KTM

Dezember
2021

Krankenhaus
TECHNIK+MANAGEMENT

Die Fachzeitschrift für den HealthCare-Markt

Management

Als familienfreundliches Krankenhaus punkten

Onboarding: Mitarbeiter erfolgreich binden

Technik

Energiewende: Neue Lösungen wagen

Smarte Beleuchtung: Es werde Licht

Special

Facility Management

Titelstory

Betrieb wirtschaftlich und flexibel organisieren

www.ktm-journal.de

fbmt fachverband biomedizinische technik

DGTelemed

KKC Krankenhaus Kommunikations Centrum

Offizielles Organ des fbmt, der DGTelemed und des KKC

Krankenhaus Kommunikations Centrum

Bild: privat

KKC-Expertin Dr. Christina Czeschik, Ärztin und Medizininformatikerin

Informationssicherheit im Gesundheitswesen: ein Wettlauf

Aktuelle Daten zeigen, dass die Pandemie noch einmal zu einer Zunahme von Ransomware-Angriffen und anderen Attacken auf IT-Systeme geführt hat – auch und besonders im Gesundheitswesen. So wurde im November der zweitgrößte Anbieter von Arztpraxissoftware medatixx mit Ransomware attackiert.

Im Vergleich zu anderen Branchen gibt es im Gesundheitswesen einen großen Anteil schlecht geschützter Einrichtungen. IT-Sicherheit macht nur einen kleinen Anteil des sowieso schon knapp bemessenen IT-Budgets aus. Und selbst dort, wo die finanziellen Mittel vorhanden sind, scheitert der Ausbau sicherer Infrastruktur oft am nächsten Problem – dem Fachkräftemangel.
Dementsprechend hat der US-Sicherheitsforscher Josh Corman kürzlich beim ‚Cybersecurity in Healthcare Briefing' das Gesundheitswesen als ‚target rich and cyber poor' beschrieben, also reich an potenziellen Angriffszielen und arm an digitaler Expertise und Ressourcen, um sich gegen Angriffe zu verteidigen. Viele Krankenhäuser in den USA und auch in Europa existierten seiner Einschätzung nach sogar unterhalb einer ‚Infrastruktur-Armutsgrenze'.
Zum Briefing hatten das US-Generalkonsulat in Düsseldorf und die US-Botschaft in Wien Teilnehmer aus der DACH-Region eingeladen. Thema war unter anderem die grenzübergreifende Zusammenarbeit im Kampf gegen Cyberkriminalität. Internationale Kooperation ist hier ein Muss, wie Erfolge von Europol aus der letzten Zeit zeigen. Denn Angreifer haben bei der Wahl ihrer Ziele noch nie vor Ländergrenzen haltgemacht. In den letzten Jahren kooperieren und expandieren sie international und erfreuen sich dabei der Synergieeffekte in einem zunehmend differenzierten ‚Markt'.
Das Fazit der Experten? Investitionen in die IT-Sicherheit im Gesundheitswesen seien nicht optional, sondern existenzielle Grundlage für die Patientenversorgung. In innovative Technologien zu investieren, ohne dass eine sichere Infrastruktur vorhanden ist, sei vergleichbar mit dem Betrieb eines OPs ohne ausreichende Hygienemaßnahmen. Hier wie dort führe die Hoffnung, dass es dieses Mal noch gut geht, zuverlässig aufs Glatteis.

Ransomware als Erfolgsgeschichte?

