CYBERANGRIFFE GIBT ES

dutzende Male täglich!

Cybersecurity-Experte **Michael Punz (x-tention)** spricht im Interview für die Online-Plattform INGO (Innovation. Gesundheit.Oberösterreich, ingo-news.at) über die erhöhte Gefährdung von Krankenhäusern und die Herausforderung durch den Faktor Mensch.

Sind die Krankenhausbetreiber in Österreich im Bereich Cybersicherheit gut aufgestellt, wie ist die Awareness für dieses Thema?

Michael Punz: Informationssicherheit hat sich von einem Nischen- zu einem Hauptthema entwickelt. Noch vor einigen Jahren musste immer wieder mal erläutert werden, warum eine Investition in Informationssicherheit notwendig ist. Das hat sich in letzter Zeit stark verändert, auch dank gesetzlicher Vorgaben wie DSGVO und NISG sowie umfassender medialer Berichterstattung. Informationssicherheit ist mittlerweile ein fixes Thema in jedem Krankenhaus. Es ist ja auch unausweichlich, sich damit auseinanderzusetzen – und das de facto jeden Tag, weil sich die Bedrohungen laufend verändern. Wer heute nicht in Informationssicherheit investiert, wird schon morgen davon eingeholt werden.

Wie oft sind Sie mit Angriffen auf Krankenhaus-IT konfrontiert?

Angriffe finden laufend statt, Dutzende Male täglich. Der absolute Großteil wird aber bereits bei den zentralen Sicherheitskomponenten, z. B. bei der Firewall, abgefangen. Wichtig ist ein mehrschichtiges Sicherheitskonzept, denn Sicherheit besteht nicht aus einer einzigen Maßnahme, sondern aus dem Zusammenspiel vieler verschiedener Maßnahmen an unterschiedlichen Stellen. Trügerischer sind Angriffe, die gar nicht als solche wahrgenommen werden, wie sogenannte „Social Engineering"-Angriffe, wo der Mensch selbst angegriffen bzw. getäuscht wird und dies oft nicht mitbekommt. Das reicht vom unabsichtlichen Verraten von vertraulichen Informationen bis zum Aufhalten von Türen zu Sicherheitsbereichen. Krankenhäuser sind da überdurchschnittlich gefährdet, weil es keinen Zaun gibt und Mitarbeiter, Patienten und Dritte gleichermaßen sich fast uneingeschränkt bewegen können.

Welche speziellen Sicherheitsanforderungen sind für Sie im Krankenhausbereich am wichtigsten?

Schulung, Schulung und nochmals Schulung! Mitarbeiter müssen verstehen, warum bestimmte Sicherheitsvorgaben einzuhalten sind – immerhin arbeiten sie jeden Tag mit vertraulichen Gesundheitsdaten. Nur ein Beispiel: Egal, wie viele technische Sicherheitsmaßnahmen im Krankenhaus ergriffen wurden, am Ende des Tages muss entschieden werden, ob und welche Gesundheitsdaten dem Mitarbeiter am Bildschirm angezeigt werden. USB-Sticks und E-Mails lassen sich technisch unterbinden. Aber ein Mitarbeiter muss auch verstehen, dass er nicht mit seinem privaten Smartphone den Bildschirm mit Gesundheitsdaten abfotografieren und in sozialen Netzwerken veröffentlichen darf. Die Technik hat einfach ihre Grenzen. Umgekehrt führen aber auch umfassende organisatorische Sicherheitsvorgaben, die zwar dokumentiert, aber kaum bekannt sind, nicht zum gewünschten Sicherheitsniveau. Am zielführendsten ist ein guter Mix von technischen und organisatorischen Maßnahmen in Kombination mit einem passenden Schulungskonzept für alle Mitarbeiter – und zwar wirklich alle.

Wo sehen Sie die größten Gefahren bzw. Schwachstellen – interne Systeme, medizinische Geräte, Mitarbeiter?

Wie gesagt ist der Faktor Mensch eine große Herausforderung für jede Organisation, denn er neigt grundsätzlich dazu, den Weg des geringsten Widerstandes zu gehen und Sicherheitsvorgaben manchmal „zu seinen Gunsten" auszulegen. Zudem ist Informationssicherheit ein verhältnismäßig neues Thema. Noch dazu ist es oft unangenehm, z. B. im Umgang mit Passwörtern, oder macht bestehende Prozesse aufwändiger, etwa durch erhöhte Dokumentations- und Freigabeanforderungen. Das Ziel muss daher sein, Informationssicherheit bestmöglich – und wenn irgendwie möglich transparent – in bestehende Prozesse zu integrieren sowie Verständnis und Akzeptanz für die Einhaltung der vorgegebenen Regelungen zu schaffen. Das erreicht man eben nur durch Schulung und durch das Vorleben der Regelungen durch die Vorgesetzten.

Wird die zunehmende Digitalisierung im Gesundheitswesen bzw. das „Internet of things" für die Cybersicherheit zum Problem? Reichen die bestehenden Normen dafür aus?

Vor allem die zunehmende Vernetzung von einzelnen Geräten führt zu großen Herausforderungen in der Informationssicherheit. Viele dieser Geräte, vor allem im medizinischen Bereich, dürfen nicht oder nur sehr aufwändig verändert – also auch nicht mit neuen Sicherheitsupdates versehen – werden. Wenn derartige Geräte mit der Außenwelt kommunizieren, sind spezielle und feingranulare Sicherheitsmaßnahmen notwendig. Grundsätzlich decken vorhandene Normen, wie ISO/IEC 27001, die Themen ab, behandeln diese aber nur aus einer „Vogelperspektive". Detailregelungen und vor allem die konkrete Interpretation des Stands der Technik sind immer wieder tagesaktuell neu einzuschätzen.

Sind Cloud-Lösungen für Krankenhäuser eine Option oder eher tabu?

Da ist meiner Meinung nach zu unterscheiden, um welche Art von Cloud es sich handelt. Eine Public-Cloud-Anbindung bedarf sicher einer sehr genauen und umfänglichen Einschätzung hinsichtlich Informationssicherheit und natürlich auch Datenschutz. In der Praxis sehen wir aber immer häufiger Private-Cloud-Lösungen, die im eigenen Rechenzentrum betrieben und Mitarbeitern und ausgewählten Externen, wie Projektmitarbeitern, zur Verfügung gestellt werden.

Das Interview führte Josef Haslinger (haslinger pr | 4925 Pramet | haslinger-pr.at)

Ihr Ansprechpartner bei x-tention

Michael Punz
Informationssicherheit & Datenschutz

mail michael.punz@x-tention.at
tel +43 7242 / 2155 - 6325
mobil +43 664 / 80009 6325

x-tention Informationstechnologie GmbH
Römerstraße 80A, 4600 Wels | x-tention.com