M/3 Typische Schwachstellen

Als Datenschutzbeauftragter einer Gesundheitseinrichtung ist es wichtig, in der Lage zu sein, Schwachstellen der IT-Sicherheit zu erkennen, diese anzusprechen und sich für eine Verbesserung der Situation einzusetzen. Insbesondere in Gesundheitseinrichtungen, die über keinen IT-Sicherheitsbeauftragten verfügen, bestehen immer wieder Situationen, in denen die angemessenen technischen und organisatorischen Maßnahmen nicht getroffen wurden. Dieses Kapitel soll den Blick auf typische Schwachstellen richten, die sich in der Praxis immer wieder finden lassen.

M/3.1 Fehlende Laptopverschlüsselung

Immer wieder finden sich in der Praxis Schwachstellen bei der Absicherung von Laptops.

Ein Laptop ist als mobiler Client insbesondere dem Risiko ausgesetzt, verloren zu gehen oder gestohlen zu werden. Diesem Risiko muss in der Praxis begegnet werden. Es reicht dabei nicht aus, sich auf den Schutz der Benutzerauthentisierung des Betriebssystems allein zu verlassen.

Hinweis: Unter **Authentisierung** wird die Anmeldung gegenüber einem System verstanden. Der Nutzer authentisiert sich gegenüber dem System als berechtigte Person. Meist geht die Authentisierung mit der Eingabe von Nutzername und Passwort einher. Es sind aber auch eine Reihe anderer Authentisierungsmerkmale denkbar, z. B. Fingerabdruck oder Token (vgl. hierzu auch M/5.2).

Die Eingabe von Nutzername und Passwort zur Anmeldung am Betriebssystem reicht nicht aus, um die auf der Festplatte gespeicherten Daten zu schützen. Ist ein Laptop z. B. nur über die Benutzerauthentisierung des Betriebssystems geschützt und geht der Laptop verloren, so kann ein unbefugter Dritter leicht Zugriff auf die Daten bzw. Zugang zum Betriebssystem erlangen. Wie genau?

- Zum einen besteht die Möglichkeit, die Festplatte aus dem Laptop aus- und in einen anderen Rechner als zweite Festplatte einzubauen. Auf die Daten der Festplatte kann dann direkt zugegriffen werden, ohne dass

das Betriebssystem noch gestartet und ein Nutzername oder ein Passwort eingegeben werden müsste.

- Eine weitere Möglichkeit besteht darin, dass der gefundene Rechner mit einem anderen Betriebssystem (welches sich z. B. auf CD oder einem USB-Stick befindet) gebootet wird. Hierzu muss im BIOS des Laptops eingestellt werden, dass von CD oder USB-Stick gestartet werden soll. Auch hier ist ein Direktzugriff auf die Daten möglich.

Hintergrundwissen: Das BIOS befindet sich auf einem im Rechner – genau genommen auf dem Mainboard – eingebauten Speicherchip. Das BIOS (basic input/output system) sorgt u. a. dafür, dass die vorhandenen Hardwarekomponenten angesprochen und der Rechner gestartet werden kann. In den BIOS-Einstellungen, die in der Regel über das Drücken bestimmter Tasten während des Startvorgangs erreicht werden können, kann u. a. festgelegt werden, ob ein Rechner zuerst auf der Festplatte oder zuerst auf einer eingelegten CD nach einem vorhandenen Betriebssystem suchen soll, um dieses zu starten. Es kann also z. B. eingestellt werden, ob das Betriebssystem auf Festplatte C:\ gestartet oder ob versucht werden soll, von der im Laptop eingelegten CD zu starten.

Zur Absicherung von Laptops ist es daher häufig sinnvoll, auch die BIOS-Einstellungen durch ein Passwort zu schützen, damit unbefugte Dritte nicht ohne Weiteres die Einstellungen verändern können.

- Noch einfacher ist es, wenn spezielle Programme verwendet werden, welche in der Lage sind, das Erfordernis der Authentisierung zu umgehen. Hierzu muss der gefundene Rechner von einem anderen Speichermedium gebootet werden (z. B. CD oder USB-Stick), welches eine Software enthält, die das Betriebssystem automatisch dazu bringt, auf die Benutzeranmeldung zu verzichten. Mit Hilfe solcher Programme, die relativ einfach im Internet zu finden sind (z. B. „Kon-Boot“), kann ein unbefugter Dritter einen gefundenen Laptop, der nicht weiter abgesichert ist, starten. Die Eingabe von Nutzername und Passwort am Anmeldebildschirm des Betriebssystems wird hiermit umgangen.

Ein wirksamer Schutz gegen ein solches Vorgehen ist die volle und sichere Verschlüsselung aller Festplatten, welche nur durch Eingabe eines Pre-Boot-Passwortes aufgehoben werden kann.

Hinweis: Eine Pre-Boot-Verschlüsselung liegt dann vor, wenn die Verschlüsselung während einer frühen Phase des Bootvorgangs und in jedem Fall vor dem Starten des Betriebssystems aufgehoben werden muss.

