E-Health konkret

"Die IT steckt oft noch in der Steinzeit"

Mi 14.09.2016 - 10:00 Uhr | Aktualisiert 14.09.2016 - 10:00
von Christoph Grau (/user/18708)

Pascal Walliser ist von 2009 bis 2013 CIO der Solothurner Spitäler gewesen. Anfang 2016 wurde er mit dem Spin-off namens Fluance eigenständig. Im Gespräch erläutert der Sicherheitsspezialist, wie IT-Sicherheit im Spital aussehen sollte.

Pascal Walliser, CEO von Fluance.

In den letzten Monaten gab es viele Berichte über Cyberangriffe in Spitälern. Ist dies auch in der Schweiz ein Problem?

Pascal Walliser: Meiner Erfahrung nach war jeder Kollege sicherlich schon einmal in irgendeiner Form von einem Cryptolocker betroffen und musste ein Back-up einspielen. In fast jedem Haus werden sich Personen finden, die betroffen sind. Leider gibt es noch keine wirksamen Tools, die Abhilfe schaffen.

Sehen Sie also eine akute Gefahr für die Spitäler?

Es gab aus meiner Sicht schon bedrohliche Fälle. Aber die Segmentierung der Spitäler in Abteilungen ist hier ein Vorteil. Viel mehr betroffen sind meiner Ansicht nach Arztpraxen. Denn diese können sich hohe Investitionen in Back-ups oft nicht leisten. Generell schätze ich die Zahlungsbereitschaft an die Erpresser aber als sehr gering ein, auch wenn der Ausfall von ein paar Tagen bei kleinen Praxen gravierende wirtschaftliche Folgen haben kann.

Wenn doch Probleme durchaus häufig auftreten, warum hört man dann nichts davon?

Solche Vorfälle werden in der Regel nicht an die grosse Glocke gehängt. Es gibt eine Mentalität der Verschwiegenheit. Die meisten glauben, geschützt zu sein, dabei werden einige Angriffe oft nicht einmal registriert.

Wie hat sich die Bedrohungslage Ihrer Meinung nach entwickelt?

Das ist schwer zu sagen. Das Hauptproblem ist, dass viele unberechtigte Zugriffe gar nicht erst registriert werden. An der Oberfläche glauben wir, sicher zu sein, aber die Informatik steckt oft noch in der Steinzeit, und die Sicherheit ist trügerisch. Und dabei sind die Spitäler noch nicht einmal voll vernetzt. Für die Angreifer könnte es noch lukrativer werden, wenn die Systeme erst einmal voll miteinander vernetzt sind und der Schaden bei erfolgreichen Angriffen entsprechend höher ausfällt.

Wo sehen Sie die Hauptschwachstelle?

Eindeutig auf der Nutzerseite. Der Umgang mit Passwörtern etwa ist noch viel zu sorglos. Zugangsdaten werden häufig noch auf Monitore oder Laptops geklebt. Das zugrundeliegende Problem ist hier die fehlende Akzeptanz. Diese hört dann auf, wenn die Usability durch die Sicherheit eingeschränkt wird. Wenn die Sicherheit zulasten der Arbeitsabläufe geht, dann wird sie von den Anwendern zu Recht abgelehnt.

Was könnte hier helfen?

Das momentan weit verbreitete Zwei-Wege-System etwa mit Passwort und Chip-Karte ist nicht praktikabel. Eventuell sind biometrische Lösungen vielversprechend. Zumindest würden diese meiner Einschätzung nach leichter akzeptiert werden als die jetzigen Lösungen. Eventuell könnte das Smartphone in Zukunft als Schlüssel fungieren. Technologisch gibt es schon zahlreiche Lösungen, bis diese aber auch für den klinischen Alltag einsatzbereit sind, könnte noch einige Zeit vergehen.

Wie sieht Ihrer Meinung nach also ein ideales Sicherheitssystem **aus?**

Es braucht Sicherheit by Design. Die Geräte sollen den User erkennen, ohne dass diese viel dazutun müssen. Dies würde die Akzeptanz erheblich steigern. Es braucht kein zusätzliches Vorhängeschloss. Nur wenn die Sicherheit schon mit in die Prozesse implementiert ist. Gleichzeitig muss sich ein kulturelles Bewusstsein für Sicherheitsfragen herausbilden. Meine Idealvorstellung ist hier ein Flugzeugcockpit. Alle Abläufe sind unter Sicherheitsaspekten optimiert und automatisiert.

GESUNDHEIT (/TAGS/GESUNDHEIT)

WEBCODE: IH021603

KOMMENTARE