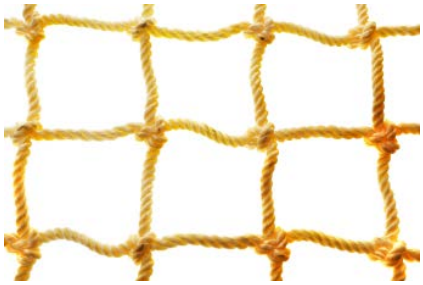

Sicherheit ungenügend

(Netzwerk: Im Test: Cloud-managed Netzwerkgeräte von Cisco Meraki; *iX* 10/2019, S. 70)

Soweit ich das sehen kann, wurde bei dem Test nicht darauf eingegangen, dass Meraki-Systeme, insbesondere Firewalls, teilweise ungenügende Sicherheitsmerkmale bieten.

Ein Beispiel, das jedoch circa 12 Monate alt ist und womöglich geändert wurde: Von Meraki Firewalls konnten IPsec VPN nur mit unzureichenden Ciphers aufgebaut werden, wie SHA1 oder DH Group 5; sehr vergleichbar mit den Einschränkungen, die man teilweise bei Cloud-Anbietern wie Azure oder AWS hat, wenn man deren Basistools einsetzen möchte, um einen Tunnel zum eigenen RZ aufzubauen.

Das öffnet potenziell Tür und Tor für staatliche Akteure (ein Schelm, wer bei Cisco, Microsoft und Amazon an die NSA denkt), bei denen man davon ausgehen muss, dass diese Ciphers nicht mehr sicher sind.

PASQUAL WEIBEL, VIA E-MAIL

Nicht Teil des Tests waren IPsec-Site-to-Site-VPN-Tunnel, sondern nur die sogenannte AutoVPN-Funktion. Nach Rücksprache teilte uns der Hersteller mit, dass die getestete Firmware unter anderem SHA2- und IKEv2-Support umfasst. Diese Funktion wird in den nächsten Versionen freigeschaltet. Grund für den verzögerten Support ist die interne Umstellung auf den Open-Source-Unterbau strongSwan. (Red.)

Ökonomischer Druck zu hoch

(Editorial: Kranke IT; *iX* 10/2019, S. 3)

Ja, es lässt einen fassungslos zurück, dass ein Viertel der untersuchten DICOM-Server offen und völlig ungeschützt erreichbar waren oder noch sind, hier kann man dem Autor nur beipflichten.

Wie bewusst dies den Verantwortlichen ist, kann ich nicht beurteilen. Folgendes sollte allerdings im Hinterkopf behalten werden, wenn man die Situation in Deutschland betrachtet: Viele öffentliche Krankenhäuser leiden unter einem hohen ökonomischen Druck und haben wenig finanziellen Spielraum für Investitionen. Dass die IT hier oftmals zu kurz kommt und eventuell sogar nur als notwendiges Übel angesehen wird, ist in meinen Augen leider brutale Realität.

Hinzu kommt, dass die öffentliche Hand für IT-Mitarbeiter wenig finanziell lukrative Stellen bereitstellt. Mit dem Gehalt, welches die bestehenden Entgeltgruppen bieten, kann man vielen Leuten doch höchstens ein müdes Lächeln entlocken. Kommen dann noch fehlende Schulungen, ständige Arbeitsverdichtungen etc. hinzu, entstehen genau solche Konstrukte wie diese unsicheren DICOM-Server.

KRITIS geht sicherlich in die richtige Richtung. Bund und Länder müssen dann allerdings dafür sorgen, dass auch finanzielle Mittel für die Umsetzungen bereitstehen, die Kliniken selbst werden dies nicht ohne Weiteres leisten können. Auch eine ausreichende qualifizierte Manpower müsste sichergestellt werden, damit alle geforderten Umsetzungen auch zeitnah erfolgen können.

Hier muss ich die Worte des Autors aufgreifen: „Viel Hoffnung habe ich allerdings nicht." – Zumindest nicht, dass sich in absehbarer Zeit etwas spürbar an der Gesamtsituation verbessern wird.

EICHHORN, VIA E-MAIL

Ausnahme, nicht die Regel

(Editorial: Kranke IT; *iX* 10/2019, S. 3)

Gestern halte ich die neue *iX* in den Händen und lese natürlich wie immer zuerst das Editorial. Eine kurze und prägnante Zusammenfassung mit Ausnahme Ihrer Schlussfolgerung.

Die hat mich schon etwas enttäuscht, insbesondere weil hier wie impliziert keine simple, monokausale Ursache vorliegt. Der Umstand, dass in einem Editorial aus vertrieblichen Gründen sehr zugespitzt formuliert wird, nimmt der unschönen Situation die Sachlichkeit für eine nachhaltige Aufarbeitung.

