Für Vertrauen gibt's kein Backup

Digitalisierung Cyberangriffe auf Spitäler, Praxen und Heime häufen sich. Entwendete Daten lassen sich (vielleicht) zurückgewinnen oder wiederherstellen – das Vertrauen der Patientinnen und Patienten jedoch kaum. Kultivieren darum auch Sie Ihr Risikobewusstsein!

Lucas Schult

Waren Sie dieses Jahr in den Sommerferien? Ich hoffe, Sie konnten sie geniessen und sind gut erholt in Ihren beruflichen Alltag zurückgekehrt. Leider soll es vorkommen, dass ein grosser Teil der Erholung bereits beim Checken der eingegangenen E-Mails wieder verfliegt… So geschehen kürzlich in einem Ärztezentrum in der Ostschweiz: Die Mitarbeitenden hatten eine E-Mail erhalten, in der (vermeintlich) die IT-Abteilung sie aufforderte, ein dringendes Update herunterzuladen. Mehrere Angestellte taten dies an ihrem ersten Arbeitstag nach den Ferien pflichtbewusst – und installierten mit dem angeblichen Update einen Computervirus auf ihrem Gerät.

Zum Glück war das Virus in diesem Fall nicht echt. Es gehörte zu einem Test, den das Ärztezentrum zusammen mit HIN durchgeführt hat, um herauszufinden, wie sensibilisiert die Mitarbeitenden gegenüber dem Thema Cyberkriminalität sind. Die gute Nachricht: Die meisten Mitarbeitenden haben sich richtig verhalten. Sie wurden stutzig und haben beispielsweise telefonisch bei der IT-Abteilung nachgefragt. Die schlechte Nachricht: Leider genügt ein falscher Klick als Einfallstor, um ganze Netzwerke den Hackern auszuliefern. Und die Gefahr, dass es sich beim nächsten Mal nicht um einen harmlosen Test, sondern um einen echten Angriff handeln wird, ist real.

Die Tricks der Cyberkriminellen sind heute ziemlich ausgefeilt, denn diese agieren gut organisiert und gewerbsmässig. In der hinter uns liegenden Feriensaison war beispielsweise eine Masche hoch im Kurs, die sich «CEO-Betrug» nennt. Dabei versuchen die Angreifer, eine angeblich dringende Zahlungsaufforderung vom Chef in ein Unternehmen einzuschleusen. Zeiten mit vielen Abwesenheiten und folglich mit leichter täuschbaren Stellvertretungen sind dafür besonders erfolgversprechend.

Ebenfalls erfolgversprechend – aus Hacker-Sicht – sind Situationen, in denen das Gegenüber eine Kontaktaufnahme erwartet. So werden Sie als Praxisinhaberin oder -inhaber bei einer E-Mail mit ZIP-Datei im Anhang kaum Verdacht schöpfen, wenn es sich dabei vermeintlich um eine Bewerbung auf Ihre offene MPA-Stelle handelt. In diesem Fall rechnen Sie ja mit einem Anhang mit den Bewerbungsunterlagen. Sie können es kaum erwarten, die ZIP-Datei zu öffnen – und erleben dabei vielleicht ein blaues Wunder. Bei einem Grossteil der Schweizer Praxen und Heime, die in den letzten Monaten Opfer von Cyberattacken geworden sind, war genau dies der Angriffsweg. Denn gerade Stelleninserate enthalten viele Informationen, welche Kriminelle für ihre Zwecke nutzen können.

Auf professionelle Betrüger hereinzufallen ist keine Schande. Umso wichtiger ist aber, dass das Thema Cyberkriminalität in der Praxis offen angesprochen und auch das richtige Verhalten trainiert wird. Gesundes Misstrauen ist ein wertvolles Potenzial, das es zu pflegen gilt. Als Menschen sind wir nämlich nicht, wie oft behauptet wird, das «schwächste Glied in der Kette», sondern vielmehr die wichtigste Ressource, um einen Angriff zu unterbinden. Wenn der Spamfilter versagt, die Firewall ausgefallen ist und das Antivirusprogramm nicht anschlägt, macht der Mensch vor dem Bildschirm den Unterschied.

Die Tricks der Cyberkriminellen sind heute ziemlich ausgefeilt. Sie agieren gut organisiert und gewerbsmässig.

Und dieser Unterschied ist enorm wichtig. Denn das Gesundheitswesen – mit seinen in kleinen Einheiten organisierten Akteuren, den vielen Schnittstellen und den grossen Mengen an sensiblen Daten – ist für Hacker besonders attraktiv. Wie Sie den vielfältigen Herausforderungen begegnen können, dazu werde ich Ihnen an dieser Stelle regelmässig Tipps geben. Auf jeden Fall ans Herz legen kann ich Ihnen, das Bewusstsein (oder neudeutsch die «Awareness») aller Mitarbeitenden zu schulen. Haben Sie das Thema der nächsten internen Weiterbildung schon festgelegt?

Letztlich muss es nicht Ihr Ziel sein, «alles» richtig zu machen, sondern überhaupt dem Thema die nötige Priorität zu geben. Alles ist besser als nichts tun. Ihre Patientinnen und Patienten haben es verdient (und ein Recht darauf – dazu ein andermal mehr). Denn gestohlene Patientendaten liessen sich allenfalls nach einem Angriff aus einem Backup wiederherstellen. Das Vertrauen in Sie dagegen wäre unwiederbringlich verloren.

Lucas Schult
CEO der Health Info Net AG (HIN). An dieser Stelle schreibt er regelmässig über digitale Sicherheit.