KRANKENHÄUSER

SEHR ANFÄLLIGE SYSTEME FÜR CYBER-ANGRIFFE

Marco Genovese
Product Manager,
Stormshield

Es ist ein Paradox, das Angst machen kann: Obwohl Vertrauen im Zentrum der Beziehung zwischen einem Krankenhaus und seinen Nutzern steht, haben laut der Plattform Orange Cyberdefense und Orange Healthcare 80% der Gesundheitsorganisationen zwischen 2016 und 2018 einen erfolgreichen Angriff erlitten. Wie kann man diese Anfälligkeit erklären und wie kann man hier Abhilfe schaffen?

DIE DATEN UND IHRE WICHTIGKEIT MACHEN AUS KRANKENHÄUSERN EIN ZIEL ERSTER KLASSE

Gesundheitsstrukturen verarbeiten hochvertrauliche Daten von Patienten und ziehen so Hacker an. **Ransomwares, Dienstverweigerungseingriffe, „Medjack“ oder auch Botnets**: Alle diese Mittel werden verwendet, um den Zugang zu diesen vertraulichen Informationen zu beeinträchtigen oder zu erlangen. Aber Daten sind nicht der einzige Beweggrund der Cyber-Angreifer. Denn wenn sie die Aktivitäten dieser Einrichtungen, in denen Leben auf dem Spiel stehen, unterbrechen können, ist dies die perfekte Möglichkeit Krankenhäuser zu erpressen und so ihre Ziele zu erreichen.

MENSCHLICHE UND STRUKTURELLE FAKTOREN ALS URSPRUNG DER BRANCHENSPEZIFISCHEN ANFÄLLIGKE

Wie lässt es sich erklären, dass so angreifbare Systeme – die bekannterweise bedroht werden – immer noch so angreifbar bleiben? Durch eine Mischung aus unterschiedlichen Versäumnissen.

Die Durchlässigkeit der Netzwerke an vorderster Front

Es ist keine Seltenheit, dass Krankenhäuser über mehrere Netzwerke mit unterschiedlichen Vertraulichkeitsebenen verfügen. Es ist zum Beispiel sehr einfach, sich über einen **WLAN-Hotspot** mit dem Patientennetz zu verbinden. Und vor dort aus kann man in das medizinische Netzwerk und dann in das Verwaltungsnetz eingreifen. Ein Segmentierungsfehler, der eine erste Schwachstelle ergibt, die von den Hackern ausgenutzt wird.

Kontinuität ist Priorität

Krankenhäuser und andere Gesundheitsorganisationen sind dazu verpflichtet, ununterbrochen Dienstleistungen bereitzustellen. Das bedeutet konkret, dass sie es sich nicht erlauben können, ihre Dienstleistungen zu unterbrechen. Wenn sich ihre Informatikinfrastruktur weiterentwickelt, kümmern sich deshalb nur wenige um die Wartung oder darum, dass die Geräte, wenn auch nur kurz, ausgeschaltet werden. Diese Arbeitsweise führt häufig dazu, dass sie die alten Methoden nicht hinterfragen und das Informationssystem nicht als globales Projekt mit eigener Verwaltung sehen. Ein praktisches Fallbeispiel: Beobachten Sie bei Ihrem nächsten Krankenhausbesuch **die verwendeten Browser oder Anwendungen.** In einem Bericht von Le MagIT, dem nationalen britischen Audit-Büro, hat das nationale Rechnungsprüfungsamt (NAO) die Auswirkungen von WannaCry auf das britische nationale Gesundheitssystem (NHS) untersucht. Es hieß: *„Der Großteil der virusverseuchten Ausstattung des NHS läuft auf Windows 7 und es wurden keine Patches angewandt*". Die Situation wird umso dringlicher, da gleichzeitig im Alltag häufig grundlegende Sicherheitsmaßnahmen vergessen werden. Dazu gehört zum Beispiel das Schließen seiner Sitzung, wenn man seinen Arbeitsplatz verlässt. So kann man weiterhin auf die Informationen in der Patientenakte zugreifen und hat möglicherweise auch administrativen Zugang.

Wenig interne Experten für Cybersicherheit

Abgesehen von diesen Schwachstellen in der Handhabung fehlt es in vielen Gesundheitseinrichtungen auch einfach an Experten für IT-Sicherheit. Doch diese Phase sollte bald schon der Vergangenheit angehören, denn die Branche unternimmt beträchtliche Anstrengungen, um den Rückstand aufzuholen. In Frankreich fand Anfang Oktober das Symposium des **Verbands für die Sicherheit der Informationssystemen im Gesundheitsbereich** (APSSIS) statt, bei dem erkennbar war, dass dieses Thema in den Debatten der Gesundheitseinrichtungen an Schwung gewinnt.

