SPRINGER NATURE

Wirtschaftsinformatik & Management

Schießen Sie auf den Administrator

Dr. Markus Morawietz

Reprinted from Wirtschaftsinformatik & Management
Vol. 14, No. 2, pp. 99–102, April 2022
© 2022 Springer Nature Limited. All rights reserved.

Schießen Sie auf den Administrator

Warum viele Krankenhäuser in Deutschland in Sachen IT schlecht aufgestellt sind.

Wirtschaftsinformatik & Management 2022 • 14 (2): 99–102
https://doi.org/10.1365/s35764-022-00409-3
Angenommen: 28. Februar 2022
Online publiziert: 17. Mai 2022
© The Author(s), under exclusive licence to Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

Dr. Markus Morawietz (✉)
ist Managing Partner der Dr. MORAWIETZ Consulting & Training GmbH, ein auf Migrationen im Microsoft-Umfeld spezialisiertes Unternehmen. Das Unternehmen betreut mittelständige Unternehmen (bis 10.000 Arbeitsplätze) und hat ca. 150 Krankenhäuser im Kundenkreis. Dort wurden mehr als 250 Migrationen erfolgreich ohne Betriebsunterbrechung durchgeführt. Das Motto ist „KIS (keep IT simple)" und leicht zu managen.
m.morawietz@morawietz.de

[1]Bensheim, Deutschland

In François Truffauts berühmtem Film „Schießen Sie auf den Pianisten" geht es natürlich um ganz andere Dinge als die Sicherheit von Daten im Krankenhaus; der Titel kam uns in den Sinn, weil viele IT-Abteilungen in Krankenhäusern mit einem einzigen Admin-Account arbeiten. Das macht es de facto unmöglich, das entsprechende Passwort zu ändern, wenn etwa ein Administrator den Betrieb verlässt. Um auf der sicheren Seite zu sein, müsste man den Admin eigentlich erschießen. Macht und will natürlich niemand. Die Folge solch fahrlässiger Vorgänge sind aber Krankenhausdaten, die viel zu leicht auszuspähen und zu missbrauchen sind. Und im Zweifel bekommt das nicht mal jemand mit, weil man gar nicht sehen kann, wer, wann welchen Zugang benutzt hat – es gibt ja nur den einen.

Mangelwirtschaft

Insgesamt ist die IT in deutschen Krankenhäusern geprägt durch Budget- und Ressourcenknappheit. IT-Ausgaben sind nicht ausreichend geplant, es dominieren Einzelentscheidungen. Und die Gehälter, die in dieser Branche IT-Fachleuten angeboten werden, sind nicht konkurrenzfähig. In der Folge bekommt man meist unterdurchschnittlich fähige Mitarbeiter, was die Probleme zusätzlich verschärft. Ein weiterer Faktor ist die Haltung der Geschäftsleitung. Diese sieht in der IT vor allem einen Kostenfaktor und nicht das Rückgrat der Prozesse. Auch das ist ein Grund für die Neigung zu punktuellen Einzelentscheidungen, die Probleme lösen, die das Krankenhaus gar nicht hat, und die bestehenden nicht angehen. So wird etwa viel Geld in Firewalls investiert, obwohl schon lange die weitaus meisten Angriffe von innen erfolgen – durch Phishing, Identitätsdiebstahl und Ähnliches. Auch der Aufbau von spezifischem Know-how wird in der Regel sträflich vernachlässigt.

KRITIS in kritischem Zustand

Insgesamt kann man sagen, dass das Thema kritische Infrastrukturen, kurz KRITIS, zu wenig als Treiber angenommen wird. Insbesondere bei den privilegierten Accounts mit umfassenden Lese- und Schreibrechten stellen in den allermeisten Fällen die IT-Abteilungen der Krankenhäuser selbst das größte Sicherheitsrisiko dar. Solche Accounts sind häufig nicht mit ablaufenden Kennwörtern geschützt. Es fehlt an einer Bedarfsermittlung, welche Rechte ein Mitarbeiter in seiner Rolle überhaupt braucht. Das führt dazu, dass unkritische Routinearbeiten mit Accounts vorgenommen werden, die über viel zu umfangreiche Rechte verfügen. Auszubildende in der EDV-Abteilung haben dann teils Domänen-Admin-Rechte, mit der Begründung, sie würden im Laufe der Ausbildung ja in unterschiedlichen Abteilungen arbeiten. Das kann man nur grob fahrlässig nennen.

Gleiche Rechte für alle

Hinzu kommt, dass Accounts mit umfassenden Rechten häufig nicht einmal personalisiert sind. Über Jahre werden Konten wie „Administrator" von mehreren Personen genutzt. Sämtliche Mitarbeiter der IT erhalten oft stan-

dardmäßig Domänen-Adminrechte, obwohl das für die meisten gar nicht erforderlich ist. Aber es kommt noch doller, auch externe IT-Dienstleister erhalten diese Rechte und, als Sahnehäubchen, die Zugriffe mittels solcher Accounts werden nicht einmal überwacht und aufgezeichnet. Das führt dazu, dass Angriffe mit hoher Wahrscheinlichkeit gar nicht erst bemerkt werden. Dabei böten kostenfreie Konzepte wie das Tier-Modell oder LAPS erhebliches Verbesserungspotenzial, ohne zu großen Mehrkosten zu führen.

Der Krankenhauszukunftsfonds (KHZF) sollte eigentlich helfen, die Probleme der Krankenhaus-IT zu beheben. Leider wurden die beantragten Gelder in vielen Fällen bis heute nicht ausgezahlt und es herrscht Unklarheit über den Status von Anträgen. Damit geraten geplante Verbesserungsinitiativen ins Stocken. Ein weiteres Ärgernis bei diesem Thema. Die entscheidende Stellschraube ist aber, wie die hier genannten Beispiele zeigen, das Bewusstsein in den IT-Abteilungen der Krankenhäuser und in der Geschäftsführung. Man kann den Betroffenen nur zurufen, wachen Sie auf, bevor Sie in ernste Schwierigkeiten geraten.

SfP
Mehr zum Thema finden Sie online
www.springerprofessional.de/wum

Hier steht eine Anzeige.

Springer