CIOS IN SPITÄLERN MÜSSEN SICH BYOD STELLEN

Bei der Verwaltung mobiler Geräte in Spitälern sehen sich IT-Verantwortliche – wie in den meisten Unternehmen auch – mit der Frage konfrontiert, wie mit der Nutzung privater Handys umgegangen werden soll. Damit Nutzer nicht unsichere Apps verwenden, müssen ihre Geräte mit einem bestmöglichen Anwendererlebnis ins Mobile Device Management eingebunden werden.

VON JOEY KEUSCH

IT-Verantwortliche in Spitälern sehen sich einer Vielzahl von Herausforderungen ausgesetzt. Steigender Kostendruck und immer höhere Anforderungen an Effizienzsteigerungen müssen in Einklang mit der Patientendatensicherheit gebracht werden. Hinzu kommt, dass die Vorschriften des im April 2017 in Kraft getretenen eidgenössischen Patientendatengesetzes strengere Auflagen für den Umgang mit sensiblen, besonders schützenswerten Patientendaten vorsehen. Aus Sicherheitsgründen ist deshalb auch in den meisten Spitälern die Nutzung privater Smartphones oder Tablets verboten.

Private Gerätenutzung ist Realität

Dennoch werden auch in Spitälern private Geräte genutzt. Fachpersonal verwendet seine eigenen Handys beispielsweise, um Patientendaten mit anderen Kollegen zwecks Diagnosestellung zu teilen. Dabei werden Tools wie Dropbox oder andere unsichere Apps verwendet. Das aber ist nicht im Einklang mit der Sicherheit der Spital-IT und der Patienteninformationen. Sei es, weil sich Nutzer der Gefahr durch Ransomware und anderer Sicherheitsprobleme gar nicht bewusst sind, sei es, weil ihnen schlicht kein anderes Werkzeug zur Verfügung steht. Das ist ganz einfach deshalb so, weil der Use Case für die Nutzung privater Geräte gar nicht vorgesehen ist. Dazu kommt, dass BYOD (Bring Your Own Device) wegen der entstehenden Sicherheitsrisiken eine der grossen Herausforderungen darstellt, denen sich auch CIOs in Spitälern ausgesetzt sehen.

Bestmögliches Anwendererlebnis bieten

Denn genauso wie in anderen Unternehmen verwenden Nutzer Anwendungen, die nicht den Sicherheitsrichtlinien entsprechen. Das betrifft indes nicht nur die Verwendung privater Smartphones. Dasselbe geschieht auch mit Geräten, die von der Organisation zur Verfügung gestellt und ins Netzwerk des Spitals eingebunden sind. Dabei werden beispielsweise Patientendaten oder Bilder von Diagnosegeräten ausgelesen und mit anderen via Dropbox oder WhatsApp geteilt. Dass die Nutzer mit der Verwendung eigener Tools aber auch Metadaten über Patienten weitergeben oder Erpressern die Möglichkeit geben, die Spital-IT lahmzulegen, sind sie sich gar nicht bewusst. Aus diesem Grund ist es unerlässlich, dem Nutzer ein bestmögliches Anwendererlebnis zu bieten. Man sollte je nach Anwendungsfall die Möglichkeit bereitstellen, ohne Barrieren zu arbeiten. Dazu gehören geeignete, sichere Tools für den Datentransfer und die Zusammenarbeit. Private Geräte müssen zudem wie Handys oder Tablets des Spitals automatisiert in das Netzwerk mit entsprechenden Sicherheitsmechanismen eingebunden werden. Gefahr droht auch durch medizinische Apparate, wenn sie mit Software betrieben werden, die in die Jahre gekommen ist.

Fazit

Anwendungsfälle mit BYOD sollten in Spitälern ernst genommen werden. Die Use Cases müssen ins Mobile Device Management (MDM) mit eingebunden und in Gruppen aufgeteilt werden, vom administrativen Personal über die Spital-Gastronomie bis hin zum medizinischen Fachpersonal. BYOD muss neben den vom Spital zur Verfügung gestellten Geräten in einer intelligenten MDM-Strategie seinen Platz haben. Damit lassen sich nicht nur Sicherheitsprobleme in den Griff kriegen und gesetzliche Auflagen erfüllen, sondern erst noch Kosten sparen. Der CIO muss sich aber der Herausforderung stellen und im Kampf gegen den sorglosen Umgang mit unsicheren Hilfsmitteln bei den Anwendern das nötige Bewusstsein schaffen, ihnen aber auch ihren Anforderungen entsprechend benutzerfreundliche Instrumente zur Verfügung stellen.

ÜBER DEN AUTOR

Joey Keusch ist Key Account Manager bei Nomasis AG

Hinweis: Dieser Artikel erschien erstmals im «IT For Health» vom 7. März 2018

IMPRESSUM

Das swissICT Magazin ist das offizielle Publikationsorgan von swissICT und wird direkt an die Mitglieder versandt. Es steht ausserdem als PDF gratis im Webshop unter www.swissict.ch zur Verfügung und erscheint 4-mal jährlich, zum nächsten Mal am 15. August 2018.

Herausgeber: swissICT, Vulkanstrasse, 8048 Zürich

Redaktionsleitung: Simon Zaugg, simon.zaugg@swissict.ch, Tel. Direkt: 043 336 40 28

Anzeigen: Carol Lechner, carol.lechner@swissict.ch

Redaktionelle Mitwirkung: Thomas Flatt, Joey Keusch, Serge Müller, Roman Pfenninger, Fridel Rickenbacher, Fritz Wuethrich

Korrektorat: Regula Sigg, Zürich

Layout & Grafik: Urs Staudenmann, Bern

Druck: bc medien ag, Print | Crossmedia | Web Pumpwerkstrasse 11, 4142 Münchenstein

Druckauflage: 4000 Exemplare