AKTUELL

IT-SICHERHEIT

Hack im Hospital?

Joël Adami

Krankenhäuser sind ein lohnendes Ziel für Hacker, es locken sensible Daten und damit vielfältige Erpressungsmöglichkeiten. Wie sicher ist die IT der Krankenhäuser?

Im Mai dieses Jahres legte eine sogenannte „Ransomware“ namens „WannaCry“ in England und Schottland über 70.000 Computer und medizinische Geräte in Krankenhäusern lahm - auch weltweit blockierte das Schadprogramm Computer und übermittelte die entsprechenden Lösegeldforderungen. Durch den erfolgreichen Angriff auf die Krankenhäuser wurde eins offenbar: Die IT-Infrastruktur in Krankenhäusern ist sehr oft gefährlich verwundbar. Während die Sache im obigen Fall noch einigermaßen glimpflich ausging - der Betrieb in den Krankenhäusern war nur für einige Zeit eingeschränkt -, sind gezieltere und in den Folgen dramatischere Angriffe auf medizinische IT-Infrastruktur durchaus denkbar.

Jelena Milosevic ist Krankenschwester in den Niederlanden und interessiert sich für IT-Sicherheit. Vergangene Woche hielt sie einen Vortrag auf der Computersicherheitskonferenz „hack.lu“, in dem sie vor mangelnder Sicherheitskultur in Krankenhäusern warnte. „Da ich oft als Freelancerin gearbeitet habe, war ich in vielen Krankenhäusern unterwegs. Ich war erstaunt, wie oft mir Kollegen und Kolleginnen ihre Zugangsdaten weitergaben und problemlos Zugriff auf das interne Netzwerk einräumten, so dass ich mir Patientendaten und E-Mails ansehen konnte“, berichtete Milosevic in ihrem Vortrag. Sie zeigte einige plakative Beispiele, die auf twitter kursierten: Post-Its mit Login-Daten, die an den entsprechenden Computern kleben, Schränke für Blutkonserven, auf denen das aus dem Jahre 2001 stammende Windows XP läuft, medizinische Geräte, die offen mit dem Internet verbunden und über dieses steuerbar sind, und jede Menge PatientInnen, die mit Computern in Behandlungszimmern unbeaufsichtigt gelassen werden. Große Sicherheitsrisiken also, deren mögliche Konsequenzen von Datenklau über Erpressung bis hin zu Mord reichen.

Milosevic hat sich auch die Webseiten von Krankenhäusern in den Niederlanden und in den USA angeschaut und festgestellt, dass nur sehr wenige ausreichend gesichert sind, also zum Beispiel über eine verschlüsselte Verbindung angeboten werden. Das mag wie ein unwichtiges Detail erscheinen, kann aber tiefgreifende Konsequenzen haben: Oft befinden sich auf den Webseiten auch MitarbeiterInnen-Logins, damit man leichter Zugang zu E-Mails oder anderen Daten hat - so kann die unsichere Webseite zum Einfallstor für AngreiferInnen werden. Mit einem Zugang zu den MitarbeiterInnen-Mails ließen sich auch realistisch aussehende Phishing-Mails verschicken - mit denen könnte wiederum Malware auf den Krankenhaus-Computern installiert werden, die HackerInnen Zugriff auf sensible Daten wie beispielsweise PatientInnenakten verschafft. Die Schuld für die Mängel der IT-Sicherheitskultur in Krankenhäusern sieht Milosevic teilweise bei ihren KollegInnen: „Viele sind sich nicht bewusst, was sie tun, wenn sie Login-Daten weitergeben. Sie denken, das Netzwerk ist ja gesichert und es wird schon nichts passieren.“ Allerdings räumt sie ein, dass die IT-Abteilungen vieler Krankenhäuser sehr klein sind und oft über keine spezielle Sicherheits-Abteilung verfügen: „In den USA haben 85 Prozent der Krankenhäuser keinen IT-Sicherheitsbeauftragten!“

