NACHRICHTEN

IT-Angriffe auf das Gesundheitswesen sorgen für Verunsicherung

Virusattacken abwehren

Bei der Cyberattacke durch die Erpressersoftware „WannaCry" waren die Computer ganzer Krankenhäuser blockiert und selbst die Fahrplananzeigen der Deutschen Bahn betroffen. An Maßnahmen zur Vermeidung von IT-Angriffen kommt auch die Pflegebranche nicht mehr vorbei.

Von Thomas Althammer

Hannover // Bei einem Blick auf die IT-Sicherheitsvorfälle der vergangenen Monate wird zweierlei deutlich: Zum einen können scheinbar selbst gut abgesicherte Systeme nicht vollständig vor Angriffen geschützt werden. Zum anderen steigen die Kosten für Präventionsmaßnahmen und die Kosten für eine Schadensbeseitigung, falls es zu einem erfolgreichen Angriff gekommen ist.

Dass es dann ein Verschlüsselungstrojaner bis auf die Monitore von Fahrplananzeigen schafft, zeigt, mit wie viel Aufwand und krimineller Energie diese moderne Form von Computerviren entwickelt wird.

Betroffen ist grundsätzlich jeder, Einrichtungen in der Pflege vielleicht in besonderer Weise, weil häufig kein eigenes IT-Personal im Haus ist und Budgets im IT-Bereich eher knapp bemessen sind. Das bedeutet, das IT-Schutzniveau ist eher geringer einzuschätzen als beispielsweise in einer Bank oder bei einer Versicherung. In 98 Prozent der vom dem Verschlüsselungstrojaner WannaCry befallenen Systeme kam Windows 7 zum Einsatz, für das zum Zeitpunkt des Ausbruchs im Mai 2017 schon seit einigen Wochen ein Sicherheitspatch von Microsoft bereitstand. Während bei den privaten Windows-Nutzern das automatische Einspielen kritischer Updates dazu führt, dass bekannte Sicherheitslücken schnell und flächendeckend gestopft werden, spielen Unternehmen und Institutionen solche Patches häufig nicht direkt in ihre Systeme ein.

Gründe dafür sind zum Beispiel unregelmäßige Zugriffe durch Administratoren, die die Einspielung der Updates erst manuell veranlassen müssen. Ein anderer Grund kann im Einsatz spezieller Branchensoftware oder anderer für die jeweilige Einrichtung angepasster Software liegen. Als Ironie des Schicksals erwies sich, dass WannaCry selbst auch über eine Art „Sicherheitslücke" verfügte. So fand ein britischer Sicherheitsexperte bei der Analyse des Verschlüsselungstrojaners Hinweise auf eine unbekannte Internet-Domäne. Mit deren Registrierung entdeckte er dabei scheinbar eine Art „Kill-Switch", der in diesem Fall nicht sonderlich gut versteckt war, die weitere Ausbreitung des Virus aber abrupt stoppte.

Aufbau eines Informationssicherheits-Managementsystems

Ein einziges wirksames Mittel zur Abwehr derartiger Angriffe – und das haben WannaCry und andere Cyberattacken in den letzten Monaten gezeigt – gibt es nicht. Jede Sicherheitsmaßnahme für sich kann im konkreten Einzelfall möglicherweise der Schlüssel für eine erfolgreiche Abwehr sein. Es gilt, nicht nur potentielle Löcher zu stopfen, sondern das Thema Informationssicherheit auch konzeptionell in den Blick zu nehmen. Aber wie lässt sich eine systematische Informationssicherheit garantieren?

Eine Konzertierung geeigneter Maßnahmen kann mit Hilfe eines bewährten Vorgehensmodells erreicht werden. Hinter dem Begriff „ISMS" verbirgt ist ein umfassendes, ganzheitliches und standardisiertes Managementsystem, mit dessen Hilfe die Definition, Steuerung, Kontrolle, Wahrung und fortlaufende Optimierung der Informationssicherheit im Unternehmen erreicht werden soll. Der Fokus liegt also zunächst nicht auf der Umsetzung einzelner Maßnahmen, sondern es wird ein strukturierter Ansatz gewählt.

Das Rad nicht neu erfinden

Die allgemeine Vorgehensweise dürfte für Unternehmen der Pflegebranche durchaus vertraut sein. Ein Sicherheitskonzept wird üblicherweise anhand des PDCA-Zyklus aufgebaut, um die kontinuierliche Betrachtung von Risiken und Maßnahmen gewährleisten zu können.

Viele Konzepte und Orientierungshilfen gibt es frei verfügbar im Netz: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat beispielsweise die IT-Grundschutz-Kataloge veröffentlicht, die insgesamt gesehen einen großen Umfang haben und die Möglichkeiten sozialer Organisationen bei einer flächendeckenden Implementierung sprengen dürften. Dennoch finden sich hier für ausgewählte Maßnahmen wertvolle Hinweise und Arbeitshilfen, die für sich genommen sehr gute Leitfäden bei der Implementierung darstellen. Eine Auseinandersetzung mit dem Thema lohnt sich auf jeden Fall: Ab 25. Mai 2018 gelten die Datenschutz-Grundverordnung und neue Gesetze zum kirchlichen Datenschutz. Mit von der Partie sind Forderungen nach der Implementierung eines wirksamen IT-Sicherheitsmanagements (vgl. Art. 32 Abs. 1 DSGVO). Damit dürften die Folgen von Cyberattacken bei Versäumnissen in der Prävention möglicherweise auch bußgeldbewährt werden.

Der Autor ist Geschäftsführer der Althammer & Kill GmbH & Co. KG. Zusammen mit seinem Team begleitet er bundesweit Einrichtungen in Pflege und Sozialwesen als externer Datenschutzbeauftragter und berät zu Fragen der Informationssicherheit.

STICHWORT VERSCHLÜSSELUNGSTROJANER

Verschlüsselungstrojaner wie WannaCry oder Locky nutzen Sicherheitslücken aus, um die Festplatte des Computers und erreichbare Netzlaufwerke zu verschlüsseln. Damit können die Anwender dann nicht mehr auf ihre Dateien und Datenbanken zugreifen. Abhilfe schafft nur eine komplette Säuberung des Systems mit anschließender Wiederherstellung der Datensicherung. Falls dies nicht gelingt, kann alternativ die Zahlung eines Lösegeldes zur Entschlüsselung der Dateien gewählt werden. Davon raten Behörden natürlich ab, in manchen Fällen ist es aber der letzte Ausweg, um einen kompletten Datenverlust zu vermeiden, zum Beispiel, weil eine funktionierende Datensicherung nicht vorliegt.

PLANUNG IT-SICHERHEITSKONZEPT

Planung
- Klassifikation von Risiken und möglicher Schäden
- Durchführung einer Risikobewertung
- Auswahl von Sicherheitsmaßnahmen, Konzepterstellung

Umsetzung
- Realisierungsplan für ein IT-Sicherheitskonzept
- Umsetzung, Überwachung und Steuerung der Sicherheitsmaßnahmen
- Schulung und Sensibilisierung der Mitarbeitenden

Überwachung
- Erkennen von Sicherheitsvorfällen im laufenden Betrieb
- Überprüfung der Einhaltung und Wirksamkeit von Vorgaben
- Durchführung von Penetrationstests und simulierten Hacking-Angriffen

Optimierung
- Beseitigung von Fehlern
- Verbesserung von Sicherheitsmaßnahmen

Lebenszyklus eines IT-Sicherheitskonzepts nach dem PDCA-Modell. Grafik: Althammer-Kill