Interview mit Pierre-François Regamey, Chief Information Officer Universitätsspital Kanton Waadt (CHUV)

«Das Schadenspotential von Cyberattacken ist sehr hoch»

Interview: Bruno Kesseli

Dr. med. et lic. phil., Chefredaktor

Mit der zunehmenden Digitalisierung des Gesundheitswesens steigt das Risiko von Cyberattacken. Als Chief Information Officer des Universitätsspitals Kanton Waadt (CHUV) ist Pierre-François Regamey fast täglich mit Angriffen aus dem Internet konfrontiert. Das nachfolgende Interview entstand anlässlich eines Vortrags, den er zu dieser Thematik im Oktober 2017 vor der Ärztekammer hielt.

Sie haben vor der Ärztekammer über Cyberkriminalität im Spitalbereich gesprochen. Wie akut ist das Problem in Schweizer Spitälern?

Es handelt sich um ein ernsthaftes Problem, weltweit, und somit auch in der Schweiz. Wir sind hier aber im Spitalbereich insofern in einer recht komfortablen Lage, als wir technisch über gute Infrastrukturen verfügen. Wenn man unsere Situation zum Beispiel mit derjenigen der Spitäler in Grossbritannien vergleicht, die im Frühling 2017 durch eine Cyberattacke mit der Ransomware «WannaCry» lahmgelegt wurden, stehen wir gut da.

Pierre-François Regamey bei seinem Referat vor der Ärztekammer im Oktober 2017.

Wieso waren Schweizer Spitäler von diesem Angriff nicht betroffen?

Die Computersysteme der betroffenen britischen Spitäler waren veraltet und wiesen dadurch Sicherheitslücken auf. Es war schlicht nicht genug Geld in die Erneuerung der Systeme investiert worden. In der Schweiz sind bisher die Mittel vorhanden, um die Systeme auf dem neuesten Stand zu halten, was Angreifern das Eindringen erschwert.

Wie häufig ist das CHUV, für das Sie zuständig sind, Attacken ausgesetzt?

Was Cyberattacken betrifft, sind Landesgrenzen inexistent. Deshalb ist das CHUV täglich mit Angriffen konfrontiert, in denen beispielsweise versucht wird, Viren ins System einzuschleusen. Gerade gestern erhielt eine unserer Mitarbeiterinnen eine E-Mail-Nachricht mit einem Anhang, den sie glücklicherweise nicht geöffnet hat. Er enthielt ein extrem gefährliches Virus, das uns vor grösste Probleme gestellt hätte. Solche Vorkommnisse registrieren wir fast täglich.

«Was Cyberattacken betrifft, sind Landesgrenzen inexistent. Deshalb ist das CHUV täglich mit Angriffen konfrontiert, in denen beispielsweise versucht wird, Viren ins System einzuschleusen.»

Sind Spitäler für Cyberkriminelle besonders attraktiv?

In Europa haben Cyberkriminelle bisher nicht speziell die Spitäler im Visier. In den USA ist dies etwas anders, weil es dort viel mehr Privatspitäler gibt und zwei Typen von personenbezogenen Daten für Hacker besonders interessant sind: die Sozialversicherungsnummer, die in den USA in vielen Bereichen als eindeutiges Identifikationsmerkmal einer Person eine zentrale Rolle spielt, und die Kreditkartennummern der «Spitalkunden», also der Patienten. Es gibt in den USA immer wieder Angriffe auf Spitäler, die zum Ziel haben, an diese Informationen heranzukommen.

Zur Person

Seit 2006 leitet Pierre-François Regamey als Chief Information Officer die IT-Abteilung des Universitätsspitals Kanton Waadt (CHUV) mit 170 Angestellten. Zuvor war er in leitenden Stellungen für den IT-Bereich einer grossen Versicherungsgesellschaft verantwortlich sowie im Management verschiedener schweizerischer und internationaler IT-Consulting-Unternehmen mit Kunden aus den Bereichen Medizin, Versicherung, Finanzen und Militär tätig.
Pierre-François Regamey verfügt über ein Diplom als Ingenieur der ETH Lausanne (EPFL) und weist weitreichende Erfahrungen in den Bereichen Software- und Applikationsentwicklung auf.

Wo liegt denn das Bedrohungspotential für europäische Spitäler?
Hier sehe ich es eher bei sogenannten «Kollateralangriffen». Die Cyberkriminalität ist durch Mafia-ähnliche Strukturen gekennzeichnet. Es wird versucht, auf betrügerische Weise möglichst viel Geld zu verdienen, zum Beispiel durch die Verschlüsselung von Daten, für deren Wiederherstellung dann ein «Lösegeld» gezahlt werden muss. Solche *Ransomware*-Attacken zielen nicht speziell auf Spitäler. Aber die Folgen eines Angriffs sind im Spitalbereich besonders gravierend, weil hier hochsensible Daten gespeichert sind und die Behandlung der Patienten gefährdet sein kann, wenn der Zugriff auf diese Informationen vorübergehend blockiert ist.

