

IT-SICHERHEIT BEI SYNEDRA

SYNEDRA Im November 2018 ließ das in Österreich ansässige Medizin-IT-Unternehmen synedra erstmals zwei seiner Produkte mithilfe eines sogenannten Penetrationstests auf ihre IT-Sicherheit und mögliche Sicherheitslücken hin überprüfen. Beauftragt wurde zu diesem Zwecke eine Sicherheitsfirma aus Deutschland, die synedra ein durchwegs positives Zeugnis im Bereich Cyber Security ausstellen konnte. **Stefan Andreatta**, Chief Technology Officer bei synedra, über die Hintergründe und Ergebnisse des Pen-Tests sowie über das steigende IT-Sicherheitsbewusstsein im Medizinbereich.

synedra entwickelt seit beinahe 15 Jahren Softwarelösungen für Gesundheitseinrichtungen. Welche Gründe gab es für synedra, nun erstmals einen Penetrationstest zu beauftragen, und welche Produkte wurden dabei getestet?

Für uns gab es zwei wesentliche Aspekte, die uns zur Beauftragung eines Penetrationstests bewogen haben: Erstens haben wir den Anspruch, unsere Produkte sicherheitsbewusst zu entwickeln. Dass wir die nötige Kompetenz dafür mitbringen, haben wir in den letzten Jahren bei zahlreichen Kundeninstallationen unter Beweis stellen können. Allerdings stoßen wir als ein auf Softwareentwicklung spezialisiertes Unternehmen auch an gewisse Grenzen. Eine Firma, die sich ausschließlich mit Cyber Security befasst, hat andere Werkzeuge zur Verfügung und weiß im Allgemeinen mehr über das Thema IT-Sicherheit. Zweitens ist es für den Angriff auf eine Software notwendig, eine andere Perspektive einzunehmen. Als Softwarehersteller versucht man zwar, seine eigene Arbeit kritisch zu beleuchten, so viele Angriffsszenarien wie möglich in Betracht zu ziehen und für diese Szenarien eine entsprechende Absicherung einzubauen. Interessant sind aber jene Angriffsszenarien, an die man selbst, als Schöpfer der Software, nicht gedacht hat. Die Software bewusst aus einer anderen Perspektive zu betrachten bzw. betrachten zu lassen, ist also sehr hilfreich.

Bei diesem ersten von uns beauftragten Penetrationstest ließen wir

unsere beiden Webapplikationen synedra Web und synedra Web Patient auf Herz und Nieren prüfen. Während synedra Web als Zuweiserportal konzipiert wurde, stehen in synedra Web Patient den Patientinnen und Patienten ihre medizinischen Bilder und Dokumente zur Verfügung. Da die beiden Portale für die externe Bild- und Befundverteilung im Internet laufen und somit auch von außerhalb des Krankenhauses erreichbar sind, ist es umso wichtiger, sie vor Angriffen zu schützen.

Welche Ergebnisse lieferte der Penetrationstest und wie bewertet synedra selbst die Resultate der Sicherheitsfirma?

Nach fünf Tagen intensiven Testens – angefangen bei Cross-Site-Scripting und SQL-Injection über Passwortstruktur und -qualität bis hin zu Session-ID und Zugriffsschutz – konnte die externe Firma keine kritischen Sicherheitslücken bei unseren Webapplikationen identifizieren. Eine als hoch eingestufte Schwachstelle ergab sich aus einem Konfigurationsfehler auf dem für den Penetrationstest zur Verfügung gestellten Testsystem. Die übrigen als mittel und niedrig eingestuft Schwachstellen hat synedra alle adressiert beziehungsweise bereits behoben. So waren auf dem Testsystem beispielsweise triviale Passwörter erlaubt, also leicht zu erratende Zahlen- oder Ziffernfolgen oder die Eingabe des Benutzernamens als Passwort. Sowohl synedra Web als auch synedra Web Patient können jedoch

so konfiguriert werden, dass die Passwortkomplexität entweder beim Setzen des Passworts oder bei jedem Login geprüft wird. Entspricht das von der Benutzerin/vom Benutzer eingegebene Passwort nicht den Kriterien, dann wird sie/er dazu aufgefordert, ein komplexeres Passwort zu wählen. Hinsichtlich der Passwortkomplexität hält sich synedra übrigens an den NIST-Standard, der gute und zielgerichtete Kriterien für die Passwortsicherheit liefert.

Alles in allem hat sich der Penetrationstest für synedra bezahlt gemacht: Wir konnten dadurch unsere Kompetenz erhöhen, unseren Blick schärfen und konkrete Sicherheitsprobleme beheben, und somit generell die Sicherheit unserer Produkte steigern.

Welche Maßnahmen ergreift synedra über den Penetrationstest hinaus, um IT-Sicherheit für die eigenen Kunden zu gewährleisten?

Prinzipiell agiert synedra auf drei Sicherheitsebenen: Da wäre erstens die Verschlüsselung des Netzwerkverkehrs, die eine zentrale Rolle spielt. Der gesamte Verkehr zwischen unseren Klienten-Applikationen und unserem Backend ist verschlüsselt. Auch für alle Kontakte zu externen Systemen bietet synedra Verschlüsselungsmöglichkeiten an.

Die zweite Ebene ist die Authentifizierung. Zugriffe auf das System finden prinzipiell in einem persönlich authentifizierten Kontext statt. Dabei spielt neben der bereits erwähnten Passwortkomplexität die Zwei-Faktor-



Sicherheit wird bei synedra IT großgeschrieben.

Authentifizierung eine immer größere Rolle.

Der dritte Aspekt ist das Auditing. Beim Auditing geht es vor allem um die Nachvollziehbarkeit durchgeführter Aktionen. Nachdem sich eine Nutzerin/ein Nutzer an einem System angemeldet hat, kann sie/er prinzipiell auf die Daten in diesem System zugreifen. Diese Datenzugriffe werden aufgezeichnet, wodurch ein zusätzlicher Sicherheitsgewinn erzielt wird. synedra setzt beim Auditing übrigens komplett auf IHE-Integrationsprofile und den DICOM-Standard.

Wie ist das Thema IT-Sicherheit im Medizinbereich generell zu beurteilen?

Das Sicherheitsbedürfnis in der Medizin-IT nimmt schon seit längerer Zeit

extrem zu. Man denke nur an diverse Vorfälle der letzten Jahre, bei denen Krankenhäuser für ihre Daten Lösegeld zahlen oder ihren Betrieb stilllegen mussten. Dadurch ist auch das Bewusstsein für das Thema Sicherheit im Gesundheitsbereich gestiegen. Als Unternehmen fanden wir uns noch vor einigen Jahren häufiger in der Situation, dass unsere Sicherheitsvorstellungen und unser Sicherheitsbedürfnis für unsere Produkte mit den Vorstellungen der Kunden nicht immer kompatibel waren. Allerdings – und das ist die gute Nachricht – schreiben sich nun immer mehr Krankenhäuser das Thema IT-Sicherheit auf die Fahnen.

synedra



information technologies

SYNEDRA IT GMBH

Feldstraße 1/13, 6020 Innsbruck, Österreich

Tel.: +43-(0)512-581505

E-Mail: office@synedra.com

www.synedra.com
