CASE STUDY

FUDO Referenz mit Herr David Hellenbart von St. Josefs-Hospital Wiesbaden

Das St. Josefs-Hospital ist ein Akutkrankenhaus in der hessischen Landeshauptstadt Wiesbaden. Als 1876 gegründetes Traditionskrankenhaus, verfügt es heute über zwölf medizinische Fachabteilungen mit 531 Betten und knapp unter 30000 jährlichen Patientenfällen. Herr Hellenbart ist bereits seit 2001 als IT Projektmanager dort tätig und war maßgeblich an der Umsetzung eines PAM-Systems beteiligt.

WIE IST DAS THEMA PAM INTERN AUFGEKOMMEN?

In der Vergangenheit gab es immer wieder die Informationen des BMI (Bundesministerium für Inneres) bezüglich der PAM Thematik in Krankenhäusern. Vor einigen Jahren hat dann unser IT-Dienstleister iKomm GmbH uns auf ein „Super Tool“ in diesem Bereich aufmerksam gemacht: FUDO. Leider hat es die ersten Jahre aus finanziellen Gründen für die Anschaffung nicht gereicht, als wir allerdings unser KIS-System (Krankenhausinformationssystem) umgestellt haben, war im Umzuge der großen Umstellung klar, dass wir ein solches System benötigen. Denn es kommen viele neue Dienstleister dazu und unsere Klinik muss wissen und regeln: Wie kommen Dienstleister auf die Server und was machen Sie darauf. FUDO erschien uns gegenüber TeamViewer und ähnlichen Lösungen als die optimale Lösung und hat sich auch bewährt.

WAS WAREN IHRE ERSTEN ASSOZIATIONEN ODER ERWARTUNGEN AN DAS PAM SYSTEM?

Wir wollten zunächst unsere Prozesse selber steuern: Ständig rufen Dienstleister an und fordern auf verschiedenen Wegen Zugriffe über unsichere Geschichten wie TeamViewer usw., wobei wir auch verschiedenste Lösungen installieren müssen und jedes Mal Aufwendungen mit dem Freischalten von Externen haben. Mit FUDO müssen wir niemanden aktiv freischalten. Jeder hat seine Wartungszugänge, wir kriegen die Benachrichtigung wenn jemand auf die Systeme geht und können währenddessen oder im Nachgang gut nachvollziehen, wer was gemacht hat.

BESCHREIBEN SIE BITTE DIE UMSETZUNG VON DER ERSTEN BERATUNG BIS ZUR EINFÜHRUNG DER LÖSUNG.

Das Projekt dauerte zwischen zwei bis vier Wochen. Wir hatten zunächst einen kurzen Webcast in dem die Feinheiten vorgestellt wurden. Danach ist auch direkt die Entscheidung gefallen, dass wir eine entsprechende Lösung wollen. Die Hardware wurde schnell geliefert, wir haben es an einem Tag mit dem Dienstleister iKomm GmbH aus der Ferne eingebaut und am Tag darauf konnten wir bereits die ersten Dienstleister drauflassen.

ZAHLEN UND FAKTEN ST JOSEFS HOSPITAL

12 – medizinische Fachabteilungen

531 – Betten

1000 – Mitarbeiter

30000 – jährliche Patientenfällen

FUDO SECURITY

DE: +49 (0) 911 - 30 91 8 30
DE: +49 (0) 911 - 30 91 8 35
EMEA: +48 22 100 67 00

sales@fudosecurity.com
www.fudosecurity.com/de

Es war absolut unproblematisch. Im Test haben wir bereits alle Dienstleister sukzessive über die FUDO auf die Systeme gelassen, sodass wir bereits nach kurzer Zeit alle Dienstleister eingebunden hatten. Klar mussten einzelne Leute näher über die FUDO informiert werden, aber wir haben die entsprechenden Ansprechpartner bei den Dienstleistern kontaktiert, die Thematik kommuniziert, ein PDF über die zukünftige Arbeitsweisen zugeschickt und es gab hier keinerlei Probleme.

WELCHES FAZIT KÖNNEN SIE, ANDERE UNTERNEHMENSABTEILUNGEN UND DIE DIENSTLEISTER NUN ZIEHEN?

Wir waren und sind hellauf begeistert, und sind so wie es momentan läuft wunschlos glücklich. Es ist wesentlich simpler geworden, auch Mitarbeiter die nicht direkt auf das Produkt geschult worden sind können intuitiv damit arbeiten. Es ist für sie sehr einfach wenn jemand anruft, einen entsprechenden Zugriff freizugeben. Wir haben einen definierten und genormten Zugang, den richten wir ein, den können wir kontrollieren. Schluss mit verschiedenen Softwares wie TeamViewer, VMC, VPN, mit was auch immer man vorher hantiert hat. Wir haben auch bemerkt, dass die User keinerlei Probleme haben. Gut, bis auf ein bis zwei Dienstleister, die in Ihrer Firewall das RDP Protokoll nicht freigegeben hatten, aber das hat sich natürlich sofort am ersten Tag geklärt und lag an den externen Dienstleistern, war aber das einzige Problem. Von Seiten der Dienstleister gab es somit keine negativen Rückmeldungen, sie verstehen, dass wir glücklicher sind, da es wesentlich unproblematischer als TeamViewer usw. ist. Unser Datenschutzbeauftragter hat die Thematik auch direkt als gute Lösung abgesegnet und ansonsten tangiert das Thema im Unternehmen niemanden.

WARUM IST DAS GESUNDHEITSWESEN SO ANFÄLLIG FÜR CYBER-ANGRIFFE?

Ich denke, dass viele inhaltlich wertvolle Daten zur Verfügung stehen. Medizinische sowohl auch persönliche Daten, die von Krankenhäusern verwendet werden. Leider kann das zu Erpressung führen und dann wird der Schaden sehr hoch falls es sich um einen Datenverstoß handelt.

LAUT EINES BERICHTS VOM VERIZON " DATA BREACH REPORT 2019" ZEIGT SICH, DASS 58% DER VORFÄLLE INSIDER BETRAFEN - DAS GESUNDHEITSWESEN IST DIE EINZIGE BRANCHE, IN DER INTERNE BENUTZER DIE GRÖßTE BEDROHUNG FÜR EIN UNTERNEHMEN DARSTELLEN. WAS IST IHRER MEINUNG NACH DER GRUND DAFÜR?

Dieser Weg ist einfach und auch weniger aufwendig. Man hat leicht Zugang zu wertvollen Daten. Natürlich ist es schwieriger von außen einzudringen, und wenn man schon im internen Netz ist, geht alles einfacher. Man kennt die Schwachstellen, und der Zeitaufwand ist geringer....die Versuchung ist leider auch vorhanden. Darum müssen sich Klinken und das ganze Gesundheitswesen dementsprechend schützen.

SEHR GEEHRTER HERR HELLENBART, WIR BEDANKEN UNS BEI IHNEN UND IHREN KOLLEGEN FÜR DAS FREUNDLICHE GESPRÄCH UND FREUEN UNS AUF EINE WEITERHIN POSITIVE ZUSAMMENARBEIT!

Fudo Security
Vertretung in der DACH Region: iKomm GmbH
Hans Bornkessel-Straße 45
90763 Fürth, Deutschland

Unsere Kontaktinformationen:
DE: +49 (0) 911 - 30 91 8 30
DE: +49 (0) 911 - 30 91 8 35
EMEA: +48 22 100 67 00

Kontakt mit der Verkaufsabteilung:
sales@fudosecurity.com
www.fudosecurity.com/de