburg, Gießen, Würzburg und Frankfurt.

[10] wie in den BSI-Empfehlungen und in der Medizinprodukte-Norm DIN EN 80001 beschrieben. Die Verfahrensschritte des Risikomanagements sind in ISO/IEC 27005 und DIN EN 14971 festgelegt. Allgemein ist für das IT-Sicherheitsmanagement die Norm ISO/IEC 27001 (und folgende) grundlegend.