Datenschutz und Datensicherheit in Krankenhaus und Praxis

Was tun im Falle der internen oder externen Bedrohung?

Markus Mohr, ManaThea GmbH, Regensburg

Selten wird im persÃ¶nlichen GesprÃ¤ch darÃ¼ber berichtet, dass ein Sicherheitsleck im Kontext von Patientendaten ausgenutzt wurde. Noch seltener wird darÃ¼ber 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 GrÃ¼nde, warum in Deutschland auf Datenschutz und Datensicherheit so viel Wert gelegt wird. Dieser Artikel geht von tatsÃ¤chlichen Bedrohungen aus und widerspiegelt die langjÃ¤hrige Insider-Erfahrung des Autors als Arzt und IT-Sicherheitsexperte. In einer schematischen Ãœbersicht bietet diese Umschau einen Ãœberblick zu den hÃ¤ufigsten Bedrohungen von innen wie von auÃŸen und versucht, Strategien fÃ¼r deren LÃ¶sung zu geben. Auch fÃ¼r den Fall des â€žin den Brunnen gefallenen Kindesâ€œ werden AnsÃ¤tze fÃ¼r eine Postphylaxe gegeben.

Ausgangssituation und HintergrÃ¼nde

Seitdem Daten erhoben werden, besteht die MÃ¶glichkeit, dass sich Unbefugte dieser Daten bemÃ¤chtigen. Dieser Prozess ist vom Medium der erhobenen Daten unabhÃ¤ngig. War es vor 20 Jahren noch einfach, sich als Arzt oder AngehÃ¶riger des medizinischen Personals verkleidet aus dem Archiv eines Krankenhauses nahezu in beliebigem Umfang Akten z. B. fÃ¼r Studienzwecke oder zur Nachuntersuchung im Rahmen einer Promotion aushÃ¤ndigen zu lassen, ist diese Situation heute durch die Ã¼berwiegend digitale Speicherung der Daten wesentlich komplexer geworden und erfordert Einiges mehr an neu erworbenen Kenntnissen und FÃ¤higkeiten.

Das AusmaÃŸ an Datenschutz [1] und Datensicherheit [2] in einer medizinischen Einrichtung hÃ¤ngt nicht nur davon ab, wie unkompliziert jemand, der dazu nicht befugt ist, an Daten herankommt, sondern â€“ in deren digitaler Form â€“ insbesondere auch von grundlegenden Sicherheitsrichtlinien, die global, d. h. fÃ¼r alle Benutzer eines Systems, eingerichtet, gepflegt und auch gelebt werden (sog. Security Policies [3]). Aber auch weit jenseits technischer Belange bestehen Gefahren im Rahmen geschickt gefÃ¼hrter GesprÃ¤che mit Mitarbeitern dieser Einrichtungen, die im Kontext logischer ErwÃ¤gungen dazu gebracht werden, Informationen, die nicht preisgegeben werden sollen, eben doch preiszugeben (sog. Social Engineering [4]).

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

Ãœber das konkrete AusmaÃŸ der Bedrohung von Datenschutz und Datensicherheit existieren keine verlÃ¤sslichen Zahlen. Aus vielen GesprÃ¤chen mit einzelnen Betroffenen lÃ¤sst sich rekonstruieren, dass es immer wieder stellenweise Angriffe aus der inneren (eigene Mitarbeiter bzw. sich im inneren Kreis aufhaltende Personen) wie aus der Ã¤uÃŸeren (rein abstrakte, digitale Angriffe durch Umsetzung bekannter oder noch nicht weit bekannter Technologien) DomÃ¤ne gibt. Insofern lassen sich bestenfalls SchÃ¤tzungen zu diesem Thema durchfÃ¼hren:

Die MajoritÃ¤t der internen Angriffe bezieht sich auf das nicht zugelassene Beziehen diagnostischer und therapeutischer Daten z. B. in der Ã–ffentlichkeit stehender Personen mit dazu geeigneten technischen Hilfsmitteln oder untere Ausnutzen hausintern bekannter sicherheitsrelevanter Schwachstellen. Die meisten externen Angriffe beziehen sich auf das Cracken von Web-Servern bzw. das Defacement (Ã„nderung von zentralen Inhaltsseiten) von Webauftritten medizinischer Einrichtungen Auch Einbruchsversuche von auÃŸen nach innen, d. h. Ã¼ber einen Web-Server in die â€žInnereienâ€œ 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 Ã¶ffentlichen 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 AktivitÃ¤t verstanden, die dazu geeignet ist oder sein soll, unbefugt an Daten Ã¼berhaupt und insbesondere Daten Dritter heranzukommen.

Die hÃ¤ufigsten Angriffsszenarien

An dieser Stelle gibt es mehrere Unterscheidungen, die die Angriffe allesamt aus verschiedenen Blickwinkeln betrachten. ZunÃ¤chst 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 dafÃ¼r in Frage kommenden Personenkreise. Bei allen Personen muss jedoch Zweierlei vorliegen, um einen erfolgreichen internen Angriff zu starten: Erstens das notwendige MaÃŸ an krimineller Energie, zweitens das technische

Know-how bzw. das VerfÃ¼gen Ã¼ber 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 bekÃ¤me.

In der englischsprachigen Literatur wird dazu hÃ¤ufig dem Schwergrad 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 fÃ¼hren einen Angriff z. B. unter Ausnutzung mehrerer (eigener oder fremder [gekaperter]) Computersysteme durch mit dem Ziel, ein spezifisches System und von diesem ausgehend mÃ¶glicherweise 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 Ã¼blicherweise gegen eine oder mehrere bekannte Schwachstellen innerhalb einer IT-Infrastruktur, die noch nicht oder gar nicht durch Sicherheits-Updates ausgemerzt worden sind. Ein Beispiel fÃ¼r einen direkten Angriff bildet der sog. Ping of Death (PoD) Angriff [6]. Zu dieser Gruppe von Angriffen gehÃ¶ren 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) ausgelÃ¶st und werden durch Presseberichte deshalb hÃ¤ufiger im Ã¶ffentlichen Leben wahrgenommen. Hierzu zÃ¤hlen selbstverstÃ¤ndlich auch alle Arten von Viren, Trojanern und anderen schadhaften Software- Programmen, die nur den einen Zweck haben, ein System von der ursprÃ¼nglich angedachten Funktionsweise in einen anderen, vom Angreifer gewÃ¼nschten Modus operandi Ã¼berzufÃ¼hren...

Â

Dokumentinformationen zum Volltext-Download
Â Titel:
Datenschutz und Datensicherheit in Krankenhaus und Praxis ArtikelÂ istÂ erschienenÂ in:
TelemedizinfÃ¼hrer 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.deSeitenzahl:
4Sonstiges:

-Dateityp/ -grÃ¶ÃŸe:PDF /Â Â 103 kBÂ Click&Buy-PreisÂ inÂ Euro:0,30

Â Rechtlicher Hinweis:

Hier gehts zum Click&Buy-Download...

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