Internet of hacked things

Vernetzte Geräte - ob professionelle medizinische Geräte oder „Internet of things“-Blutdruckmesser für die EndverbraucherInnen - sieht die Krankenschwester ebenfalls kritisch: „Wir sollten uns wirklich überlegen, was wir alles online haben wollen. In Wirklichkeit gibt es viele Geräte, die nicht ständig online sein müssen. Aus Bequemlichkeit wird es doch getan. Manchmal wollen auch die Hersteller mehr Daten generieren, ohne dass Patienten und Patientinnen oder Krankenhäuser darüber informiert werden“. Wie konkrete Szenarien, beispielsweise ein Angriff auf eine automatisierte Injektionspumpe, aussehen könnten, führt Milosevic lieber nicht aus: „Ich will niemanden Ideen geben, aber die Konsequenzen könnten sehr schwerwiegend sein.“

Könnte mit einem Hacker-Angriff auch in Luxemburg ein Krankenhaus lahmgelegt - oder, schlimmer noch, PatientInnen-Datenmaterial gestohlen werden? Im Centre Hospitalier Emile Mayrisch (CHEM) sieht man sich gut gewappnet. Die Netzwerke seien segmentiert, so dass nicht alle NutzerInnen auf alle Informationen zugreifen können, erklärt man der woxx auf Nachfrage. Außerdem sei das CHEM, wie alle anderen Krankenhäuser in Luxemburg, nicht direkt, sondern über das nationale „Healthnet“-Netzwerk mit dem Internet verbunden, sei also geschützt. Im CHEM läuft nur noch auf 0,5 Prozent der Computer Windows XP. Zusätzlich werden die CHEM-MitarbeiterInnen in Zusammenarbeit mit „security made in Luxembourg“ geschult. „Vor einem Jahr haben wir Phishing-Testmails versendet, um zu sehen wo wir in diesem Bereich stehen“, erklären Patrick Horsmans von der IT-Abteilung und Christophe Chaudy von der Abteilung für Informationssicherheit des CHEM.

Jelena Milosevic bemüht sich unterdessen weiter, ihre KollegInnen und die Öffentlichkeit für das Thema zu sensibilisieren. Sie ist auch in der Cyberethik-Gruppe „I Am the Cavalry“ aktiv, die z.B. einen hypokratischen Eid für vernetzte medizinische Geräte entwickelt hat. Mit solchen Initiativen - und mit stärkerer Zusammenarbeit zwischen medizinischem Fachpersonal und InformatikerInnen - könnte die darniederliegende IT-Sicherheit in den Krankenhäusern tatsächlich auf den Weg der Genesung gebracht werden.

EPA/MAST IRHAM

Auch in Jakarta, Indonesien, traf die „WannaCry“-Malware Krankenhäuser; es kam zu langen Wartezeiten.

I Am the Cavalry

(ja) Autonome Autos, vernetzte Herzschrittmacher, intelligente Stromnetze und ein „smartes“ Heim, in dem jeder Lichtschalter per Smartphone betätigt werden kann – die Zukunft aus Science Fiction-Filmen ist zum Greifen nah. Allerdings weisen diese Geräte und Infrastrukturen allesamt auch große Schwächen auf: Sie sammeln viel zu viele Daten, können nur schwer mit Updates versorgt werden und sind leicht zu hacken. PolitikerInnen sind damit überfordert, sichere Standards einzuführen, und die Hersteller zeigen oft nur wenig Interesse, selbst welche zu entwickeln. Die Cyberethik-Gruppe „I Am the Cavalry“ versucht, diese Lücke zu füllen. Die SicherheitsforscherInnen beschäftigen sich mit vernetzten Geräten in den Bereichen Medizin, Automobil, „Smart Home“ und öffentliche Infrastruktur. Die Gruppe, die einige hundert Mitglieder zählt, will Öffentlichkeit für die Probleme schaffen, PolitikerInnen und NutzerInnen informieren und gemeinsam mit der Industrie an Lösungen arbeiten. Dabei richtet sie sich aber auch an HackerInnen und schlägt Ethik-Richtlinien vor, mit denen Sicherheitslücken so aufgedeckt werden sollen, dass dabei möglichst niemand zu Schaden kommt. Daneben hat „I Am the Cavalry“ Leitfäden entwickelt, die zum Beispiel Sicherheitsstandards für die Entwicklung und das Updaten (teil)autonomer Autos vorschlagen.
iamthecavalry.org