Am 9. November gelang einer Europol-Gruppe ein wichtiger Schlag gegen die Cyberkriminalität. Bei einer internationalen Polizeiaktion in 17 Ländern wurden mehrere Hintermänner einer Hackerbande festgenommen, die mit der Erpressersoftware REvil rund 7.000 Ziele angegriffen hatten. Nach der Einschleusung auf 175.000 Computern weltweit kassierten sie mindestens 200 Millionen Dollar Lösegeld. Zumindest alle Verschlüsselungsopfer vor dem 13. Juli 2021 können nun ihre Daten wieder entschlüsseln, nachdem seit September 2021 bei www.bitdefender.de ein kostenloser Decryptor veröffentlicht ist. Einen Monat später gelang es internationalen Ermittlern, die Infrastruktur von REvil zu hacken und deren Websites abzuschalten.
Beim Geschäftsmodell ‚Ransomware as a Service' (RaaS) vermieten die Entwickler ihre Software an Erpressergruppen. KKC-Expertin Dr. Christina Czeschik schreibt dazu in ihrem Serapion-Blog: „RaaS funktioniert analog zu anderer ‚Software as a Service' (SaaS) wie Zoom oder Microsoft Office 365. Die Entwickler sind für Programmierung und Support zuständig, der Kunde für den Einsatz der Software. Für Ransomware heißt das: Der Kunde kauft die Lizenz, eine bestimmte Ransomware benutzen zu dürfen. Wie er sie unter die Leute bringt, ist dann seine Sache – die Entwickler geben aber hilfreiche Tipps oder stellen sogar Community-Foren zum Erfahrungsaustausch zur Verfügung.
Diese Professionalisierung führt auch zu mehr ‚Kundenfreundlichkeit' in Richtung der Angriffsziele: Hier gibt es Handbücher, Support-Websites und sogar Hotlines, in denen unbedarfte Ransomware-Opfer sich erklären lassen können, wie sie eine Überweisung in einer Kryptowährung tätigen oder wo auf der Benutzeroberfläche sie schließlich den erkauften Schlüssel eingeben können. So viel Aufwand kostet natürlich. Dabei sind die Preismodelle so unterschiedlich wie bei legaler SaaS: Die Entwickler bieten verschiedene Leistungsumfänge zu verschiedenen Festpreisen an oder verlangen eine prozentuale Beteiligung am Gewinn (also den Lösegeldern)."
Das kriminelle Businessmodell entwickelt sich weiter, wie Dr. Czeschik beobachtet: „Als es sich herumgesprochen hatte, dass die Wieder-

herstellung der eigenen Daten aus Sicherheitskopien ein sicherer Ausweg aus dem Ransomware-Dilemma ist, drohten die ersten Angreifer mit Veröffentlichung der erbeuteten Daten. Einige Angreifer verzichten schon auf die Verschlüsselung der Daten und versprechen als Gegenleistung für die Ransom-Zahlung Immunität gegenüber zukünftigen Angriffen, jedenfalls vor der eigenen Bande. Also Schutzgeld statt Lösegeld. Wenden sich die Cyberhacker bald der Kleinkriminalität zu, indem sie auf spektakuläre Angriffe verzichten und nur kleine Summen von Schutzgeld von vielen Opfern erpressen?“
www.serapion.de

BSI-Bericht 2021 zur IT-Sicherheit: Angespannt bis kritisch

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) deckt mit seinem aktuellen Bericht zur IT-Sicherheit in Deutschland den Zeitraum der Corona-Pandemie bis Mai 2021 ab. Ausgelöst auch durch die massive Auslagerung von Firmenarbeiten auf den Homeoffice-Bereich haben sich die cyberkriminellen Erpressungsmethoden spürbar ausgeweitet. Wurden im vorigen Berichtszeitraum noch durchschnittlich 322.000 neue Varianten pro Tag bekannt, so lag der Tagesindikator im aktuellen Berichtszeitraum bei durchschnittlich 394.000 Varianten. Das entspricht einem Zuwachs von gut 22 Prozent. Insgesamt haben Angreifer im aktuellen Berichtszeitraum damit rund 144 Millionen neue Schadprogramm-Varianten produziert. *

HOGAST CARE

Gebündelter Einkauf für Sozialeinrichtungen

Krankenhäuser und Pflegeheime bewegen sich innerhalb enger Budgetgrenzen. Daher gilt es, wirtschaftlich zu denken, um Spielraum für das soziale Handeln zu gewinnen. Eine Möglichkeit für die Ausgabensenkung, die bisher kaum genutzt wurde, ist der gemeinsame Einkauf. Dieser Bedarfsbündelung hat sich Hogast.Care verschrieben. Die Einkaufsgemeinschaft nutzt das Lieferpartner-Netzwerk der Hogast Deutschland, einer seit vielen Jahren aktiven Einkaufsorganisation für Hotels und Gastronomiebetriebe, und das Know-how der österreichischen Handover im Medizinbereich. Mitglieder profitieren von optimierten Konditionen in allen relevanten Warenbereichen: von Food & Beverage über Non-Food-Artikel, Strom und Gas bis hin zu Medizinprodukten. Besonderes Gewicht wird auf regionale und nachhaltige Anbieter gelegt.*