Eine solche Absicherung führt dazu, dass ausgebaute Festplatten nicht mehr im Klartext gelesen werden können. Sichtbar wären lediglich die verschlüsselten Daten, mit denen ein unbefugter Dritter jedoch nichts anfangen könnte. Auch das Booten von einem anderen Speichermedium wäre nicht mehr erfolgreich, da die Daten ebenfalls verschlüsselt blieben und somit weder ein Zugriff noch eine Änderung der Authentisierungsprozesse möglich wäre.

Bei der Auswahl des Passwortes, welches zur Entschlüsselung eingegeben werden muss, sollte unbedingt darauf geachtet werden, dass dieses lang und komplex genug ist. Das Passwort sollte mindestens acht Zeichen lang sein, mindestens eine Zahl, ein Sonderzeichen, einen großen und einen kleinen Buchstaben enthalten und nicht leicht zu erraten sein. Andernfalls hätte ein Angreifer die Möglichkeit, das Passwort zu knacken. Hierzu stehen Programme zur Verfügung, die in Sekundenschnelle automatisch hunderttausende von Passwörtern ausprobieren. Es wird hierdurch also nicht versucht, die sichere Verschlüsselung zu knacken, sondern das oftmals viel unsicherere Passwort. Wenn möglich sollte daher eine Software zur Verschlüsselung gewählt werden, welche die Einstellung von Passwortkonventionen erlaubt und diese auch technisch erzwingt. Zudem sollte die Software im Idealfall falsche Passworteingaben erkennen und die erneute Eingabe verzögern bzw. ab einer gewissen Anzahl sperren.

Hinweis: Ein wichtiger Baustein bei der Absicherung von mobilen Clients ist die sichere Pre-Boot-Vollverschlüsselung der Festplatte. Ein Einsatz ohne Vollverschlüsselung ist unsicher und in der Praxis grundsätzlich nicht akzeptabel.

Gelegentlich wird in der Praxis als Argument gegen eine Vollverschlüsselung angeführt, dass Nutzer ihr Passwort oft vergessen und sich auf dem Laptop sowieso keine schützenswerten lokalen Daten befänden, weil die Nutzer nur auf dem Unternehmensserver Dateien speichern dürfen.

Hier ist jedoch zu entgegnen, dass es kaum ausgeschlossen werden kann, dass nicht doch sensible personenbezogene Daten auf dem Laptop lokal gespeichert sind. So besteht immer die Gefahr, dass Nutzer Daten auf lokalen Datenträgern ablegen – sei es absichtlich oder unwissentlich – oder Anwendungen ohne Wissen des Nutzers Daten zumindest temporär lokal speichern. Je nach Ausgestaltung der IT-Landschaft befinden sich auf dem Laptop möglicherweise auch Sicherheitszertifikate, die vor unbefugtem Zugriff geschützt werden müssen. Schließlich ist auch zu bedenken, dass Laptops nur durch eine Vollverschlüsselung vor einer Manipulation während des Verlusts angemessen geschützt werden können. Andernfalls ist es denkbar, dass ein Angreifer einen Laptop stiehlt, den nicht geschützten Laptop manipuliert (z. B. einen Trojaner oder Keylogger installiert), den Laptop wieder zurückgibt und somit Zugriff zum Netzwerk der Gesundheitseinrichtung erlangt.

M/3.2 Echtdaten sind keine Testdaten

In der Praxis entsteht an unterschiedlichen Stellen immer wieder das Verlangen nach Testdaten. Dies ist z. B. häufig der Fall, wenn eine Gesundheitseinrichtung ein altes Softwareverfahren durch ein neues Softwareverfahren ablösen möchte und das neue Verfahren von der Herstellerfirma noch auf die individuellen Bedürfnisse der Gesundheitseinrichtung angepasst werden soll. Sehr wahrscheinlich wird die Herstellerfirma bereits im Rahmen der Anpassungsarbeiten nach Testdaten fragen, um die Funktion der Software mit möglichst realistisch aufgebauten Datensätzen testen zu können. Die neue Software wird vor ihrer Einführung zudem den Mitarbeitern der Gesundheitseinrichtung im Rahmen von Schulungen vertraut gemacht werden müssen. Auch hierfür werden Testdaten benötigt.

Ein Export von personenbezogenen Echtdaten in eine Testumgebung sollte jedoch grundsätzlich vermieden werden. Eine Verwendung von personenbezogenen Daten zu Testzwecken verstößt grundsätzlich gegen das datenschutzrechtliche Zweckbindungsgebot und ist bereits daher regelmäßig unzulässig.

Im Umfeld von Gesundheitseinrichtungen ist zudem an die Wahrung der berufsrechtlichen Schweigepflichten aus § 203 StGB zu denken. Die Weitergabe von echten Patientendaten zu Softwaretestzwecken ist mit der Schweigepflicht grundsätzlich nicht zu vereinbaren.

