

# Datenschutz und Datensicherheit in Krankenhaus und Praxis

Was tun im Falle der internen oder externen Bedrohung?

Markus Mohr, ManaThea GmbH, Regensburg

Selten wird im persönlichen Gespräch darüber berichtet, dass ein Sicherheitsleck im Kontext von Patientendaten ausgenutzt wurde. Noch seltener wird darüber auf Sicherheitskonferenzen oder in anderen geeigneten Medien referiert. Trotzdem sind Sicherheitsprobleme im Umgang mit Patientendaten jedoch immer wieder an der Tagesordnung, nicht zuletzt einer der Gründe, warum in Deutschland auf Datenschutz und Datensicherheit so viel Wert gelegt wird. Dieser Artikel geht von tatsächlichen Bedrohungen aus und widerspiegelt die langjährige Insider-Erfahrung des Autors als Arzt und IT-Sicherheitsexperte. In einer schematischen Übersicht bietet diese Umschau einen Überblick zu den häufigsten Bedrohungen von innen wie von außen und versucht, Strategien für deren Lösung zu geben. Auch für den Fall des „in den Brunnen gefallenen Kindes“ werden Ansätze für eine Postphylaxe gegeben.

## Ausgangssituation und Hintergründe

Seitdem Daten erhoben werden, besteht die Möglichkeit, dass sich Unbefugte dieser Daten bemächtigen. Dieser Prozess ist vom Medium der erhobenen Daten unabhängig. War es vor 20 Jahren noch einfach, sich als Arzt oder Angehöriger des medizinischen Personals verkleidet aus dem Archiv eines Krankenhauses nahezu in beliebigem Umfang Akten z. B. für Studienzwecke oder zur Nachuntersuchung im Rahmen einer Promotion ausshändigen zu lassen, ist diese Situation heute durch die überwiegend digitale Speicherung der Daten wesentlich komplexer geworden und erfordert Einiges mehr an neu erworbenen Kenntnissen und Fähigkeiten.

Das Ausmaß an Datenschutz [1] und Datensicherheit [2] in einer medizinischen Einrichtung hängt nicht nur davon ab, wie unkompliziert jemand, der dazu nicht befugt ist, an Daten herankommt, sondern „in deren digitaler Form“ insbesondere auch von grundlegenden Sicherheitsrichtlinien, die global, d. h. für alle Benutzer eines Systems, eingerichtet, gepflegt und auch gelebt werden (sog. Security Policies [3]). Aber auch weit jenseits technischer Belange bestehen Gefahren im Rahmen geschickter Gespräche mit Mitarbeitern dieser Einrichtungen, die im Kontext logischer Erwägungen dazu gebracht werden, Informationen, die nicht preisgegeben werden sollen, eben doch preiszugeben (sog. Social Engineering [4]).

Dem Datenschutz liegt in Deutschland das Recht auf informationelle Selbstbestimmung zugrunde. Wegweisend ist hierbei das Bundesdatenschutzgesetz (BDSG).

Über das konkrete Ausmaß der Bedrohung von Datenschutz und Datensicherheit existieren keine verlässlichen Zahlen. Aus vielen Gesprächen mit einzelnen Betroffenen lässt sich rekonstruieren, dass es immer wieder stellenweise Angriffe aus der inneren (eigene Mitarbeiter bzw. sich im inneren Kreis aufhaltende Personen) wie aus der Außenwelt (rein abstrakte, digitale Angriffe durch Umsetzung bekannter oder noch nicht weit bekannter Technologien) Domäne gibt. Insofern lassen sich bestenfalls Schätzungen zu diesem Thema durchführen:

Die Majorität der internen Angriffe bezieht sich auf das nicht zugelassene Beziehen diagnostischer und therapeutischer Daten z. B. in der Öffentlichkeit stehender Personen mit dazu geeigneten technischen Hilfsmitteln oder unter Ausnutzen hausintern bekannter sicherheitsrelevanter Schwachstellen. Die meisten externen Angriffe beziehen sich auf das Cracken von Web-Servern bzw. das Defacement (Änderung von zentralen Inhaltsseiten) von Webauftritten medizinischer Einrichtungen. Auch Einbruchsversuche von außen nach innen, d. h. über einen Web-Server in die „Innereien“ eines dahinterliegenden Computer-Netzwerkes sind bekannt, diese sind aber aufgrund der Tatsache, dass viele derartige Web-Server innerhalb einer sog. Demilitarisierten Zone (DMZ) liegen oder von einem öffentlichen Internet Service-Provider (ISP) gehostet werden, weniger erfolgreich und geeignet, um an sensible Daten heranzukommen.

