MIT DIGITALER ACHTSAMKEIT RISIKEN MINIMIEREN

Lucas Schult

Geschäftsführer (CEO) der Health Info Net AG (HIN)

Wenn Praxen die Digitalisierung erfolgreich meistern wollen, müssen die IT-Systeme sicher und sensible Daten geschützt sein. Technische Massnahmen sind wichtig – entscheidend sind achtsame, gut ausgebildete Mitarbeitende.

Lucas Schult

Health Info Net AG
Tel. 0848 830 740
lucas.schult@hin.ch
www.hin.ch

Wir alle nutzen täglich vernetzte digitale Systeme. Sei es im Berufs- oder im Privatleben, sei es bewusst oder unbewusst. Dass diese Systeme vor unrechtmässigen Zugriffen und Missbrauch geschützt werden müssen, steht ausser Frage. Oft denkt man dabei einseitig an technische Massnahmen. Wenn es um den Schutz sensibler Daten – wie jene der Patientinnen und Patienten – geht, kann sich jedoch niemand seiner Verantwortung entziehen. Denn «digitale Sorglosigkeit» kann gravierende Konsequenzen haben.

Sicherheit kostet Geld, in der IT ebenso wie überall. Doch auch wenn bei Sicherheitslecks (z. B. Kompromittierung oder Verlust von Patientendaten) zunächst die betroffenen Patienten die Leidtragenden sind, so gilt es doch auch die Folgen für die Praxis selbst zu vergegenwärtigen. Ein irreparabler Reputationsschaden kann dabei langfristig gravierender sein als direkte Schadenersatzansprüche.

Digitalisierung als Chance begreifen

Die Schuld für Mehraufwände in Sachen Datensicherheit bei der Digitalisierung selbst zu suchen, wäre falsch. Bringt doch gerade diese oft erst bestimmte Sicherheitsprobleme in Organisationen ans Licht. Digitalisierung ist – sofern PraxisinhaberInnen die IT-Sicherheit ganzheitlich angehen – eine Chance, um die ganze Praxis sicherer zu machen. Denn clevere digitale Lösungen können die Schwachstellen analoger Prozesse teilweise beheben.

Korrekt verschlüsselte E-Mails beispielsweise sind schneller und sicherer als Faxen. Digitale Sicherheitskopien anzufertigen, ist einfacher und effizienter als das Kopieren von analogen Dokumenten. Auch können digitale Systeme die Anzahl und Art der Zugriffe auf eine Datei fälschungssicher protokollieren, während dies bei Papierakten so nicht möglich ist. Sicherheit steht also nicht per se im Gegensatz zu Effizienz und Einfachheit, sondern kann mit diesen einher gehen.

Gesundheitsfachpersonen befähigen

Neben den Systemen müssen vor allem die Mitarbeitenden als sicherheitsrelevanter Faktor im Fokus stehen. Mitarbeitende, die – auch unbewusst – vertrauliche Informationen von sich, von Kunden oder aus dem Unternehmen preisgeben, sind für Cyberkriminelle zentraler Ansatzpunkt für Datendiebstahl, Industriespionage oder digitale Erpressung. Das Gesundheitswesen mit seinen sensiblen Daten, den vielen Austauschprozessen und den immer häufiger zeit- und ortsunabhängig zusammenarbeitenden Fachpersonen ist hier verletzlicher als andere Branchen.

Vorgesetzte, aber auch die Mitarbeitenden, können dazu beitragen, diese Risiken zu minimieren. Technische Massnahmen wie ein Antivirenprogramm sind dabei nur eine von drei Säulen der IT-Sicherheit. Ebenso wichtig sind organisatorische und verhaltensbezogene Massnahmen in den Praxen. Diese reichen von der Wahl sicherer (langer, komplexer) Passwörter über die Nutzung der E-Mail-Verschlüsselung (z. B. HIN E-Mail) bis hin zu klaren Vorgaben zum Umgang mit Daten. Doch der eigentliche Knackpunkt ist die Achtsamkeit der Mitarbeitenden im Arbeitsalltag.

