

INTERVIEW

IT-Sicherheit im Gesundheitswesen und in der MedTech-Branche: Gefahren und Lösungsansätze



Die SySS GmbH wurde 1998 von Diplom-Informatiker Sebastian Schreiber gegründet, um hochwertige Sicherheitstests anzubieten. Gegenwärtig beschäftigt die SySS GmbH rund 160 Mitarbeiterinnen und Mitarbeiter, von denen sich über 110 ausschließlich mit Sicherheitstests beschäftigen. 2022 belief sich der Umsatz auf 20 Mio. Euro. Kunden der SySS GmbH sind Unternehmen aller Branchen und Größen.

Interview mit SySS-Geschäftsführer Sebastian Schreiber, SySS Expert IT Security Consultant Wolfgang Zejda und SySS Senior IT Security Consultant Tobias Jäger

Im September 2020 wurde das Universitätsklinikum Düsseldorf Opfer eines erfolgreichen Cyberangriffs. Hacker verschlüsselten auf einmal 30 Server, das Krankenhaus musste sich von der Notfallversorgung abmelden und Operationen absagen. Ihre Erpressung zogen die Täter zwar zurück, nachdem klar war, wessen Systeme sie da genau lahmgelegt hatten – das Unheil war jedoch nicht mehr aufzuhalten. Der Fall zeigt zweierlei: Cyberangriffe mit Lösegeldforderungen werden immer häufiger und gerade bei kritischen Infrastrukturen wie dem Gesundheitssektor können die möglichen Folgen sogar Menschenleben kosten. Herr Schreiber, was sind die Gründe für diese Entwicklung?

➤ Sebastian Schreiber: Ursächlich ist, dass wir auf der einen Seite eine komplexer werdende IT-Umwelt haben. Wir verlassen uns mit der zunehmenden Digitalisierung immer mehr darauf, Daten auch elektronisch verarbeiten zu können. Zum anderen ist es so, dass die Systeme, welche die Daten verarbeiten, immer feinmaschiger vernetzt werden. Dies erschwert eine Separation der einzelnen kritischen Systeme zunehmend. Außerdem ist das Geschäftsmodell der Kriminellen, die Erpressung von Lösegeld durch Kryptoransomware sehr erfolgreich, weil sie mit geringem Entdeckungsrisiko für die Täter und mit wenig Aufwand vonstattengeht.

Wie können Verantwortliche dieser Bedrohung begegnen?

➤ Sebastian Schreiber: Der erste Schritt ist, das Gewicht dieser Entwicklung überhaupt zu erkennen. Derartige Angriffe können Unternehmen jedweder Branche essentiell gefährden. Das muss den Verantwortlichen und den Aufsichtsorganen bewusst sein. Eine Klinik darf sich schlicht nicht hacken lassen. Die einzige Möglichkeit, das zu kontrollieren, ist die Durch-

führung von simulierten Cyberangriffen, sogenannten Penetrationstests.

Herr Zejda, Sie führen solche Penetrationstests durch, häufig auch in Kliniken. Was sind die Besonderheiten von Tests in Krankenhäusern?

➤ Wolfgang Zejda: Im Prinzip laufen Tests in Kliniken ähnlich ab wie bei anderen Unternehmen. Alle operativen Betriebe haben eine klassische IT (Anwendungscomputer, Server, Drucker etc.) und eine operative IT. Bei Kliniken sind dies meist medizinische Geräte.

Generell unterscheiden wir bei internen Tests zwei Hauptszenarien. Das erste Szenario ist das „Reinigungspersonalszenario“. Hier versuchen wir uns mit eigenen Geräten technisch Zugang zum Netz zu verschaffen, so wie es z. B. Reinigungskräfte oder Patient könnten. Im einfachsten Fall können wir uns direkt anschließen und bekommen eine IP-Adresse, mit der wir am Netz teilnehmen können. In den komplizierteren Fällen müssen wir erst noch einen Netzzugangsschutz umgehen. Anschließend überprüfen wir die Netzstruktur und die angebotenen Dienste.

Im zweiten Szenario – dem „Praktikantenszenario“ – erhalten wir einen normalen Account, wie ihn die Beschäftigten haben. Damit können wir uns dann normal anmelden und verschaffen uns einen Überblick über die – meist – Windows „Active Directory“-basierte Umgebung. Zum Beispiel prüfen wir, welche Accounts (Nutzer wie Maschinen) welche Rechte haben. Auch ein Blick auf die Freigaben lohnt sich meist, da dort immer wieder Passwörter hinterlegt sind. Auch die Softwareverteilung ist oft ein lohnendes Ziel.

