# Cyberangriffe im Gesundheitswesen sind eine Realität

**Rosmarie Borle Oussama Zgheb** Die Digitalisierung durchdringt die verschiedensten Lebens- und Arbeitsbereiche immer mehr. Damit nehmen auch Risiken und Bedrohungen zu – gerade im Gesundheitswesen. Die Kommunikation durch Verschlüsselung zu schützen, ist wichtiger denn je, genügt aber nicht mehr. Im Interview erklärt der IT-Sicherheitsexperte der Health Info Net AG (HIN), weshalb die Sensibilisierung und Befähigung der Gesundheitsfachpersonen (die Awareness) eine immer wichtigere Rolle spielt.

**Oussama Zgheb**
Leiter Engineering & Security, Health Info Net AG (HIN)
Oussama Zgheb ist bei HIN als Security Officer für die Förderung und Kontrolle der Informationssicherheit zuständig. Er ist verantwortlich für die Führung von Entwicklungsressourcen und die Koordination von Entwicklungsprojekten.

Eine Ergotherapeutin betritt am Morgen ihre Praxis. Ein Morgen wie jeder andere – könnte man meinen. Doch als sie versucht, den Computer zu starten, geht nichts mehr. Die Daten wurden über Nacht durch einen sogenannten Krypto-Trojaner verschlüsselt – eine Schadsoftware, die sämtliche Dateien auf dem Computer für das Opfer unbrauchbar macht. Die Ergotherapeutin hat nicht einmal mehr Zugriff auf Termine und Kontaktangaben der Patienten. Stattdessen wird ihr ein «Sperrbildschirm» angezeigt, der sie auffordert, eine bestimmte Summe in Form von Bitcoins an die Angreifer zu bezahlen, damit die Dateien wieder entschlüsselt werden. Ob sie sich nun von den Hackern erpressen lässt oder nicht: Die Kontrolle über ihre Dateien hat sie verloren; die Daten sind möglicherweise für immer weg – oder liegen längst auf dubiosen Servern im Internet. Diese Geschichte ist fiktiv. Das zugrundeliegende Bedrohungsszenario ist jedoch sehr real. In den letzten Monaten schafften es mehrere Fälle in die Medien, in denen ganze Spitäler von Krypto-Trojanern lahmgelegt wurden. Dass die sensiblen Daten des Gesundheitswesens ein beliebtes Ziel von Hackern sind, erstaunt kaum.

**Was für Folgen könnte ein Fall wie der beschriebene für eine Ergotherapeutin haben?**
**Oussama Zgheb:** Die unmittelbare Folge wäre sicher ein Chaos in der Praxis, wenn die Terminplanung und die elektronische Patientenkartei plötzlich nicht mehr verfügbar sind. Viel schwerwiegender wären jedoch die langfristigen Folgen. Durch einen Hackerangriff können sensible Daten in falsche Hände geraten oder gar für jeden öffentlich einsehbar sein. Stellen Sie sich den Vertrauensverlust seitens der Patienten oder der überweisenden Ärzte vor. Diese erhalten den Eindruck, dass mit ihren Daten unsorgfältig umgegangen wird – ein Super-GAU für die Praxis und die dort beschäftigten ErgotherapeutInnen.

**Was kann man unternehmen, um sich gegen Bedrohungen aus dem Internet zu schützen?**
Die Gefahren, welche die Digitalisierung mit sich bringt, sind vielseitig. Entsprechend vielseitig sind auch die möglichen Schutzmassnahmen. Diese lassen sich in drei Kategorien einteilen: technische, organisatorische und verhaltensbezogene Schutzmassnahmen. Ich sage Ihnen ganz offen: Einen hundertprozentigen Schutz gibt es nicht. Wichtig ist aber, das Schutzniveau so hoch zu halten, dass sich die Mühe eines Angriffs für einen Hacker nicht lohnt. Der Mensch folgt dem physikalischen Gesetz vom «Weg des geringsten Widerstands», so auch ein Angreifer. Daher können Sie schon mit verhältnismässig wenig Aufwand Ihren Schutz signifikant erhöhen.

«Einen hundertprozentigen Schutz gibt es nicht.»

