Auf den Punkt

„Auf den Punkt“ ist ein neues Infoformat von *WIR in der Praxis*. Damit bieten wir Ihnen Inhalte in kurzen, knackigen Häppchen. Damit es auch hängen bleibt, bieten wir online ein kleines Quiz dazu. Schauen Sie einfach mal rein www.wir-in-der-praxis.de/aufdenpunkt/cybersecurity

© momius / stock.adobe.com

Kleines 1×1 der Cybersecurity

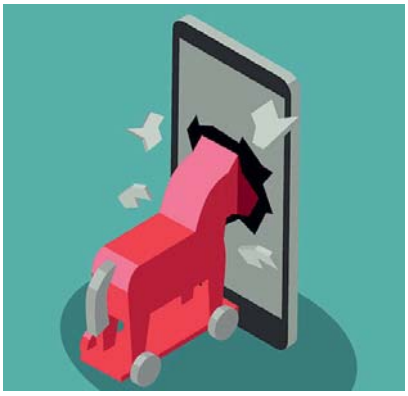
Jan Siol M.A., auxmed, Schloß Holte und Dipl.-Ing. Elmar Niebling, IT Service Manager, Moers

Messenger-Dienste = trojanische Pferde?

Messenger wie WhatsApp, Facebook Messenger oder Telegram werden nicht nur im privaten, sondern auch vermehrt im dienstlichen Umfeld eingesetzt. Die leichtfertige Verwendung von Messengern birgt ein enormes Schadenspotenzial für Praxen und ihre Patienten. Aber worin liegen eigentlich die Risiken?

Auch wenn die Messenger im direkten Chat verschlüsselt sind, ist es etwas anderes, wenn über diese Verbindung Dokumente oder beliebige andere Dateien versendet werden. Diese müssen nicht zwangsweise auch verschlüsselt sein. Die gesicherten Daten werden meist unverschlüsselt gespeichert!

Wenn aus der Praxis Patientendaten an Patienten, Labore oder Ärzte gesendet werden, ist nicht zwingend sichergestellt, dass nicht auch andere Zugriff auf diese Daten erhalten können. Eine Datenschutzverletzung nach Datenschutz-Grundverordnung (DSGVO) liegt dann zwangsläufig vor. Auch arbeitsrechtlich ist es schwierig, wenn z. B. in der internen Messenger-Gruppe über Krankschreibungen, Urlaub oder Dienste gesprochen wird. Und: Private Handys sind für den Dienstgebrauch auf keinen Fall zu empfehlen!



© Tomas Knopp / Getty Images / iStock

Updates und andere nervige Meldungen

Wer kennt das nicht, dass irgendwo eine Meldung kommt, dass ein Update ansteht und dafür der PC neu gestartet werden muss. Natürlich schließt jeder von uns in diesem Moment alle offenen Programme, fährt den PC runter und trinkt in Ruhe einen Kaffee, denn die Patienten haben dafür jedes Verständnis und warten gerne. Ein Beispiel hierzu ist ganz anschaulich: Die Schadsoftware WannaCry aus dem Jahr 2017 hat eine Sicherheitslücke ausgenutzt, die zum Zeitpunkt der meisten Schäden seitens der Softwarehersteller schon monatelang geschlossen war. Hiermit wurden unter anderem auch Praxen befallen und deren Daten unwiederbringlich verschlüsselt, sofern man nicht bereit war, den Erpressern ein Lösegeld zu bezahlen. Es ging dabei nicht nur um Patientendaten, sondern auch um die Abrechnungsdaten. Resümee: Updates sind nervig, aber wichtig!

© Marta Sher / stock.adobe.com

Die Türsteher Ihrer Systeme

Firewalls sind Ihr digitaler Türsteher oder Wachschutz. Eine Zutrittsanfrage aus dem Netzwerk wird gemäß den vorgegebenen Regeln überprüft, und wenn sie sicher ist, wird der Zutritt ins interne Netzwerk freigegeben. Umgekehrt gilt das natürlich auch. Bei einer Anfrage aus dem internen Netzwerk, um auf eine bestimmte Webpage zu gehen, prüft die Firewall, ob diese als unbedenklich eingestuft wird. Ist dem so, wird der Zugang zu dieser Webpage erteilt. Anderenfalls wird der Zugang verweigert und dem anfragenden System ein Fehler mitgeteilt. Was passiert nun, wenn sich doch eine Schadsoftware in das System geschlichen hat? Ein Antivirenprogramm achtet darauf, dass sich keine Viren, Trojaner und andere Software-Schadkomponenten im System ausbreiten, um dort schwere Schäden zu verursachen. Da die Verbreitung neuer Viren und Trojaner ohne Unterlass stattfindet und täglich neue Exemplare auftauchen, ist es dringend empfohlen, die Schädlingssignaturen immer auf einem aktuellen Stand zu halten. Am besten geht das über die automatische Update-Funktion, bei der das Programm mehrmals am Tag automatisch nachschaut, ob es neue Signaturen gibt. Ist dem so, werden sie selbsttätig heruntergeladen und installiert.

© IDjessi85 / stock.adobe.com

Offene WLAN-Geräte


© vladwel / stock.adobe.com

Mit offenen WLAN-Geräten sind hier z. B. Drucker oder Scanner gemeint, die als Voreinstellung ein WLAN eingestellt haben. Machen Sie ganz einfach einen Test. Stellen Sie sich mit Ihrem Handy in die Praxis und schauen in die WLAN-Liste. Wird dort ein offenes WLAN angezeigt, das nicht passwortgeschützt ist, oder ließe sich hinter dem einen oder anderen Netzwerknamen ein Produkt vermuten? Damit ist gemeint, dass viele Hersteller ihre eigenen WLAN-Namen nach den Produkten vergeben, etwa mit der Seriennummer des Druckers oder dem Druckerhersteller im Namen (bspw: [Druckerhersteller] 45839i WLAN). Diese WLANs sind häufig ein einfaches Einfallstor, da die Geräte nach einiger Zeit zwar weiter genutzt werden, aber keine Updates mehr erfahren und somit Sicherheitslücken entstehen. Zum anderen ist nur schwer nachvollziehbar, welche Daten vom Hersteller gesammelt und ausgewertet werden.

Das „elektronische Herz" der Praxis

Ein Herz muss gut geschützt sein. In diesem Sinne auch die IT-Zentrale. Sie sollte auch nicht nebenbei eine Abstellkammer für alle möglichen Büroutensilien oder Reinigungsmittel sein. Der Zugang sollte auch nur den Personen gestattet sein, die wirklich etwas mit der IT zu tun haben (und wissen, was sie tun). Die offene Tür zum Schrank oder IT-Raum birgt aber auch noch ganz andere Gefahren. Jeder, der sich in den Praxisräumen aufhält, könnte mehr oder weniger unbemerkt ungewollte Aktivitäten entwickeln. Sei es, dass er mit einem Griff Back-up-Datenträger entwendet, in die Kabel greift und Unterbrechungen herbeiführt oder sich einfach nur informiert, welche Systeme vorhanden sind.


© rukanoga / stock.adobe.com