Die Schwachstellen, die wir finden, sind meist vielfältig: eine flache, historisch bedingte Netz-

struktur, nicht scharfe Firewalls zwischen den Netzen sowie Standard- oder triviale Zugangsdaten.

Gibt es Probleme, die Sie speziell in Krankenhäusern bzw. bei medizinischen Geräten vorfinden?

- Wolfgang Zejda: Ja. Insbesondere sind veraltete Systeme in Kliniken ein großes Problem. Teure Maschinen werden einmalig angeschafft und können bzw. dürfen (aufgrund der Medizinproduktezertifizierung) nicht „einfach so“ aktualisiert werden. Auch sind viele medizinische Protokolle – beispielsweise für die medizinische Bildübertragung – historisch unverschlüsselt und werden erst nach und nach umgestellt. Hier ist auch zu überlegen, was passiert, wenn z. B. die Zertifikate auslaufen, wie es bei der Telematikinfrastruktur für Ärzt von der Gematik der Fall war.

Außerdem sind Passwörter ein schwieriges Thema in Kliniken. Obwohl die Daten der Patient sehr schutzbedürftig sind, treffen wir immer wieder die Situation an, dass nur sehr ungern starke Passwörter gewählt oder überhaupt Rechner gesperrt werden. In gewisser Hinsicht ist das verständlich: Besonders im Notfallbetrieb wollen Mediziner schnellstmöglich arbeiten können, ohne sich vorher anmelden zu müssen. Hier ist eine Sensibilisierung für die – durchaus ebenfalls lebensbedrohlichen – möglichen Folgen mangelnder IT-Sicherheit erforderlich; dann muss die eine Gefahr mit der anderen gewissenhaft abgewogen werden.

Lassen Sie uns einen genaueren Blick auf die Sicherheit von Medizinprodukten werfen. Herr Jäger, Sie haben als Experte für Embedded Security viel mit Medizinprodukten zu tun. Worin sehen Sie die besonderen Herausforderungen beim Einsatz solcher Geräte im Hinblick auf die Sicherheit?

- Tobias Jäger: Eine besondere Herausforderung stellt die Tatsache dar, dass die Geräte in einem Spannungsfeld stehen zwischen der Verarbeitung hochsensibler (Patienten-)Daten, einer absoluten Ausfallsicherheit und dem Betrieb in

einer halböffentlichen Umgebung. Denken wir an ein Patientenzimmer: dort sind die Patient – und ggf. deren Besucher – durchaus auch längere Zeit mit den Medizinprodukten alleine. Zudem haben die medizinischen Geräte einen Lebenszyklus von vielen Jahren, d. h. ihre Sicherheit muss über viele Jahre hinweg gewährleistet werden.

Können Sie von einem konkreten Test berichten?

- Tobias Jäger: In einem Projekt sollten wir sicherstellen, dass einzelne Mitarbeiter der Krankenhäuser die Medizinprodukte bzw. die Verbrauchsteile nicht manipulieren und dadurch die Ausfallsicherheit gefährden können. Es ist nämlich tatsächlich vorgekommen, dass Änderungen an Geräten vorgenommen worden sind, um Kosten zu sparen. Und hier muss die Haltung ganz klar sein, dass Sicherheit oberste Priorität hat.

Was empfehlen Sie Medizintechnikunternehmen, insbesondere den Herstellern von Medizinprodukten, damit diese technisch „auf der sicheren Seite“ sind?

- Tobias Jäger: Meine erste Empfehlung lautet: Reduzieren Sie die Angriffsfläche, vor allem in Richtung Netzwerkschnittstellen. Wichtig ist aber auch die physische Absicherung, z. B. sollten alle Speichermedien verschlüsselt werden, außerdem sollte Secure Boot aktiviert sein und alle Debug-Schnittstellen sollten deaktiviert werden. Zentral ist auch ein fester Updateprozess, sodass das Einspielen aktueller Updates gewährleistet ist.

Bei der Auswahl der Software sollte auf den Lebenszyklus geachtet werden. Hier ist die Frage zu stellen, ob ein Betriebssystem überhaupt so lange mit Sicherheitsupdates unterstützt wird, wie das betreffende Gerät planmäßig eingesetzt werden soll. Darüber hinaus sollte man zu einem frühen Zeitpunkt in der Entwicklung über Fernwartung nachdenken und für diese Zwecke ein sinnvolles Konzept ausarbeiten.

Liebe Experten, herzlichen Dank für diese Einblicke!



➤ **Sebastian Schreiber**
Gründer und
Geschäftsführer



➤ **Tobias Jäger**
Senior IT Security
Consultant



➤ **Wolfgang Zejda**
Expert IT Security
Consultant