**Wäre das Antiviren-Programm auf meinem Computer so eine technische Massnahme?**
Genau, zu den technischen Schutzmassnahmen gehören ein Virenscanner oder auch eine Firewall. Diese beiden Massnahmen sind ohne grossen Aufwand umzusetzen und verbessern den Schutz Ihrer Geräte massiv. Auch empfiehlt es sich, Updates immer umgehend – am besten automatisch – zu installieren, damit Sicherheitslücken sofort geschlossen werden. Wer nicht besonders IT-affin ist oder sich lieber auf sein Kerngeschäft fokussieren möchte, kann den technischen Geräteschutz auch an einen darauf spezialisierten Partner delegieren. Wir nennen unsere Dienstleistung in diesem Bereich «Endpoint Security Service». Dieser beinhaltet moderne Schutzsoftware

für Arbeitsgeräte und die Anbindung an das HIN Security Operation Center. Im Ernstfall helfen einem dann Sicherheitsexperten dabei, Arbeitsgeräte von Schadsoftware zu befreien.

**Was muss ich mir unter organisatorischen Massnahmen vorstellen?**
Technische Massnahmen allein reichen nicht aus. Der beste und teuerste Virenscanner nützt nichts, wenn die Personen, die mit dem Gerät arbeiten, die Grundregeln der IT-Sicherheit nicht beherrschen. Da kommen organisatorische Massnahmen ins Spiel. Dazu gehören Vorgaben, beispielsweise zum Umgang mit personenbezogenen Daten. Ebenso eingespielte Prozesse, beispielsweise regelmässige Backups – hat man eine vollständige Kopie seiner Daten an einem sicheren Ort gespeichert, ist man weniger leicht erpressbar. Über alldem steht die Ausbildung der Mitarbeitenden. Diese müssen regelmässig geschult werden, damit sie die Risiken kennen und sich ein sicherheitsbewusstes Verhalten zu eigen machen – eben beispielsweise einen verdächtigen E-Mail-Anhang nicht leichtfertig öffnen. Wir nennen das neudeutsch «Awareness». HIN führt diesen Herbst zusammen mit dem EVS eine solche Weiterbildung durch. Für die regelmässige Auffrischung der Kenntnisse haben wir ein E-Learning-Tool entwickelt. Ich möchte an dieser Stelle festhalten, dass Informationssicherheit Chefsache ist. Organisatorische Massnahmen sollten «von oben» initiiert, getragen und durchgesetzt werden.

«Der beste Virenscanner ist nutzlos, wenn die Awareness der Mitarbeitenden fehlt.»

**HIN EVS ABO: DIE VERGÜNSTIGTE VERBANDSLÖSUNG**
Ergotherapeutinnen und Eregotherapeuten stehen häufig mit Hausärzten, Spitälern und Krankenversicherungen in Kontakt. Der HIN Anschluss macht den Austausch von elektronischen Informationen bei der interdisziplinären Zusammenarbeit einfach, sicher und datenschutzkonform. Zudem sichert er den Zugriff auf das elektronische Patientendossier. Als EVS-Mitglied erhalten Sie den HIN Anschluss zu vergünstigten Konditionen. Das exklusive HIN-EVS-Abo ermöglicht Ihnen die sichere elektronische Kommunikation mit allen Leistungserbringern und Patienten in Übereinstimmung mit den gesetzlichen Vorgaben.
Informationen und Anmeldung: www.hin.ch/evs

**Sie haben auch von verhaltensbezogenen Massnahmen gesprochen. Was ist darunter zu verstehen?**
Die verhaltensbezogenen Massnahmen bilden neben Technik und Organisation die dritte Säule der IT-Sicherheit. Diese sollte man nicht vernachlässigen. Ich gebe Ihnen ein Beispiel: Die gesamten technischen und organisatorischen Sicherheitsvorkehrungen können ausgehebelt werden, wenn das gewählte Passwort leicht zu erraten ist – oder wenn es auf einem Post-it-Zettel neben dem Computer klebt… Zu den wichtigsten Verhaltensregeln gehört also, dass man sichere Passwörter wählt und diese geheim hält. Eine weitere wichtige Massnahme ist die strikte Trennung von privaten und geschäftlichen Daten. Das heisst, man sollte die geschäftliche E-Mail-Adresse nicht für private Zwecke – beispielsweise als Login für seine Social-Media-Accounts – verwenden.

«Ein seriöser Anbieter wird nie per E-Mail oder Telefon nach dem Passwort fragen.»

