Foto: alphaspirit - Fotolia

Die Trojaner greifen an

Krankenhaus-IT: Der Feind ist oft schon drin

Erst kürzlich hat der Trojaner „Locky“ mehrere Krankenhäuser in Arnsberg (NRW) regelrecht lahmgelegt. Locky infizierte das Betriebssystem von Microsoft, verschlüsselte Daten auf den Festplatten und sorgte somit für einen Absturz der Betriebssysteme. Er hatte sich rasend schnell auf Rechnern in Deutschland, den Niederlanden und den USA ausgebreitet. Dies sorgte zum ersten Mal auch für ein großes Presseecho bezüglich der IT-Sicherheit in Krankenhäusern.

Laut Medienberichten waren weitere Krankenhäuser in Mönchengladbach, Essen, Kleve und Köln von ähnlichen Trojanern betroffen, selbst das nordrhein-westfälische Innenministerium war Dezember 2015 Opfer eines Ransomware-Angriffs. Der Locky-Trojaner legte jegliche digitale Kommunikation lahm.

Dies kann zu Vertauschungen von Blutproben, Verwechslung von Patienten bis hin zu verzögerten Alarmmeldungen führen. Notfallpatienten können nicht aufgenommen werden und müssen weitere Anfahrtswege in Kauf nehmen. Diese Folgen können einzeln oder in Kombination zu schweren Patientenschäden bis hin zum Versterben von Patienten führen.

Krisenmanagement ist gefordert

Neben den finanziellen und personellen Aufwänden eines „ad hoc“-Krisenmanagement mit Eindämmung der neuartigen Bedrohung werden Patienten verunsichert und Krankenhausabläufe spürbar beeinträchtigt. Eine der betroffenen Kliniken musste das komplette IT-System herunterfahren. Der Trojaner wurde auf über 200 Klinikservern entdeckt. Die Angreifer haben erpresserisch Geldforderungen gestellt. Diese Ransomware (Erpressersoftware) wird meistens mittels Email-Anhänge nach Zufallsprinzip versendet. Die Angreifer fordern Geld gegen Entschlüsselungscode. Oft nützt die Geldzahlung herzlich wenig und es wird seitens des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) geraten, auf die Forderungen der Angreifer nicht einzugehen. Das Krisenmanagement ist gefordert, unter diesen widrigen Bedingungen die Folgeschäden so gering wie möglich zu halten. Es gilt, den Betrieb mit alternativen Lösungen – unter anderem Kommunikation mittels vorgefertigter Papierdokumente und Faxmitteilungen – solange zu überbrücken, bis der Trojaner entfernt und die IT-Systeme wieder laufen. Das Krisenmanagement

Der Feind ist bereits in unserem Haus. So in etwa muss man sich einen APT - Advanced Persistent Threat - vorstellen. Heutige Angriffe erfolgen wohlüberlegt und von langer Hand geplant. Die Angreifer verfügen über spezielle IT-Kenntnisse und verfolgen langfristige Ziele. Sie nutzen Trojaner mit individuell zugeschnittenen Angriffsvektoren und stellen so sicher, dass sie dauerhaft eine Zugriffsmöglichkeit auf das infizierte System, sei es ein Industrieunternehmen oder ein Krankenhaus, haben. Sie spähen aus, rauben Daten und analysieren Schwachstellen. Es kann vorkommen, dass Sie als KIS-Betreiber überhaupt nicht bemerken, dass Sie bereits infiziert sind. In der Regel sind die Angreifer auf wertvolle Geschäftsgeheimnisse von Spitzen-Industrieunternehmen aus, jedoch rücken auch immer mehr Krankenhäuser in den Fokus der Angreifer. Potentielle Ziele der Angreifer sind Patientendaten, die Manipulation von Medizingeräten und Erpressungen. Hier sind die KH-IT-Leitungen und die Krankenhausführung gefordert, mit entsprechenden Mitteln gegenzusteuern, so dass es erst gar nicht zu Patientenschäden kommen kann.