Unter Angriff wird dabei jede wie auch immer geartete menschvermittelte Aktivität verstanden, die dazu geeignet ist oder sein soll, unbefugt an Daten überhaupt und insbesondere Daten Dritter heranzukommen.

## Die häufigsten Angriffsszenarien

An dieser Stelle gibt es mehrere Unterscheidungen, die die Angriffe allesamt aus verschiedenen Blickwinkeln betrachten. Zunächst einmal kann grob danach unterschieden werden, ob es sich um einen internen oder einen externen Angriff handelt.

Der interne Angriff stammt in der Regel aus dem eigenen Haus: Eigene Mitarbeiter, Zeitpersonal oder unbefugte Fremde sind die dafür in Frage kommenden Personenkreise. Bei allen Personen muss jedoch Zweierlei vorliegen, um einen erfolgreichen internen Angriff zu starten: Erstens das notwendige Maß an krimineller Energie, zweitens das technische

Know-how bzw. das Verfügen über ausreichende Skills beim Social Engineering (v. i.).

Der externe Angriff geschieht im Wesentlichen abstrakt und anonym ausgetragen auf einer rein technischen Ebene, ausgehend von einem oder mehreren Rechnern aus einem oder verschiedenen Netzwerken, ohne dass man in aller Regel die dahinter stehenden Einzelpersonen zu Gesicht bekommt.

In der englischsprachigen Literatur wird dazu häufig dem Schweregrad nach unterschieden zwischen folgenden Angriffsformen:

- Koordinierter Angriff
- Direkter Angriff
- Indirekter Angriff
- Unstrukturierter oder unkoordinierter Angriff

Der koordinierte Angriff entspricht demselben taktischen Vorgehen wie im Kriegsfall: Mehrere Personen planen und führen einen Angriff z. B. unter Ausnutzung mehrerer (eigener oder fremder [gekaperter]) Computersysteme durch mit dem Ziel, ein spezifisches System und von diesem ausgehend möglicherweise in einer Kettenreaktion mehrere Zielsysteme auszuschalten oder in die eigene Gewalt zu bringen. Ein typischer Vertreter dieser Angriffsform ist der sog. Distributed Denial of Service (DDoS) Angriff [5].

Direkte Angriffe richten sich üblicherweise gegen eine oder mehrere bekannte Schwachstellen innerhalb einer IT-Infrastruktur, die noch nicht oder gar nicht durch Sicherheits-Updates ausgemerzt worden sind. Ein Beispiel für einen direkten Angriff bildet der sog. Ping of Death (PoD) Angriff [6]. Zu dieser Gruppe von Angriffen gehören insbesondere auch

- Angriffe gegen die Authentifizierung eines Computersystems,
- Angriffe gegen Datenbanken und
- Angriffe gegen einzelne Software-Produkte.

Indirekte Angriffe werden meist durch sog. Schadsoftware (engl. Malware) ausgelöst und werden durch Presseberichte deshalb häufiger im öffentlichen Leben wahrgenommen. Hierzu zählen selbstverständlich auch alle Arten von Viren, Trojanern und anderen schadhafte Software-Programmen, die nur den einen Zweck haben, ein System von der ursprünglich angedachten Funktionsweise in einen anderen, vom Angreifer gewünschten Modus operandi überzuführen...

Ä

Dokumentinformationen zum Volltext-Download

Ä Titel:

Datenschutz und Datensicherheit in Krankenhaus und Praxis Artikel ist erschienen in:  
Telemedizinführer Deutschland, Ausgabe 2009

Kontakt/Autor(en):

Dr. Markus Mohr  
CEO  
ManaThea GmbH  
Josef-Engert-Strasse 11 / II  
BioPark 2  
D-93053 Regensburg  
Tel: +49 (0) 9 41 / 9 10 69 - 1 54  
Fax: +49 (0) 9 41 / 9 10 69 - 1 69  
info@manathea.de  
www.manathea.de  
Seitenzahl:  
4  
Sonstiges:

-Dateityp/ -größen:PDF /Ä Ä 103 kBÄ Click&Buy-PreisÄ inÄ Euro:0,30

Ä Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Ä  
Hier gehts zum Click&Buy-Download...

Allgemeine Infos zu Click&Buy finden Sie hier... Ä