Die gängige, aber nicht kontrollierte Gepflogenheit BYOD

Ein anderer Faktor, der die Anfälligkeit der Krankenhäuser verstärkt, ist direkt mit der Arbeitsweise der Ärzte verbunden: Viele teilen ihre Zeit zwischen einer privaten Arztpraxis und einem Krankenhaus auf und verwenden dafür denselben Computer und dasselbe Smartphone. Die Geräte, die sie nicht vom Krankenhaus erhalten, erfüllen nicht immer alle Sicherheitsregeln des Krankenhauses.

Neue medizinische Technologien mit geringem Sicherheitslevel

Die wichtigsten Krankenhäuser verwenden immer häufiger vernetzte medizinische Geräte. Doch der Sicherheitsaspekt wird beim Entwurf dieser Geräte noch nicht wirklich berücksichtigt, wie ***ein Sprecher von „Medjack" behauptet.***

Generalisierung der Systeme für technisches Gebäudemanagement

Die Systeme für technisches Gebäudemanagement ermöglichen unter anderem die Fernsteuerung von Geräten wie Klimaanlagen, Feuermeldern oder Fahrstühlen. Durch das Hacken eines solchen Geräts kann man beispielsweise die Evakuierung eines Krankenhauses erzwingen. Diese Systeme werden entsprechend den *„physischen"* Sicherheitsstandards entworfen und sind für die digitale Sicherheit nicht ausreichend ausgestattet.

WIE KÖNNEN KRANKENHÄUSER IHRE WIDERSTANDSFÄHIGKEIT GEGEN CYBER-ANGRIFFE STÄRKEN?

Die erste Maßnahme ist die **Bewusstseinsschärfung für die Angreifbarkeit dieser Gesundheitsstrukturen und das Thema Cybersicherheit muss eine Priorität der Organisation werden.** Hierzu gehören auch die entsprechenden Investitionen (Personal, Organisation, Geräte, spezifisches Budget usw.).

Lösungen für die Netzwerksicherheit und zertifizierte und qualifizierte Geräte nutzen

Konkret gesagt, müssen auf jeden Fall Lösungen verwendet werden, die die Arbeitsplätze und das Netzwerk sichern, sodass sie gegen Eindringlinge geschützt sind und die Kontinuität der Dienstleistungen garantieren können. Diese Lösungen müssen verpflichtend für alle Geräte sein, die für die Behandlung der Patienten verwendet werden, egal ob sie der Einrichtung gehören oder nicht.

Das Personal sensibilisieren

Damit das Gesundheitspersonal davon überzeugt werden kann, bewährte Praktiken im Bereiche Cybersicherheit anzuwenden, muss man regelmäßig auf die Herausforderungen hinweisen und die Verfahren gemeinsam mit dem Personal durchgehen. In diesem Sinne arbeitet die Kooperationsgemeinschaft E-Gesundheit im Departement Pays de la Loire (GCS) gemeinsam mit Orange Cyberdefense an der Ausarbeitung eines **Escape Game mit dem Namen Sant'escape – Digitale Sicherheit.** Das Prinzip? Die bewährten Verfahren in der Gesundheitsbranche werden spielerisch erklärt und müssen dann angewendet werden!

Vorfälle der Regionalen Gesundheitsagentur (ARS) melden

IIn Frankreich sind die Gesundheitseinrichtungen verpflichtet, alle Vorfälle oder Verdachtsfälle gesundheitlicher Natur oder im Bereich Cybersicherheit auf einem von der Regierung zur Verfügung gestellten **Portal** zu melden. Die regionalen Gesundheitsagenturen sind anschließend dafür zuständig, diese Informationen an die *„Begleitung für Cybersicherheit für Gesundheitseinrichtungen"* (ACSS) weiterzugeben. Dieser nationale Hilfemechanismus wurde von der französischen Agentur für digitale Sicherheit (ASIP) ins Leben gerufen und sorgt nicht nur für eine bessere Nachverfolgung, sondern arbeitet auch Empfehlungen aus.

Die Krankenhäuser und die gesamte Gesundheitsbranche allgemein müssen heute ihre Kosten reduzieren und zugleich alle digitalen Möglichkeiten ausschöpfen, wie beispielsweise **neue Dienste für die Telemedizin.** Doch das Sicherheitsdefizit ihrer Informationssysteme könnte einen besonders hohen Preis für die Vertraulichkeit und die Sicherheit der Patienten darstellen. Jedenfalls so lange die Cybersicherheit keine vollwertige Priorität im Gesundheitsbereich wird.