AKTIONSBÜNDNIS PATIENTENSICHERHEIT

APS-Liste: Ereignisse, die wir sicher vermeiden wollen

In den USA und Großbritannien gibt es sie schon lange: Listen mit ‚Serious Reportable Events‘ oder ‚Never Events‘, also Vorkommnisse mit hohem Schadenspotenzial, die prinzipiell verhinderbar sind. Nun veröffentlicht das Aktionsbündnis Patientensicherheit e. V. (APS) eine erste Liste ‚Schwerwiegender Ereignisse, die wir sicher verhindern wollen‘ (SEVer-Liste). Sie umfasst insgesamt 22 Vorkommnisse, die im Krankenhaus, aber auch in anderen Gesundheitseinrichtungen auftreten können. Von der Veröffentlichung in Deutschland erwartet sich das Aktionsbündnis Patientensicherheit, dass die Einrichtungen des Gesundheitswesens ihre Anstrengungen nochmals erhöhen, die gelisteten Vorkommnisse mittels geeigneter Maßnahmen sicher zu verhindern.

Chronischer Tinnitus: Was wirklich hilft – und was eher nicht

Bei Tinnitus rauscht, piepst oder klingelt es ständig im Ohr, ausgelöst beispielsweise durch einen Hörsturz oder Knallgeräusche. Dies beeinträchtigt die Lebensqualität der Betroffenen erheblich, zumal dann, wenn die körpereigenen Ohrgeräusche chronisch werden. Rund zehn Millionen Menschen erkranken jährlich, bei rund 1,5 Millionen ist dieses Leiden chronisch. Diese Patientengruppe steht im Focus der überarbeiteten S3-Leitlinie, die unter Federführung der Deutschen Gesellschaft für Hals-Nasen-Ohren-Heilkunde, Kopf- und Hals-Chirurgie e. V., Bonn, auf den neuesten Stand gebracht wurde. Die aktualisierte Leitlinie verbessert die Orientierung sowohl für Ärzte als auch für Patienten. *

‚Mannheimer Hygieneskandal‘ strafrechtlich abgeschlossen

Der Bundesgerichtshof (BGH) hat die Verurteilung des früheren Geschäftsführers des Mannheimer Universitätsklinikums wegen vorsätzlichen Betreibens von Medizinprodukten entgegen § 14 Satz 2 des früheren Medizinproduktegesetzes (MPG) bestätigt (1 StR 335/21). Das Urteil des Landgerichts Mannheim vom 26. April 2021 (203 KLs 400 Js 2051/15) ist damit rechtskräftig. *

Brückenbauer Tage Herford 2022

Die Brückenbauer Tage (BBT) 2022 am 27. und 28. April 2022 auf dem BildungsCampus in Herford werden die drängenden Gesundheitsthemen unserer Zeit in jeder Hinsicht schrankenlos und neu gedacht. Die Veranstaltung wird durch eine begleitende Industrie-Ausstellung aufgewertet und damit noch interessanter.
www.brueckenbauertage.de

KKC-Terminkalender

Alle Termine finden Interessierte im KKC-Terminkalender, in dem auch alle Verbände und Förderpartner ihre eigenen Termine eintragen können: www.kkc.info/veranstaltungentermine/termineintragen

* Alle Beiträge sind in Gänze auf www.kkc.info nachzulesen.

Weitere Fragen zum KKC?
Lesen Sie auf Seite 65 dieses Hefts!

KKC-Geschäftsstelle
c/o I.O.E. Wissen GmbH
Hermann-Löns-Straße 31
53919 Weilerswist/Kreis Euskirchen
Tel.: +49 2254 8347-880
office@kkc.info
www.kkc.info