IT-Bedrohungs-szenarien

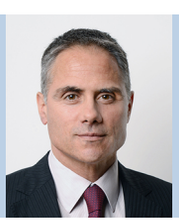
Generell können Bedrohungen in Anlehnung an die Gefährdungskataloge der IT-Grundschutz-Kataloge in fünf Kategorien unterteilt werden und sollten gezielt angegangen werden:

- Natürliche Ereignisse
- Technisches Versagen (von IT-Systemen, Datenspe ichern, Netzen oder der Versorgung)
- Menschliche Fehlhandlu ngen (an IT-Systemen, Software oder Daten)
- Vorsätzliche Handlungen (an IT-Systemen, Software oder Daten)
- Organisatorische Einflüsse (interne, externe)

eines der Krankenhäuser urteilte, dass „der Kommunikations- und Abstimmungsaufwand bei einem Ausfall des IT-Netzwerks erheblich höher sei. Ärzte und Pflegeteam mussten sich mit schriftlichen Aufzeichnungen von medizinischen Daten und Laborwerten behelfen. Wo erforderlich wurden Befunde zwischen den Standorten wieder per Fax übertragen“. All dies wurde durch eine erhöhte Personalstärke aufgefangen.

Windows XP als Einfallstor für Angriffe

Viele Medizingeräte verfügen über eine abgespeckte Betriebssoftware von Windows XP, die jedoch weder aktualisiert wird, noch mit aktuellen Patches vor Angriffen geschützt wird. Laut dem Wired-Magazin konnte Scott Erven, ein bekannter IT-Sicherheitsforscher bei einem Gesundheitsdienstleister, bei Medizingeräten verschiedener US-Krankenhäuser zahlreiche Sicherheitsmängel finden, unter anderem gelang es ihm, OP-Roboter fernzusteuern, tödliche Elektroschocks zu simulieren oder Blutkonserven in einem Kühlschrank zu erwärmen, ohne dass dies vom Alarmsystem registriert wurde. Häufig sind sich die Medizingerätehersteller und Krankenhausbetreiber der Gefahr nicht einmal bewusst, da sie keine Tests in diese Richtung durchführen.



Dr. Alexander Euteneier MBA
Geschäftsführer
Euteneier Consulting für klinisches Risikomanagement und Prozessmanagement
Herrsching am Ammersee

Weitere Angriffsflächen auf der Hardware - Ebene

Neben dem Microsoft – Betriebssystem ist die PC-Hardware selbst zum Angriffsziel verschiedener Trojaner und Viren geworden. So bietet Intel® für Rechner mit einer im Mainboard implementierten Management-Lösung (AMT) eine vermeintlich komfortable Fernwartungsfunktion. Diese ermöglicht damit das Auslesen von Statusinformationen, das Ändern von Konfigurationen und das Ein- und Ausschalten des PCs. Diese Funktionen greifen jedoch selbst bei abgeschalteten oder abgestürzten Systemen in die Verwaltung, Inventarisierung, Diagnose und Reparatur von PCs ein. Denkt man dieses Szenario weiter, kann diese Fernwartungsfunktion dazu missbraucht werden, Geräte mit diesem Chipsatz zu manipulieren und deren Funktionen zu verändern. Ausschlaggebend ist die einfache, typischerweise unkonfigurierte und mit einem Standardpasswort versehene Sicherung dieser AMT-Funktion. Das Passwort ist Profi-Hackern schnell zugänglich, und kann zum Beispiel auf „darknet websides“ beschafft werden. Es ist deshalb dringend anzuraten, vorhandene Subsysteme, unabhängig von ihrer späteren Verwendung, vor Geräteeinsatz mit einem neuen, sicheren Passwort zu versehen. Dies betrifft insbesondere Medizingeräte, wie Beatmungs- und Narkosegeräte sowie Monitoring-Systeme. Erst durch einen sicheren Passwortschutz macht es Sinn, das Subsystem in den BIOS-Settings zu deaktivieren. Das alleinige Deaktivieren von AMT-Funktionen ermöglicht stets eine erneute remote Rekonfigurierung der Einstellungen.

Medizingeräte und medizinische Netzwerke

Generell werden Medizingeräte immer häufiger zur Angriffsfläche. Bereits 2013 warnte laut Heise Online das Industrial Control System-CERT (ICS-CERT) vor Sicherheitslücken in medizinischen Geräten. Zusammen mit der US-amerikanischen Food and Drug Administration (FDA) identifizierten sie „rund 300 medizinische Geräte von circa 40 Unternehmen“, die durch hard coded – fest voreingestellte – Passwörter leicht zu manipulieren sind. Diese Geräte sind immer öfter in das Krankenhausnetzwerk eingebaut und so potenziell auch aus dem Internet zugänglich.