Fehlende digitale Instinkte

Die Digitalisierung ist in der Menschheitsgeschichte ein ziemlich junges Phänomen. Anders als zum Beispiel im Umgang mit heissen Herdplatten und spitzen Gegenständen haben wir im Umgang mit digitalen Systemen weder ein angeborenes noch ein von Kindsbeinen an erworbenes Risikoempfinden. Dazu trägt bei, dass wir die Gefahren von digitalen Technologien häufig nicht direkt wahrnehmen können, da sich die Konsequenzen von Datenmissbrauch oft erst langfristig äussern.

Durch die Digitalisierung sind «neue Bedrohungslagen hinzugekommen, auf welche wir noch nicht instinktiv reagieren können». Dem kann man nur begegnen, indem entsprechende Kompetenzen bei den Mitarbeitenden kontinuierlich aufgebaut werden. Da in den meisten Ausbildungslehrgängen bisher das Thema IT-Sicherheit kaum vorkommt, bleibt einstweilen nur die betriebliche Weiterbildung.

Der Schlüssel: Security Awareness

In einem ersten Schritt müssen die Mitarbeitenden verinnerlichen, dass ihr Verhalten direkt sicherheitsrelevant ist. Während dies für medizinisches Personal in anderen Themenbereichen (etwa im Bereich Hygiene) mehr oder weniger selbstverständlich ist, muss beim Thema Praxis-IT dieses Bewusstsein – die sogenannte Security Awareness – erst noch geschaffen werden. In vielen IT-Schulungen wird zwar der Security-Aspekt angesprochen, aber kaum jener der Awareness. Erst die Verknüpfung von Security und Awareness befähigt die Mitarbeitenden jedoch tatsächlich, ihre Verantwortung wahrzunehmen.

Denn IT-Sicherheit erschöpft sich nicht darin, zu vermitteln, wie Mitarbeitende Spam-E-Mails identifizieren oder einen Anhang auf Malware überprüfen können. Mitarbeitende müssen vielmehr verstehen, warum bestimmte Regeln gelten. Sie müssen deren Vorteile für sich und die Praxis erkennen. Nicht zuletzt müssen sie gewillt sein, die Sicherheitsmassnahmen mitzutragen und IT-Sicherheit im Alltag zu leben. Jede in der Praxis

geltende Regel braucht somit eine nachvollziehbare Erklärung.

Heikle Themen und Win-win

Anwender sind zwar keine Experten, aber durchaus lernbereit, wenn sie die Zusammenhänge kennen und verstehen. Ein wichtiges Thema, das angesprochen werden muss, ist die Unzulänglichkeit der Technik. Schliesslich müssen die Mitarbeitenden dort in die Bresche springen, wo diese versagt. Doch wäre Angstmacherei verfehlt, eher sollte der Nutzen herausgestellt werden. Viele der essenziellen Regeln und Techniken – zum Beispiel die Nutzung eines Passwort-Safes – lassen sich auch im privaten Umfeld sinnvoll einsetzen. Mitarbeitende und Praxen können so von Schulungen doppelt profitieren, denn positive Erfahrungen der Mitarbeitenden im privaten Bereich kommen letztlich auch der Praxis zugute.

Um eine Praxis gemäss dem Prinzip der integralen Sicherheit auf- und umzubauen, ist die Security Awareness der Mitarbeitenden der Schlüssel. Sich «digitale Instinkte» anzutrainieren, geht aber nicht über Nacht. Dafür braucht es regelmässige Schulungen, am besten über das Jahr verteilt in kleinen Lerneinheiten. Solche können beispielsweise mittels E-Learning einfach in den Alltag integriert werden. HIN stellt entsprechende Werkzeuge bereit – es liegt an den Praxisinhaber/innen, sie zu nutzen.

Quellen:

1. «ECSM: Mitarbeiter können zur IT-Sicherheit im Unternehmen beitragen», URL: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2015/ECSM_Mitarbeiter_zu_IT-Sicherheit_in_Unternehmen_beitragen_01102015.html;jsessionid=1B91348789E-ECF078AEE8246BCA82EF5.2_cid369, 01.10.2015, [abgerufen am 31.10.2019].

2. Weber, Stefan G.: «IT-Sicherheit und Nutzer: Chancen und Risiken der Digitalisierung», in: Wittpahl, Volker (Hrsg.): Digitalisierung: Bildung, Technik, Innovation, Berlin 2017, S. 28.

