Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 28. September 2017

„Cyber-Sicherheit scheitert oft am Gerät der Gesundheitsfachperson“

Cybercrime-Attacken im Gesundheitswesen gefährden Leben. Deshalb ist es wichtig, nicht nur gute Tools zu haben oder gut ausgebildet zu sein, sondern auch das eigene Gerät umfassend zu schützen. Lucas Schult, IT-Experte im Gesundheitswesen, erzählt von einer Lösung, die ganzheitlichen Schutz vor Bedrohungen aus dem Internet bietet.

Legende: Lucas Schult: „Das Zusammenspiel von Awareness, guten Tools und eigens dazu eingesetzten Spezialisten führt zu einem umfassenden Schutz vor Cybercrime.“

Herr Schult, fast täglich wird das Gesundheitswesen in irgendeiner Art bedroht. Was denken Sie ist die grösste Gefahr für zum Beispiel Spitäler und Praxen in Bezug auf Cybercrime?

Aus meiner Sicht ist die grösste Gefahr, dass bei Cyber-Angriffen wichtige Gesundheitsdaten nicht mehr zur Verfügung stehen. Ich denke hier konkret an die vergangenen WannaCry-Attacken, weswegen Personen nicht operiert werden konnten und so deren Leben gefährdet waren. Eine weitere Gefahr ist sicher auch, dass Daten gestohlen und somit schützenswerte Informationen für nicht Berechtigte zugänglich werden.

Um diese Bedrohungen zu minimieren, werden heute Awareness-Schulungen oder verschiedene Tools wie beispielsweise Virenscanner empfohlen. Reicht die Anwendungen dieser Massnahmen aus?

Solche Massnahmen sind gut, vor allem wenn ich an Awarness-Schulungen denke so wie sie HIN anbietet, aber schlussendlich liegt der Erfolg in der richtigen Kombination derselben. Kombiniert man Virenscanner mit einer gut ausgebildeten MPA, kann die Sicherheit erheblich erhöht werden. Beispiel: eine MPA bekommt eine E-Mail mit einem Anhang. Je nach Awareness der MPA weiss sie, dass man nicht jeden Anhang unüberlegt öffnen sollte. Und je nach Qualität des Tools erkennt dieses, ob der Anhang gut- oder bösartig ist. Würde das Tool versagen, könnte die MPA aufgrund Ihrer Awareness-Schulung Schaden verhindern.

Um die Sicherheit noch mehr zu steigern, braucht es zusätzlich eine dritte Komponente: Sicherheitsexperten, die Vorfälle analysieren und Handlungsempfehlungen geben. Sie monitoren Geräte proaktiv im Security Operation Center, reagieren auf Angriffe und alarmieren die Betroffenen. In unserem Beispiel unterstützen sie die MPA zusätzlich mit Handlungsanweisungen und wichtigen Empfehlungen.

Sie haben drei Dinge angesprochen: Awareness, Tools und Experten im Security Operation Center. Diese drei Nenner ergeben also eine optimale Endpoint-Security. Was ist der Nutzen dieser Lösung?

Leider ist es so, dass heute viele Firmen – darunter auch Arztpraxen - viel Geld für Sicherheits-Infrastruktur ausgeben. Dabei wird oft vergessen, den Endpoint, also das Gerät des Arztes oder der MPA, genügend zu schützten. Ist das der Fall, sind die übrigen Investitionen defacto nutzlos, da sämtliche Sicherheitsperimeter durch den unsicheren Endpoint schlicht umgangen werden. Deshalb ist es wichtig, einen starken Fokus auf den Endpoint zu legen. Dies geschieht, indem man die verschiedenen Komponenten (Awareness Schulung, Tools und Security Operation Center) gemeinsam anwendet. Dadurch kann ein umfassender Schutz aufgebaut werden – die Sicherheit im Gesundheitswesen verstärkt sich.

Sie sagen also, kurz zusammengefasst, dass Endpoint Security die Verfügbarkeit, den Datenschutz sowie die Datensicherheit verbessern kann. Das tönt für mich wie eine Art rundum Schutz, eine Art Vollkasko-Versicherung?

Nein, das ist es sicher nicht – Vollkasko bezüglich Sicherheit gibt es nicht, man hat immer einen Selbstbehalt, also ein Restrisiko. Ein Arzt gibt ja auch nie die Garantie, dass seine OP zu hundert Prozent erfolgreich verlaufen wird. Ähnlich wie bei jeder OP etwas schiefgehen kann, gilt das gleiche bei der IT-Security.

Es lohnt sich jedoch auf jeden Fall, den Schutz so hoch wie möglich zu halten. Nichts und niemand ist vollständig vor Cybercrime-Attacken geschützt – je mehr wir aber dagegen machen, desto grösser ist die Möglichkeit, einen Schaden erfolgreich abzuwehren. Mit einer optimalen Endpoint-Security können Risiken für Datenverlust, Betriebsunterbrüche und Verstösse gegen den Datenschutz und Berufsgeheimnisgesetzte deutlich minimiert werden.

HIN hat geplant, in naher Zukunft (Anfang 2018) einen solchen Endpoint-Security Service anzubieten. Wie kann ich mich derweil trotzdem möglichst effizient vor den Gefahren aus dem Internet schützen?

Ein Rezept das immer hilft: Kritisch sein. Misstrauen in Bezug auf Cybercrime ist wichtig! Man soll sich immer zwei Mal überlegen, ob z.B. 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.

Und dann wie gesagt: auf die Awareness der Mitarbeiter achten und entsprechend ausbilden!

Lucas Schult ist als CIO und als Mitglied der Geschäftsleitung für ein zuverlässiges und sicheres Funktionieren sämtlicher Informations-Systeme der HIN verantwortlich. Lucas Schult ist Certified Network Security Engineer (CNSE) und Certified in Risk and Information System Control (CRISC). Er verfügt über langjährige Erfahrung im IT-Bereich.