Torsten W. Remmerbach
Chefredakteur Oralchirurgie Journal

Cyberangriff: Erbeutete Patientendaten als Waffe

Hacker dringen immer häufiger in den Computernetzwerken von Krankenhäusern und anderen gesundheitsrelevanten Organisationen ein. Nicht nur große Maximalversorger, wie z. B. das Universitätsklinikum in Düsseldorf, wurden Ziel eines Cyberangriffs, sondern auch kleinere Krankenhäuser sowie Arzt- und Zahnarztpraxen. Oftmals geht es den Kriminellen darum, Daten auf den Klinikservern oder Praxiscomputern zu verschlüsseln und anschließend eine Art Lösegeld für die Freigabe zu verlangen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte die Schuldigen an der Düsseldorfer Uniklinik schnell benannt: Der einfache Grundschutz hätte gereicht – so der BSI-Präsident Arne Schönbohm – den Hackerangriff abwehren zu können. Das Amt hatte nach eigenen Angaben bereits im Januar 2020 vor einem Problem mit den weitverbreiteten Produkten der US-amerikanischen Firma Citrix gewarnt.

Der sogenannte „SolarWinds-Hack" gilt als größter Hacking-Angriff seit Jahren. Bei der Firma SolarWinds handelt es sich um einen US-Dienstleister für Softwarelösungen für das IT- und Netzwerkmanagement. So wurde an mehr als 18.000 Kunden ein kompromittiertes System verkauft, was unbemerkt bei dem entsprechenden Kunden Zugriffe auf das System erlaubte. Die Liste der betroffenen Firmen wächst täglich: Nationale Verwaltung für Nukleare Sicherheit in den USA, Softwareentwickler wie Microsoft oder VMware gehören zu den Opfern ebenso wie Equifax, die Wirtschaftsprüfer von Deloitte sowie Firmen wie Nvidia, Belkin, Intel und Cisco. Ferner werden Plattformen der Firma SolarWinds in deutschen Behörden eingesetzt.

Besonders perfide ist ein Hackerangriff auf das größte finnische Psychotherapiezentrum Vastaamo. Hier wurden im großen Ausmaß Krankenakten geraubt und die Patientendaten für jeden lesbar im Internet verbreitet.

Kommen wir nun zu der alles entscheidenden Frage: Wie sicher sind Ihre Server in Ihrer Praxis? Können Sie sich auf Ihren IT-Spezialisten verlassen? Wer trägt die Verantwortung, wenn Patientendaten von Ihrem Server geklaut und im Internet verbreitet werden?

Die Aufsichtsbehörde des finnischen Gesundheitssystems musste einräumen, dass aufgrund von Sparmaßnahmen nur eine Person mit den Vorfällen zur Cybersicherheit beschäftigt war – und diese nur auf Nachfrage tätig wurde. In Deutschland sieht es wahrscheinlich nicht besser aus – ganz im Gegenteil.

[Infos zum Autor]

Ihr Torsten W. Remmerbach