Man hört, dass es heutzutage einfacher sei, durch eine Cyberattacke zu viel Geld zu kommen als durch einen Banküberfall. Trifft dies im Spitalbereich zu?
Jein. Historisch gesehen trifft es zu, dass viele Spitäler im IT-Bereich ungenügend geschützt waren. In den letzten Jahren wurden aber enorme Fortschritte erzielt. Nach meiner Einschätzung sind die Spitäler heute gut gegen Angriffe gewappnet, insbesondere in der Schweiz. Diesbezüglich stehen sie auch im Vergleich mit Banken und Versicherungen nicht schlecht da.

Gab es in der Schweiz Fälle, in denen effektiv Geld von Spitälern erpresst wurde?
Im Gegensatz zu den USA sind mir solche Fälle für Europa nicht bekannt. Wie erwähnt haben Attacken mit Ransomware hierzulande nicht speziell Spitäler im Visier. Das Schadenspotential von Cyberattacken ist trotzdem sehr hoch, weil nach einem erfolgreichen Angriff ein enormer Aufwand betrieben werden muss, bis die Systeme wieder normal funktionieren. Wenn Sie zum Beispiel den Betrieb der Notfallstation einschränken müssen oder keine Operationen durchführen können, weil nicht auf die benötigten Daten zugegriffen werden kann, ist das für ein Spital verheerend.

Wie sieht es denn mit Erpressungen von «Lösegeld» zur Wiederherstellung blockierter Daten aus?
Für solche Fälle sind wir im CHUV insofern gewappnet, als wir unsere Daten stündlich in Backups sichern. Vor drei Jahren hatten wir einen Angriff, bei dem einige administrative Dateien verschlüsselt wurden. Wir haben sie aber nicht verloren, sondern konnten sie nach der Entfernung des Virus aus dem System dank des Backups wiederherstellen. Die sensiblen klinischen Daten sind in speziell geschützten Datenbank-Systemen gespeichert und deshalb durch übliche Ransomware nicht angreifbar. Durch solche Sicherheitsnetze sind wir gegen Angriffe dieser Art sehr gut abgesichert.

Gibt es spitalspezifische Schwachstellen, die Angreifer nutzen können?
Spitäler sind leider sehr vulnerabel, weil sie sehr offen sind. Ein Spital ist zwangsläufig viel offener als eine Bank oder auch eine Kaserne. Banken können ohne grosse Schwierigkeiten sehr hohe Sicherheitsstandards etablieren, auch auf der IT-Ebene. Das ist im Spital aus verschiedenen Gründen nicht so einfach. So müssen Ärztinnen und Ärzte von verschiedenen Stellen aus sehr rasch auf Patientendaten zugreifen können, damit eine gute Behandlung möglich ist. Im physischen Bereich ist das übrigens ähnlich. In verschiedenen Genfer Privatbanken müssen mehrere Sicherheitsschleusen passiert werden, bis man «drin» ist, während man im Spital mit einem weissen Kittel fast überall Zutritt hat.

Wie schaffen es Cyberkriminelle, die Sicherheitssysteme der Spitäler auszutricksen?
Die verbreitetste Methode besteht sicher darin, Mails an die Mitarbeiter zu schicken, die Links oder Anhänge enthalten. Werden diese angeklickt, installiert sich ein Schadensprogramm. Daneben gibt es weitere Möglichkeiten, zum Beispiel eine Art «Scanner» aus dem Internet, die systematisch nach Schwachstellen suchen, die das Eindringen in gesicherte Systeme erlauben. Es gibt zwar Mittel, das zu verhindern. Aber es ist ein wenig wie in einem riesigen Hotel: Wenn Sie dort den ganzen Tag durch die Gänge gehen und jede Tür ausprobieren, finden Sie wahrscheinlich einmal eine, die offen ist. Dann können Sie eintreten und etwas stehlen. Solche Attacken finden täglich zu Tausenden statt.

«Es ist ein wenig wie in einem riesigen Hotel: Wenn Sie dort den ganzen Tag durch die Gänge gehen und jede Tür ausprobieren, finden Sie wahrscheinlich einmal eine, die offen ist.»

Ist es überhaupt möglich, alle Türen geschlossen zu halten?
Das ist unsere Aufgabe, und wir versuchen uns laufend zu verbessern. Eine Möglichkeit, die wir dafür nutzen, besteht darin «ethische Hacker» anzustellen. Das sind Spezialisten, die in unserem Auftrag versuchen, in unsere Systeme einzudringen. Als wir vor 15 Jahren damit begonnen haben, waren sie ziemlich erfolgreich im Aufspüren offener Türen. Mittlerweile haben wir sehr viel dazugelernt, aber wir führen solche Tests nach wie vor periodisch durch und profitieren davon. Dies ist auch deshalb nötig, weil täglich neue Bedrohungen auftauchen und weil sich unsere Systeme ständig weiterentwickeln und dadurch neue Schwachstellen entstehen können.