Warum Dick Cheney nicht mehr ruhig schlafen konnte

Marie Moe, eine bekannte IT-Sicherheitsforscherin, forderte ihre Kollegen aus der Hacker- und IT-Sicherheits-Community auf, ihr „das Herz zu brechen“. Sprichwörtlich, denn seit vier Jahren ist sie Trägerin eines Herzschrittmachers, der von der Ferne aus gesteuert werden kann. Neben ihr ist auch der ehemalige Vizepräsident der Vereinigten Staaten von Amerika Träger eines Herzschrittmachers mit Defibrillatorfunktion. Aus Sorge um sein Herz ließ Dick Cheney die remote-Funktion deaktivieren. Anscheinend war sein Vertrauen in den Schutz vor einem Hackerzugriff auf seinen Herzschrittmacher nicht groß genug.
Marie Moe hingegen erforschte über mehrere Jahre intensiv Möglichkeiten der Manipulation von Herzschrittmachern und stellte ihre Ergebnisse zusammen mit Éireann Leverett auf dem 32. Chaos Communication Congress 2015 vor. Teile ihrer Forschungsergebnisse hielt sie aus Sorge vor Missbrauch weiterhin unter Verschluss.

Bedrohungen ernst nehmen – für Achtsamkeit sorgen

Die wohl wichtigste erste Maßnahme besteht darin, das Bedrohungsszenario ernst zu nehmen. Cyberangriffe schaffen ein überaus relevantes Risiko für KH-Betreiber und Patienten. Ein IT-Krisenmanagement-Konzept sollte alle Eventualitäten in Betracht ziehen. Auch jene, die zwar bis dato eher unrealistisch klingen, jedoch schnell zu einer konkreten Bedrohung ausarten können. In einem weiteren Schritt sind die Mitarbeiter auf die möglichen Bedrohungen im Rahmen von Fortbildungen aufmerksam zu machen.

Erfassen der Bedrohung

Es bleibt weiterhin eine Herausforderung, das tatsächliche Bedrohungspotenzial objektiv zu erfassen. Ein möglicher Ansatz besteht darin, Angriffe auf das Intranet der Klinik und deren Subsysteme mittels sogenannter Honey Pots zu erfassen. Honey Pots geben sich als vielversprechende Angriffsziele aus. So registrierten laut Heise online Sicherheitsforscher an ihren zehn aufgestellten Honeypots, die sich als MRT- und Defibrillator-Geräte ausgaben, innerhalb von sechs Monaten „55.416 erfolgreiche Anmeldungen via SSH und Web-Oberfläche, 299 Angriffe mit Malware, die in 24 Fällen mit Exploits eigene Codes ausführten."

Weitere Abwehrstrategien bestehen darin, über spezielle Network Intrusion Detection Systeme (NIDS) und Network Intrusion Prevention Systeme (NIPS) schädliche IP-Anfragen aus dem Internet zu detektieren und abzuwehren. Die Analyse des Datenverkehrs gibt hilfreiche Aufschlüsse darüber, ob Angriffe tatsächlich stattfanden.

Fehlerquellen ausmerzen

Häufig bestehen Nachlässigkeiten unachtsamer Mitarbeiter im Umgang mit den IT-Systemen des Krankenhauses. Verstärkt wird dies durch IT-Abteilungen, die diesem Verhalten unbeteiligt zusehen. Die mangelhafte Passwortvergabe der Mitarbeiter biete Angreifern eine leichte Angriffsfläche. So nachvollziehbar es auch sein mag, dass das Verwalten persönlicher, sicherer Passwörter mühsam ist, besonders wenn Mitarbeiter sich viele Passwörter merken müssen, so darf dies keine Entschuldigung sein, mittels trivialer Passwörter ein Einfallstor für Angriffe zu schaffen. Zum einen müssen Passwörter einem definierten Sicherheitsstandard genügen, was heute durch entsprechende Passwortvorgaben IT-technisch leicht konfigurierbar ist, zum anderen müssen die IT-Betreiber alles unternehmen, durch entsprechende Single Sign On – Lösungen für ein komfortables Arbeiten innerhalb der verschiedenen Krankenhaus-IT-Subsystemen zu sorgen. Des Weiteren besteht die Möglichkeit, durch intelligente Rollen/Rechtevergabe die Zugriffsmöglichkeiten auf sensible Bereiche einzuschränken.

