Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 06. Juli 2017

“In Zukunft müssen wir uns im Gesundheitswesen noch stärker mit den Risiken der Cyberkriminalität beschäftigen”

Cyberkriminalität gefährdet Leben – dies zeigt der weltweite Hacker-Angriff mit der Erpresser-Software «Wanna Cry», die Einrichtungen wie Krankenhäuser und andere Infrastrukturen attackiert und lahmgelegt hat. Über zehntausend Computer waren davon betroffen. Christian Greuter, Geschäftsführer von HIN, nimmt Stellung zu diesem präsenten Thema und beantwortet die wichtigsten Fragen.

Legende: Christian Greuter (CEO von HIN): “Aktuell findet ein Wettrüsten wie im kalten Krieg statt.”

Herr Greuter, mit „Wanna Cry“ ist nun jedem klar, dass Cyberkriminalität auch im Gesundheitswesen angekommen ist. Wie schätzen sie die Situation in der Schweiz konkret ein?

Cyberkriminaliät hat auch früher keinen Halt vor dem Gesundheitswesen gemacht. Die Mehrheit der Angriffe sind nach wie vor nicht gezielt, sondern treffen Institutionen, PC’s und Server zufällig. Auch „Wanna Cry“ war nicht gezielt, hat aber eben auch Spitäler in England getroffen, was in den Medien besonders aufmerksam verfolgt wurde.

Institutionen im Gesundheitswesen gehören 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. Deshalb gehen wir 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.

Die „Wanna Cry"-Attacke hat die Computer der betroffenen Kliniken, Organisationen, Firmen und Behörden mit sogenannten Erpressungstrojanern befallen, die Daten verschlüsseln und Lösegeld verlangen. Auch HIN verschlüsselt Daten...

Da haben Sie recht. Verschlüsselung kann zum Guten und zum Schlechten eingesetzt werden. Die Verschlüsselung von Daten wird hauptsächlich für den Schutz von Daten angewendet, im Speziellen vor nicht berechtigter Einsicht. Leider kann diese Technologie aber auch gegen den Besitzer der Daten angewendet werden. Dritte verschlüsseln persönliche Daten, so dass diese weder les- noch nutzbar sind, um Betroffene damit zu erpressen.

Und übrigens - das gutartige Verschlüsseln von Daten schützt nicht vor einer bösartigen Attacke, denn im schlimmsten Fall werden die Daten einfach nochmals verschlüsselt.

Welche Massnahmen und Verhaltensregeln sind im Zusammenhang mit der Sicherheit im digitalen Raum heute besonders zu beachten?

Das wichtigste ist die Awareness - ein Bewusstsein für die existierenden Risiken. Das ist die Basis für alle Schutzmassnahmen. Weiter ist eine ausgewogene Mischung von verschiedenen Massnahmen zu empfehlen, technischer aber auch organisatorischer Art. Die essentiellen Schutzmassnahmen haben wir auf einem Merkblatt zusammengestellt. Eine der wichtigsten Regeln vorweg: in E-Mails nur Links anklicken, die bekannt oder vertrauenswürdig sind.

Inzwischen gibt es eine ganze Industrie von Cyberkriminellen, die in rasanten Tempo neue Variationen und Varianten an Schadsoftware entwickeln. Dementsprechend müssen auch laufend neue Abwehrmechanismen entwickelt werden - es ist wie eine Art Wettrüsten im kalten Krieg. Beispielsweise für den Schutz vor Verschlüsselungstrojaner gibt es aktuell eine neuartige Software, die auf dem System laufende Verschlüsselungen nach ihrer Gut- oder Bösartigkeit überprüft und so versucht, Daten zu retten. Es wird aber sicher nicht lange dauern, bis auch dieser Schutz entweder auf Grund einer Lücke oder einem noch ausgeklügelteren Verfahren geknackt wird...

Christian Greuter ist als Geschäftsführer der Health Info Net AG (HIN) für die Gesamtkoordination und die Umsetzung der Strategie verantwortlich. Der Informatikingenieur mit Weiterbildung in Business Administration und Verkauf verfügt über langjährige Erfahrung als IT-Experte im Gesundheitswesen.