Erpresser-Software gegen Spitäler: «Beim Schutz wird das Geld dann oft zu knapp»

Veröffentlicht am: 21. Februar 2016 17:03

«Solche Vorfälle gab es auch schon hier»: Urs Achermann, Chief Information Security Officer HINT AG (PD)

Reihenweise wurden in den letzten Tagen Kliniken in Amerika und Europa gehackt, blockiert und so erpresst. Könnte das auch in der Schweiz passieren? IT-Sicherheits-Experte Urs Achermann weiss es. Das Interview.

Herr Achermann, in den letzten Tagen hörte man von massiven Hackerangriffen auf Spitäler in Deutschland und den USA. Die IT der Kliniken wurde durch* Malware *lahmgelegt, dann forderten die Täter «Lösegeld», um die blockierten Systeme wieder zu entschlüsseln. Ist das Zufall – oder ist das Gesundheitswesen derzeit besonders bedroht?

Es handelt sich gar nicht so sehr um einen gezielten Angriff auf Kliniken. Doch heute ist die Medienaufmerksamkeit viel grösser. Früher wurde eher über andere Hackerprobleme berichtet, etwa über Diebstahl von Kundendaten bei Banken. Die Spitäler sind nun einfach neues Thema.

Dabei geht es nicht um Diebstahl, sondern um eine Art Erpressung. Sind Kliniken hier speziell gefährdet?

Es ist lediglich eine neue Vorgehensweise. Wie gesagt: Die Angriffe richten sich nicht nur auf das Gesundheitswesen. Andererseits liegt der Gesundheitssektor technisch teils etwa fünf bis zehn Jahre zurück, verglichen beispielsweise mit den Banken. Ich arbeite seit über 15 Jahren in den verschiedensten Branchen im Sicherheitsbereich, und da stellt man das schon

fest. Natürlich investieren die Spitäler sehr viel Geld in die Technik – denken Sie nur an die MRI-Geräte –, aber beim Basissystem und beim Schutz wird es eher knapp. Das liegt auch daran, dass es oft am Bewusstsein fehlt für die Problematik.

Urs Achermann ist Chief Information Security Officer bei der HINT AG, einem Spezialunternehmen für ICT-Prozesse im Gesundheits- und Sozialwesen. Er ist seit 1993 in der Informatik tätig, davon mehr als 17 Jahre als Spezialist für Informationssicherheit und Datenschutz. Urs Achermann war unter anderem Information Security Officer bei Holcim und bei Julius Bär. Er ist diplomierter Wirtschaftsinformatiker und verfügt über einen Master in Informationssicherheit.

Woher kommt das?

Der Druck von aussen ist geringer. Bei den Banken gibt es eine Aufsichtsbehörde wie die Finma, die sehr strenge Vorgaben erlässt und deren Einhaltung überprüft. Etwas Ähnliches gibt es im Gesundheitswesen nicht. Und wenn dieser äussere Druck fehlt, wirkt sich das aufs Bewusstsein der Verantwortlichen aus. Dabei denke ich gar nicht nur an die IT-Leute, sondern auch an Vorgesetzte oder Anwender.

Die aktuellen Hacker-Angriffe auf Spitäler hatten Erfolg, weil einzelne Mitarbeiter die Viren herunterluden, indem sie fälschlicherweise einen «verseuchten» Anhang öffneten. Das ist eine gängige Falle, die immer wieder funktioniert – Bewusstsein hin oder her.

So ist es. Gerade deshalb denke ich auch, dass diese Hacker sich gar nicht so gezielt gegen Spitäler richteten. Die Infektion kann durch Email-Anhänge geschehen. Und im vergangenen August entdeckten wir solche Kryptoviren, die durch so genannte «Drive by»-Downloads ins System eines Kunden gelangt waren: Ein Mitarbeiter ging auf eine bestimmte Website, diese Site war infiziert – und die Viren gelangten auf sein Gerät, ohne dass überhaupt etwas angeklickt wurde.

Da hilft keine Sensibilisierung mehr.

Ja, in solchen Fällen können die Nutzer gar nichts machen. Natürlich sollten die Mitarbeiter wissen, dass sie möglichst nicht auf alles klicken sollten, aber gegen «Drive by»-Downloads hilft das auch nichts. Die einzige Lösung wäre, das Internet vom internen Netz zu trennen.

Cyberattacken aufs Gesundheitswesen: Was ist geschehen?

In Deutschland wurden in den letzten Tagen gleich ein halbes Dutzend Kliniken von Computerviren angegriffen, Operationen mussten abgesagt und Patienten verschoben werden. In Kalifornien wurde das System eines Spitals über sechs Tage lang völlig blockiert. Zugleich wurden auch deutsche Online-Apotheken Opfer von Online-Erpressungen.

