Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 23. Mai 2018

Cyberkriminalität: Wie Sie ruhig schlafen können

Die Bedrohungen aus dem Internet werden ausgefeilter, und das Gesundheitswesen kommt verstärkt ins Visier. Patrick Raths von der Health Info Net AG verrät, wie Gesundheitsdaten optimal geschützt werden.

Legende: «Erpressungsversuche werden in Zukunft vermehrt gezielt auf Institutionen ausgeübt werden»

Herr Raths, immer wieder hört man das Wort «Cyberkriminalität». Darunter versteht man Straftaten, für die zur Ausübung moderne Informationstechniken genutzt werden. Ist die Gefahr wirklich so gross oder wird das Thema aufgeblasen?

Nein, die Gefahr ist ganz klar da. Institutionen im Gesundheitswesen gehören sogar zur sogenannten «kritischen Infrastruktur», da viele Menschen – insbesondere Patienten – von korrekt funktionierenden IT-Systemen abhängig sind. Ein Spital ohne Zugriff auf Daten hat Mühe, den regulären Betrieb aufrecht zu halten. Wir gehen davon aus, dass Erpressungsversuche in Zukunft vermehrt gezielt auf Institutionen ausgeübt werden. Besonders auf solche, die stark von digitalen Daten abhängig sind. Das erhöht die IT-Risiken im Gesundheitswesen und bedingt eine Verstärkung der Sicherheitsmassnahmen.

Welche konkreten Gefahren gehen denn von einem Cyberkriminellen aus?

Inzwischen gibt es eine ganze Industrie von Cyberkriminellen, die in rasantem Tempo neue Variationen und Varianten von Schadsoftware entwickeln. Die Gefahr, von Viren, Trojanern oder Würmern infiziert zu werden, ist heute fast unausweichlich. Diese können zu Datendiebstahl- und Manipulation, zu Finanzbetrug oder sogar zu Erpressungen führen. Ein wesentlicher Teil der Sicherheitsrisiken für die moderne IT folgt aber aus dem fehlenden Bewusstsein, aus Bequemlichkeit und der Gutgläubigkeit der Menschen. Das fängt damit an, dass man Patientendaten nicht einfach weitergibt und endet mit der gedankenlosen Angabe eines Passwortes am Telefon. Die Informationssicherheit wird so sehr häufig durch die Unachtsamkeit von Menschen bedroht. Deshalb hat die Awareness von Gesundheitsfachpersonen oberste Priorität, um Cyber-Attacken bestmöglich zu verhindern.

Sie haben es bereits angesprochen: Wie kann ich mich am besten vor Cyber-Attacken schützen?

Das wichtigste ist die Awareness ... ein Bewusstsein für die existierenden Risiken. Das ist die Basis für alle weiteren technischen und organisatorischen Schutzmassnahmen. Durch eine gezielte Sensibilisierung und Schu-

lung gerade der Gesundheitsfachpersonen, kann der Datenschutz und die Sicherheit auch in der digitalen Welt massiv erhöht werden.

Ein Rezept das immer hilft: Kritisch sein. Misstrauen in Bezug auf Cybercrime ist wichtig. Man soll sich immer zweimal überlegen, ob zum Beispiel ein Anhang geöffnet werden soll oder ob die E-Mail wirklich von einem bekannten Empfänger stammt. Dasselbe gilt natürlich auch für Social-Engineering-Attacken am Telefon. Weiter ist es wichtig, die Geräte und die Software auf dem neusten Stand zu halten, das heisst Updates regelmässig durchführen und insbesondere Security-Patches installieren.

Leider fällt mir immer wieder auf, das vor allem Arztpraxen wenig Zeit für das komplexe Thema der IT aufwenden oder aufwenden können. Das Thema ist jedoch sehr wichtig. Daher bietet HIN einen neuen, einzigartigen Service an. Mit dem HIN Endpoint Security Service schützen Sie Arbeitsgeräte umfassend vor Bedrohungen aus dem Internet. Im Ernstfall werden Sie von erfahrenen Sicherheitsexperten proaktiv bereut.

Gibt es noch weitere Tipps und Tricks für einen umfassenden Schutz?

Ich empfehle immer eine ausgewogene Mischung von verschiedenen Massnahmen, technischer aber auch organisatorischer Art. Eine der wichtigsten Regeln vorweg: in E-Mails nur Links anklicken, die bekannt oder vertrauenswürdig sind.

Weitere Massnahmen sind:

- Seien Sie vorsichtig bei verdächtigen E-Mails, selbst wenn diese von Ihnen bekannten Absendern stammen. Leider können Absenderadressen sehr einfach gefälscht werden.
- Löschen Sie verdächtige Nachrichten umgehend, ohne angefügte Dateien im Anhang zu öffnen. Löschen Sie die Nachrichten auch im Papierkorb Ihrer E-Mail Ablage.
- Verwenden Sie für jede Applikation ein anderes Passwort. Dabei sind acht bis zehn Stellen das Minimum.
- Halten Sie Ihr System immer auf dem neuesten Stand (Browser, E-Mail-Programm, Virenschutzprogramm, Betriebssystem, Office et cetera). Installieren Sie Updates umgehend, insbesondere, wenn es sich um Sicherheitsupdates handelt. Firewall und Virenscanner sind ein Muss.
- Versenden Sie sensible Daten per Mail nur verschlüsselt. Die meisten Spitäler und Arztpraxen in der Schweiz sind bereits an HIN angeschlossen. Steht im Betreff der E-Mail [HIN secured] wurde die E-Mail via HIN verschlüsselt versendet und sensible Daten gelangen sicher von A nach B.

Die Health Info Net AG (HIN) bietet zudem – wie erwähnt – verschiedene Services an, die Sie noch besser vor Cyberkriminalität schützen.

Mit dem HIN Awareness Portal schulen Sie sich und alle Ihre MitarbeiterInnen rund um die Informationssicherheit. Der HIN Endpoint Security Service schützt Arbeitsgeräte in einzigartiger Weise.

Hier erhalten sie nähere Informationen.

Patrick Raths ist bei der Health Info Net AG (HIN) als System Engineer & 2nd Level Supporter für die technische Unterstützung der Kunden verantwortlich. Nebst einer Ausbildung als Konstrukteur studierte er Informatik und verfügt über eine mehrjährige Berufserfahrung in der IT-Branche.