Man soll und darf nicht verschweigen, dass in manchen Kliniken oder Praxen erhebliche technisch-organisatorische Mängel bei Datenschutz und IT-Sicherheit vorliegen. Bei der Mehrheit jedoch nicht, denn dann wäre die Anzahl solcher Vorfälle höher. Geballte IT-Inkompetenz verorte ich im Gegensatz zu Ihnen an anderer Stelle und kann das tagtäglich belegen.

Externe IT-Dienstleister, die bei tagelangen Versuchen der Inbetriebnahme von

IT-Komponenten auffordern, doch einfach mal die Firewall zu deaktivieren oder mal alle Ports zu öffnen, weil sie mit der Konfiguration ihrer eigenen Produkte nicht zurechtkommen. Anbieter, die Produkteigenschaften wie Privacy by Design schlichtweg nicht kennen oder sich über die „überzogenen" Anforderungen der IT-Abteilung bei der GF beschweren.

Nicht dass Sie vermuten, hier bellt ein getroffener Hund. Dem ist nicht so. Jedoch weiß ich, dass viele Kolleginnen und Kollegen in Krankenhäusern und Praxen täglich auf hohem fachlichen Niveau ihr Bestes geben – und trotzdem kommt es zu Fehlern. Den Begriff IT-Inkompetenz allerdings macht man an diesen Personen oder dieser Gruppe fest und selbiger ist in dem Kontext mehr als unpassend.

DR. MANFRED CRIEGEE-RIECK,
VIA E-MAIL

Nicht gehackt, schon gar nicht automatisiert

(Sicherheit: Muraena und NecroBrowser hacken Zwei-Faktor-Authentifizierung; *iX* 10/2019, S. 96)

Wenn man bei einer Zwei-Faktor-Authentifizierung (2FA) einen der beiden Faktoren „fälschen" kann, dann ist das ein Problem des gewählten Faktors, nicht ein Problem des gewählten Verfahrens.

Wenn man SIM-Karten leicht fälschen kann, dann sind sie eben nicht als zweiter Faktor geeignet, aber deswegen ist das 2FA-Verfahren an sich nicht das Problem. Bei einem Faktor, der darauf beruht, dass man etwas hat, was andere nicht haben, ist es natürlich unerlässlich, dass dieser Faktor fälschungssicher ist.

Mit Muraena und NecroBrowser hatte ein solcher Angriff wie auf Jack Dorsey aber gar nichts zu tun: Entsprechend überraschte es nicht, dass Hacker das Konto des Twitter-CEOs trotz aktiver Zwei-Faktor-Authentifizierung übernehmen konnten. Und es ist schlichtweg auch falsch, dass Muraena 2FA hackt. Muraena ist ein Proxyserver, der auf einer Phishingseite läuft, bis sich ein Nutzer ganz regulär bei einem Dienst anmeldet (da wird nur Datenverkehr durchgeschleift bzw. mitgelesen) und den Session Cookie abgreift. Session Cookie Stealing ist aber ein uraltes Angriffsverfahren und völlig unabhängig von der Authentifizierungsmethode.

Den Session Cookie könnte Muraena bei U2F/FIDO2 genauso abgreifen, nur würde dort die Software merken, dass das eine Phishingseite ist, weil die Adresse nicht mit der Adresse der bekannten Seite übereinstimmt und für diese Phishingseite kein Schlüsselpaar vorliegt – daher würde die Anmeldung fehlschlagen. Aber genau das Gleiche wäre der Fall, wenn der Nutzer einen Passwortmanager nutzt, denn auch die würden die URL nicht zuordnen können und daher dem Nutzer gar nicht erst anbieten, sein Kennwort in das Passwortfeld zu füllen. Wie bei allen Phishingangriffen basiert auch dieser darauf, dass der Nutzer denkt, er spricht mit Seite X, und in Wahrheit spricht er aber mit Seite Y.

/MECKI78, AUS DEM *IX*-FORUM

Ergänzungen und Berichtigungen

Industrielle Sicherheit: Marktübersicht: Produkte zur Absicherung industrieller Netzwerke; *iX* 9/2019, S. 42

In der Marktübersicht fehlt die sematicon AG, die Kryptografieprodukte für die Industrie entwickelt (se.SAM-Produktfamilie) und Software zur Fernwartung von Industrie- und Steuerungsanlagen (se.MIS-Produktfamilie) anbietet.

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.

Der direkte Draht zu

Direktwahl zur Redaktion: 0511 5352-387

Redaktion iX | Postfach 61 04 07
30604 Hannover | Fax: 0511 5352-361
E-Mail: post@ix.de | Web: www.ix.de

www.facebook.com/ix.magazin
twitter.com/ixmagazin (News)
twitter.com/ix (Sonstiges)

Für E-Mail-Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion gern zur Verfügung.

Listing-Service:
Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/