3. Dombach, Ralph / Schmitz, Peter: «Mehr Erfolg mit Security Awareness. Verständnis wecken für IT-Sicherheit», URL: https://www.security-insider.de/verstaendnis-wecken-fuer-it-sicherheit-a-716942/, 15.06.2018 [abgerufen am 31.10.2019].

RÉDUIRE LES RISQUES PAR LA VIGILANCE NUMÉRIQUE

Lucas Schult

Directeur général (CEO) de la société Health Info Net SA (HIN)

Si les cabinets médicaux veulent maîtriser le passage à la numérisation avec succès, les systèmes informatiques doivent être sûrs et les données sensibles bien protégées. Dans ce contexte, les mesures techniques sont importantes, mais il est primordial d'avoir des collaborateurs vigilants et bien formés.

Nous utilisons tous les jours des systèmes numériques interconnectés, que ce soit dans la vie professionnelle ou privée, consciemment ou inconsciemment. Personne ne remettra en question la nécessité de protéger ces systèmes contre l'accès illégal ou les abus. On pense alors d'abord aux mesures techniques. Pourtant, lorsqu'il s'agit de protéger des données sensibles comme celles des patients, personne ne peut échapper à ses responsabilités, car l'«insouciance numérique» peut avoir de graves conséquences.

La sécurité coûte de l'argent, dans l'informatique et partout ailleurs. Même si en cas de brèches de sécurité (p. ex. compromission ou perte de données de patients), ce sont en premier lieu les patients qui en sont les victimes, il s'agit tout de même de prendre conscience des conséquences que cela implique pour le cabinet médical. En effet, une atteinte irréparable à la réputation peut à long terme être bien plus grave que des prétentions directes en dommages-intérêts

Considérer la numérisation comme une opportunité

Rendre la numérisation responsable des coûts supplémentaires qu'elle engendre en matière de sécurité des données est faux, car c'est souvent précisément elle qui met en évidence certains problèmes de sécurité. Pour autant que les propriétaires de cabinet adoptent une approche globale pour la sécurité informatique, la numérisation est une opportunité pour renforcer la sécurité du cabinet médical dans son ensemble. Des solutions numériques intelligentes sont capables d'éliminer partiellement les points faibles de processus analogiques.

L'envoi d'e-mails cryptés est par exemple plus sûr et plus rapide que l'envoi de documents par fax. Il est également bien plus simple de produire des copies de sécurité numériques que de copier des documents analogiques. De plus, les systèmes numériques sont en mesure de journaliser le nombre et le type des accès à un fichier, alors que cela n'est pas possible avec des dossiers sur papier. La sécurité ne s'oppose donc pas en soi à l'efficacité et à la simplicité, mais peut aller de pair avec celles-ci.

Responsabiliser les professionnels de la santé

Parmi les facteurs pertinents en matière de sécurité ne figurent pas que les systèmes, mais aussi, et surtout, les collaborateurs. Les collaborateurs qui divulguent des informations personnelles sur eux-mêmes, sur les clients ou sur l'entreprise, même s'ils le font inconsciemment, représentent une cible facile pour les cybercriminels et constituent donc le point de départ pour le vol de données, l'espionnage industriel ou le chantage numérique. Avec ses données sensibles, ses nombreux processus d'échange et les professionnels collaborant toujours plus indépendamment du temps et du lieu, le système de santé est plus vulnérable que d'autres branches.

Les supérieurs hiérarchiques tout comme les collaborateurs peuvent contribuer à réduire ces risques. Dans ce contexte, les mesures techniques, comme p. ex. un logiciel antivirus, ne sont qu'un des piliers de la sécurité informatique. Les mesures organisationnelles et comportementales dans les cabinets médicaux sont tout aussi importantes. Celles-ci vont du choix de mots de passe sûrs (longs, complexes) jusqu'à des prescriptions claires sur la manière de gérer les données, en passant par l'utilisation d'un cryptage des e-mails (p. ex. e-mail HIN). Pourtant, c'est la vigilance des collaborateurs qui représente le véritable défi.