Für die IT-Sicherheit sind primär Spezialisten wie Sie zuständig. Inwiefern gehen Sicherheitsfragen auch die Ärztinnen und Ärzte an, die in Spitälern arbeiten?
Tatsächlich machen technische Fragen, um die sich die Spezialisten kümmern, nur einen Teilbereich aus. Gerade bei Angriffen vom Typ «Social Engeneering» ist die Sensibilisierung der Mitarbeiter sehr wichtig. Dabei werden beispielsweise via soziale Netzwerke personenspezifische Daten gesammelt, die dann genutzt werden, um bestimmte Personen zu adressieren und dabei glaubwürdig zu wirken.

Wie läuft das konkret ab?
Wenn Sie als Ärztin oder Arzt zum Beispiel eine E-Mail-Nachricht erhalten, die aufgrund bestimmter Detailkenntnisse ihrer Person glaubwürdig wirkt, aber trotzdem vom Kontext her auffällig ist, sollten bei Ihnen die Alarmglocken läuten. Zum Beispiel ist es nicht normal, dass ein Oberarzt im Spital eine Rechnung der Swisscom erhält – was bei uns tatsächlich passiert ist. In solchen Fällen sollte man Links oder Anhänge nicht aus Neugier anklicken. Es gehört zu den Aufgaben eines IT-Verantwortlichen, in diesem Bereich eine gewisse Unternehmenskultur zu etablieren.

Bei Angriffen vom Typ «Social Engineering» ist die Sensibilisierung der Mitarbeiter sehr wichtig.

Kommt es im CHUV häufig vor, dass es wegen zu sorglosen Umgangs ärztlicher Mitarbeiter mit E-Mails zu Sicherheitsproblemen kommt oder gar Schaden entsteht?
Fehlverhalten von Mitarbeiterinnen und Mitarbeitern ist ziemlich häufig. Immerhin haben wir im CHUV 12 000 Computerarbeitsplätze. Grösserer Schaden wird aber meist schon dadurch verhindert, dass die wenigsten Mitarbeiter Administratorenrechte haben. Wenn ein Arzt in der Hektik des Arbeitsalltags durch einen Klick ein Schadensprogramm aktiviert, so kann sich dieses in aller Regel nicht auf dem PC installieren, weil der Mitarbeiter dafür über Administratorenrechte verfügen müsste. Auf dem eigenen PC zuhause hat man dagegen die Administratorenrechte, so dass das Risiko eines Schadens dort ungleich höher ist.

Gelten für alle Mitarbeiterinnen und Mitarbeiter des CHUV dieselben Sicherheitsstandards?
Es gibt schon Unterschiede. Für Forscher ist es heutzutage sehr wichtig, vernetzt zu sein, sich mit Kollegen in der ganzen Welt auszutauschen und dabei vielleicht auch mal ein Programm auszuprobieren, das sie von einem Kollegen in San Diego oder London erhalten. Diese Möglichkeiten, auf die etwa Pflegefachpersonen zur Ausübung ihrer Arbeit nicht angewiesen sind, müssen wir ihnen geben. Wir haben im CHUV deshalb zwei Netzwerke. Eines mit klinischen Daten, das extrem gut geschützt ist, und eines für Daten aus der Forschung, das vergleichsweise offen ist. Aber das kostet natürlich.

Im Spitalbereich werden wir immer Kompromisse zwischen dem technisch Machbaren und den operationellen Bedürfnissen finden müssen.

Denken Sie, dass das (ärztliche) Personal in Bezug auf Cyberkriminalität speziell geschult werden müsste?
Auf jeden Fall – das ist sehr wichtig. Wir arbeiten daran, eine neue Sicherheitskultur zu etablieren. Sensibilisierungsmassnahmen für neue Mitarbeiter gibt es bei uns schon länger. In den nächsten Monaten werden wir zusätzlich spezifische Programme für einzelne Mitarbeitergruppen einführen, etwa für Pflegefachpersonen oder für Ärztinnen und Ärzte.

Ein Spital, das gegen Cyberattacken immun ist, wird es aber wohl auch in Zukunft nicht geben?
Gerade im Spitalbereich werden wir immer Kompromisse zwischen dem technisch Machbaren und den operationellen Bedürfnissen finden müssen. Es ist nicht immer einfach, schnelle Zugriffsmöglichkeiten auf sensible Daten, auf die Sie als Arzt angewiesen sind, mit höchsten Sicherheitsstandards zu vereinbaren. Aber in der Schweiz sind wir Spezialisten für Kompromisse, deshalb kriegen wir auch das ganz gut hin.

Bildnachweis:
Porträtfoto: zVg P.-F. Regamey.
Foto Referat Ärztekammer: Tobias Schmid/FMH.

bkesseli[at]emh.ch