Das Vorgehen ähnelt sich stets: Mit Kryptoviren verschlüsseln die Hacker die Daten der Institutionen – dann folgt ein Erpressermail: Gegen eine bestimmte Summe, zahlbar in Bitcoins, erhalten die Opfer einen «Schlüssel», um ihre Daten wieder zu verwenden.

Es kommen auch immer wieder neue Virenformen. Das heisst: Letztlich lässt es sich nicht hundertprozentig vermeiden.

Schwierig. Wir setzen natürlich auf allen Ebenen verschiedene Antiviren-Software ein. Die Antivirenhersteller arbeiten dabei mit Signaturen: Sie melden Beschreibungen von verdächtigen Mustern. Aber sobald die Gegenseite etwas an diesem Muster ändert, wird es mit herkömmlichen Mitteln sehr schwierig. Und heute verändern sich diese Muster ständig. Beim erwähnten Fall im August war entscheidend, dass wir innert 18 Minuten den Benutzer identifizieren konnten, um sein Gerät vom Netz zu trennen. In jenen 18 Minuten schafften es die Viren trotzdem, etwa 20'000 Dateien zu verschlüsseln. Jetzt stellen Sie sich nur vor, dass so etwas übers Wochenende geschieht.

In den USA bezahlte das betroffene Spital tatsächlich Lösegeld, damit die Angreifer ihre Programme und Dateien wieder freigaben. Kann das wirklich eine Lösung sein?

Ohne die Entschlüsselung der Erpresser gibt es nur eine Möglichkeit, um die Daten wiederzuerlangen: Man muss sie aus dem Backup holen. Aber was tun, wenn man kein Backup hat – oder nur ein unvollständiges? Und es ist bereits ein grosser Aufwand, 20'000 Dateien zu finden, zu löschen und die Originaldateien wieder zurückladen. Wenn man aber mehr Pech hat und Millionen Dateien blockiert wurden, dann ist es betriebswirtschaftlich verlockend, wie im US-Fall einfach 17'000 Dollar zu bezahlen.

Die HINT AG ist ein führender Anbieter von IT-Dienstleistungen im Schweizer Gesundheits- und Sozialwesen. Das Unternehmen mit Sitz in Lenzburg konzipiert, implementiert und betreibt modulare eHealth-Lösungen und unterstützt so die integrierte Versorgung. Zur Unterstützung der Kunden dient zudem ein Healthcare Competence Center.

2004 gegründet, beschäftigt die HINT AG heute 130 Mitarbeitende und erwirtschaftete 2014 einen Umsatz von 36,1 Millionen Franken.

Die Kernfrage haben Sie wohl schon weitgehend beantwortet: Könnte das auch in der Schweiz passieren?

Definitiv ja. Solche Vorfälle sind auch schon eingetreten. In allen Fällen, die ich live erlebt habe, konnten wir Gottseidank rasch die Problembereiche isolieren. Beim ersten Vorfall kamen wir recht ins Schwitzen! Oft ist es ja so: Man sieht den Schaden – aber die eigentliche Malware lässt sich in den riesigen vernetzten Systemen nur schwer finden. Wir haben viel aus dem ersten Fall gelernt und konnten bei den folgenden Vorfällen sehr schnell und professionell handeln.

Und wenn es geschieht, werden auch unsere Spitäler gleich klinikübergreifend lahmgelegt, von Radiologie über Onkologie bis hin zur Buchhaltung?

Auch das ist logisch. Die verschiedenen Bereiche wollen ja heute vernetzt sein. Und man will immer stärker, dass die Daten zentral erfasst werden.

Die Sicherheitsbehörden beschäftigen sich bereits mit der nächsten Stufe: nämlich der Gefahr, dass Hacker aus der Ferne die Kontrolle über Medtech-Geräte wie Infusionspumpen, OP-Roboter oder gar Herzschrittmacher übernehmen. Ist das Science Fiction – oder macht Ihnen das auch schon Sorgen?

Definitiv. Heute will man alles digital, und alles soll vernetzt sein. Das bietet enorme Vorteile. Wenn ein Herzschrittmacher autonom meldet, dass etwas nicht mehr stimmt beim Patienten, dann kann dies lebensrettend sein. Aber genau diese Vernetzung macht das Gerät dann angreifbar. Es ist denkbar, dass man mit üblen Absichten einen Menschen quasi virtuell entführen kann, dass man ihn erpresst und ihm androht, beim Herzschrittmacher die Frequenzen zu verändern.

Diese Vernetzung der Dinge birgt ein grosses Gefahrenpotential, übrigens nicht nur in der Medizin. Denken Sie nur an die selbststeuernden Autos – auch da liesse sich Gas- oder Bremspedal plötzlich von aussen steuern.