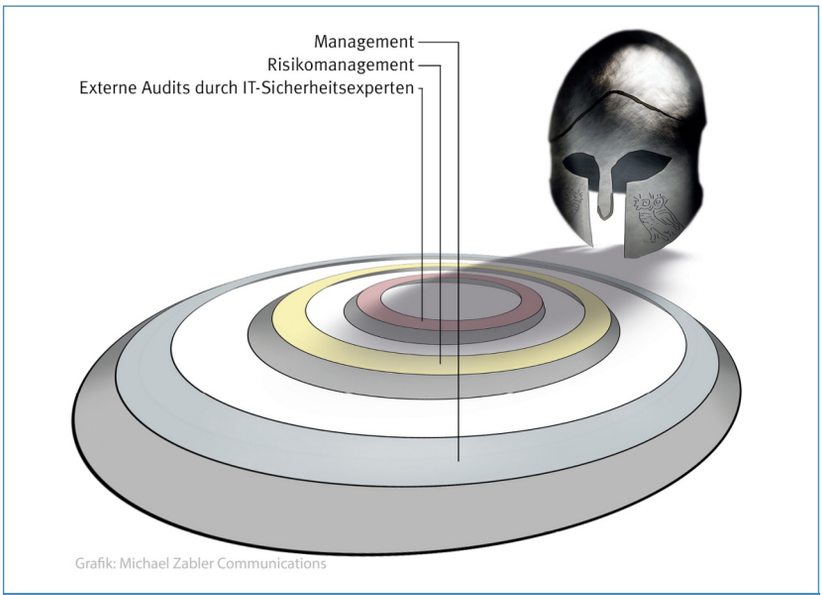


Abb.: Die drei Verteidigungslinien des BSI.

IT –Sicherheitsgesetz und Beratungsmöglichkeiten

Der derzeit diskutierte Entwurf zum IT-Sicherheitsgesetz zielt darauf ab, die Sicherheit informationstechnischer Systeme in Deutschland zu verbessern. Dabei gilt insbesondere für kritische Branchen, wie Krankenhäuser, eine Meldepflicht zu Sicherheitsvorkommnissen. Im Gesetz werden bereits bestehende Aktivitäten zur Cybersicherheitsstrategie und der Allianz für Cybersicherheit aufgegriffen. Siehe www.allianz-fuer-cybersicherheit.de

Die Nutzung IT-spezifischer Beratungsmöglichkeiten kann ebenfalls dazu beitragen, dass Risiken frühzeitig erkannt und eingedämmt werden. Hier erscheint es besonders hilfreich, wenn die Beratung sowohl IT-technische Fragestellungen als auch klinische Fragestellungen adressiert, da mittlerweile beide Bereiche über Schnittstellen eng miteinander verknüpft sind. So bleibt die Entwicklung von IT-Ausfallszenarien eine Herausforderung, um weiterhin eine fach(arzt)gerechte Versorgung der Patienten zu gewährleisten.

Drei Verteidigungslinien

Das BSI schlägt den Aufbau von drei Verteidigungslinien vor:

1. Linie – Management
2. Linie – Risikomanagement
3. Linie – Externe Audits durch IT-Sicherheitsexperten

Die erste Linie erfordert, dass das Management die Notwendigkeit von Maßnahmen zur Cyber-Sicherheit, den Schutzbedarf der Geschäftsprozesse sowie deren Abhängigkeiten und Bedrohungen erkennt. Die zweite Linie erfordert die Implementierung eines proaktiven Risikomanagements, welches auch Cyber-Sicherheitsrisiken gezielt eindämmt. Dabei werden auch diesbezügliche Entscheidungen der Leitung und des Managements bewertet. Haben Cyber-Attacken stattgefunden oder besteht hierzu die Sorge, bietet sich die Option reaktiver bzw. präventiver Maßnahmen mittels Durchführung eines Cyber-Sicherheits-Checks an. Diese werden in der Regel durch IT-Experten, z. B. des BSI nach einem standardisierten Prozess durchgeführt.

Krankenhäuser sind bei weitem nicht die einzigen Ziele krimineller IT-Machenschaften. So haben Angriffe auf den deutschen Bundestag, Automobilsteuerungs-Software, Dating-Portale, Banken sowie Offshore-Firmen das neue Bedrohungspotenzial eindrücklich bewiesen.

„Nichts ist absolut sicher", um mit den Worten des Fraunhofer-Präsident Neugebauer zur Datensicherheit zu sprechen. Können Angreifer jedoch Narkosegeräte hacken und Patienten dadurch aus der Ferne schädigen oder sogar töten, ist Gefahr in Verzug. ■

Dr. Alexander Euteneier MBA
Euteneier Consulting GmbH
Neuhauserweg 5
82211 Herrsching am Ammersee
E-Mail: ae@euteneier-consulting.de