Instincts numériques insuffisants

Le phénomène de la numérisation est relativement récent dans l'histoire de l'humanité. Contrairement à la manière d'utiliser des plaques de cuisson et des objets pointus, notre manière d'aborder les systèmes numériques ne peut s'appuyer sur aucune capacité de perception des risques innée ou acquise dès l'enfance. A cela vient s'ajouter que nous ne sommes souvent pas capables de percevoir directement les dangers émanant des technologies numériques compte tenu du fait que les conséquences d'un abus de données ne deviennent généralement visibles qu'à long terme.

De nouvelles menaces sont venues s'ajouter avec la numérisation et nous ne pouvons pas encore y réagir de manière instinctive. Or, on ne peut répondre à ces menaces qu'en renforçant continuellement les compétences en la matière des collaborateurs. Mais comme la plupart des formations n'abordent jusqu'ici pour ainsi dire pas le thème de la sécurité informatique, la formation interne à l'entreprise reste pour le moment la seule option.

La clé: sensibilisation à la sécurité

Les collaborateurs doivent en premier lieu réaliser que leur comportement est important pour la sécurité. Alors que dans d'autres domaines (p. ex. l'hygiène), le personnel médical est conscient de l'importance de son comportement, cette prise de conscience de l'importance de la sécurité doit encore avoir lieu dans le domaine de l'informatique du cabinet médical. L'aspect de la sécurité est abordé dans la plupart des formations informatiques. C'est par contre moins le cas pour ce qui concerne la sensibilisation. Finalement, c'est le lien entre sécurité et sensibilisation qui permet aux collaborateurs d'effectivement assumer leur responsabilité, car la sécurité informatique ne se limite pas à enseigner aux collaborateurs comment identifier des spams ou vérifier que la pièce jointe ne contient pas de maliciel. Les collaborateurs doivent avant tout comprendre pourquoi certaines règles s'appliquent. Ils doivent comprendre leurs avantages pour eux-mêmes et la pratique. Finalement, ils doivent être désireux d'appuyer les mesures de sécurité et de mettre en pratique au quotidien la sécurité informatique. Chaque règle applicable dans le cabinet médical doit donc être accompagnée d'une explication claire.

Sujets délicats

Les utilisateurs ne sont peut-être pas des experts, mais ils sont assurément disposés à apprendre s'ils comprennent les tenants et aboutissants. Un sujet important qui doit être abordé est l'insuffisance de la technique. En effet, les collaborateurs doivent sauter dans la brèche là où cette dernière est défaillante. Il ne s'agit cependant pas de peindre le diable sur la muraille, mais plutôt de souligner les avantages. Beaucoup des règles et techniques essentielles, comme p. ex. l'utilisation d'un gestionnaire de mots de passe, peuvent aussi être utiles dans le domaine privé. Les collaborateurs et les cabinets médicaux peuvent ainsi doublement profiter des formations, car les expériences positives acquises par les collaborateurs dans le domaine privé sont finalement tout à l'avantage du cabinet médical.

La sensibilisation à la sécurité des collaborateurs est un élément clé pour établir et transformer un cabinet selon le principe de la sécurité intégrale. Evidemment, ce n'est pas du jour au lendemain que l'on peut acquérir les «instincts numériques». Pour cela, il faut des formations régulières, si possible réparties en petites unités sur toute l'année. Cela permet d'intégrer des contenus au quotidien par le biais de l'apprentissage en ligne. HIN met à disposition les outils correspondants. Il est de la responsabilité des propriétaires de cabinet de les utiliser.

Sources:

1. «ECSM: Mitarbeiter können zur IT-Sicherheit im Unternehmen beitragen», URL: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2015/ECSM_Mitarbeiter_zu_IT-Sicherheit_in_Unternehmen_beitragen_01102015.html;jsessionid=1B91348789E-ECF078AEE8246BCA82EF5.2_cid369, 01.10.2015, [abgerufen am 31.10.2019].

2. Weber, Stefan G.: «IT-Sicherheit und Nutzer: Chancen und Risiken der Digitalisierung», in: Wittpahl, Volker (Hrsg.): Digitalisierung: Bildung, Technik, Innovation, Berlin 2017, S. 28.

3. Dombach, Ralph / Schmitz, Peter: «Mehr Erfolg mit Security Awareness. Verständnis wecken für IT-Sicherheit», URL: https://www.security-insider.de/verstaendnis-wecken-fuer-it-sicherheit-a-716942/, 15.06.2018 [abgerufen am 31.10.2019].