**Was macht ein sicheres Passwort aus?**
Ein sicheres Passwort ist komplex und sollte aus mindestens zehn bis zwölf Zeichen bestehen – Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. Zudem darf es keinen Bezug zu Personen haben, also keine Geburtsdaten, Autokennzeichen oder Telefonnummern als Passwort benutzen. Es ist wichtig, dass Sie für jeden Zugang ein anderes Passwort verwenden. Wird beispielsweise Ihr E-Mail-Konto geknackt, ist es für einen Hacker ein Leichtes, auch an Ihr E-Banking-Login zu kommen, wenn Sie dort dasselbe Passwort haben. Nutzen Sie ausserdem, wo immer diese zur Verfügung steht, die sogenannte Zwei-Faktor-Authentisierung. Dabei haben Sie neben dem Passwort noch eine zweite Login-Komponente, beispielsweise einen SMS-Code. So kann ein Hacker nicht auf den jeweiligen Dienst zugreifen, selbst wenn er das benötigte Passwort geknackt hat. Die Zwei-Faktor-Authentisierung ist im Gesundheitswesen state-of-the-art. Aber auch im privaten Gebrauch macht es durchaus Sinn, sie zu verwenden.

**Haben Sie weitere Verhaltenstipps, die Ergotherapeutinnen einfach umsetzen können?**
Auch wenn das hart klingt: Seien Sie misstrauisch! Wir alle tendieren dazu, einem Gegenüber von vornherein einmal keine böse Absicht zu unterstellen. Das gilt auch für den digitalen Raum. Ein solcher Vertrauensbonus kann aber schwerwiegende Folgen nach sich ziehen, denn Internetkriminelle nutzen Gutgläu-

bigkeit und Unachtsamkeit gezielt und gnadenlos aus. Vielmehr gilt es, sich eine grundsätzlich kritische und wachsame Haltung anzueignen. Insbesondere bei E-Mails von unbekannten Absendern ist erhöhte Aufmerksamkeit geboten. Sogenannte Phishing-Attacken, bei denen Betrüger versuchen, an vertrauliche Daten ahnungsloser Internetnutzer zu kommen, sind oft so aufgebaut, dass sie beim Empfänger Angst auslösen oder Druck auf ihn ausüben. In so einer Situation muss man dem Drang zu einer emotional gesteuerten Reaktion widerstehen können und kühlen Kopf bewahren. Alle Alarmglocken sollten läuten, wenn man nach Benutzername und Passwort gefragt wird. Seriöse Anbieter fragen nie per E-Mail oder Telefon nach den Login-Daten eines Nutzers.

### WEITERBILDUNG HIN/EVS IN IT-SICHERHEIT & AWARENESS

Nicht nur Spitäler und Heime, sondern auch therapeutische Praxen und andere Gesundheitsfacheinrichtungen sind bevorzugte Ziele von Internetkriminellen. Hacker-Attacken mit gravierenden Folgen wie Datenverlust, Verletzung des Patientengeheimnisses oder finanziellen Schaden treten immer häufiger auf. In der Weiterbildung lernen Sie wichtige Sicherheitsmassnahmen und Werkzeuge kennen, um sich optimal vor den Gefahren aus dem Internet zu schützen.
Datum und Ort: 14. September 2019, 09.00–11.30 Uhr, Zürich. Kursausschreibung siehe Seite 45.
Infos und Anmeldung: www.ergotherapie.ch

## BERUFSPOLITIK

### Ergogipfel 2019 Interprofessionalität

**Ein ganzer Tag wurde dem Thema Interprofessionalität gewidmet. Dank vielseitigen, interessanten Referaten wurde mir klar, dass Interprofessionalität noch viel mehr beinhaltet als mir bewusst war. Viele mögen glauben, dass sie bereits jetzt interprofessionell unterwegs sind. Unter Umständen täuscht man sich.**

Rita Mühlebach

Interprofessionalität findet auf ganz vielen Ebenen statt. Es umfasst mehr als eine Haltung und eine Arbeitsweise direkt in Bezug zu Patienten. Vielmehr umfasst es sämtliche Bereiche und Abläufe im ganzen Gesundheitswesen.
Was Zusammenarbeit zwischen Berufsverbänden heissen kann, stellten wir zu zweit mit einem Kurzreferat vor. Herr Dr. med. Jürg Zollikofer, Präsident der SGV (Schweizerischer Verband für Vertrauens- und Versicherungsärzte) und ich stellten unser gemeinsam erarbeitetes Produkt, den Berichteraster vor. Neu für Sie ist möglicherweise die Information, dass es sich dabei um ein Zusammenarbeitsprodukt mit dem SGV handelt. Ein Arbeitspapier, das zwei Seiten dienen soll, soll auch gemeinsam entstehen. Diese einfache Botschaft konnten wir mit ein paar Folien glaubhaft darlegen. Den Schlusssatz des kurzen Referates präsentierte ich besonders gerne: «Gute Zusammenarbeit öffnet Türen». Die bewährte Zusammenarbeit zwischen EVS und SGV soll weitergehen. Ein regelmässiger Austausch der Verbände findet statt.

(Die französische Version erscheint in Ergotherapie 7/19)