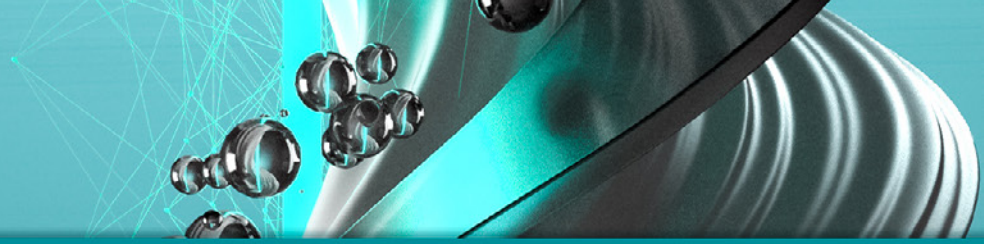
DER ZUSTAND DER IT-SICHERHEIT DEUTSCHER KLINIKEN IST VERBESSERUNGSWÜRDIG



ESET PROTECT

IT-SECURITY: EINFACH. SICHER. PASSGENAU.

Dr. Nicolas Krämer, 46 Jahre alt, Autor, Speaker und Krankenhausmanager. Als Geschäftsführer eines großen kommunalen Krankenhauses im Rheinland musste ich im Frühjahr 2016 erleben, wie es sich anfühlt, Opfer eines Hackerangriffs zu werden. Die Risiken und Nebenwirkungen der Digitalisierung wurden mir damals auf dramatische Art und Weise vor Augen geführt. In meinem spannenden Vortrag #angriffausderdunkelheit gehe ich auf unterhaltsame Art und Weise auf den Beipackzettel der Digitalisierung ein und beschreibe die Gefahren, die von fehlender Cybersicherheit ausgehen, sowie Lösungsansätze. Bekannt aus Funk und Fernsehen bin ich immer dann ein gefragter Berater und Gesprächspartner, wenn es um das Thema IT-Sicherheit geht, deren Verbesserung nicht nur im Gesundheitswesen mir eine Lebensaufgabe geworden ist.

Interview mit Dr. Nicolas Krämer

Kliniken geraten vermehrt ins Visier von Cyberkriminellen. Thorsten Urbanski von ESET Deutschland sprach mit Dr. Nicolas Krämer über den aktuellen Status in deutschen Krankenhäusern, über die Ursachen für die angespannte Bedrohungslage und über das Krankenhauszukunftsgesetz. Seit 2016 ist Nicolas Krämer ein gefragter Experte im Bereich IT-Sicherheit von Kliniken. Damals zeigte er sich als Krankenhausmanager des Lukaskrankenhaus Neuss, das 2016 Opfer eines Ransomware-Angriffs wurde, als hervorragender Krisenmanager.

Kliniken - wie zuletzt das Düsseldorfer Uniklinikum - werden immer häufiger zum Ziel von Cyberangriffen und das mit zum Teil fatalen Folgen. Wie bewerten Sie die aktuelle Lage?

Dr. Nicolas Krämer: Das Gesundheitswesen ist ohnehin schon die am häufigsten von Hackerangriffen betroffene Branche. Corona beschäftigt die Kliniken seit Anfang 2020, gegen die weltweite Pandemie der Computerviren kämpfen wir im Gesundheitswesen schon seit mehreren Jahren. Nun erleben die Häuser die Krise in der Krise, denn COVID-19 sorgt dafür, dass Online-sprechstunden und andere IT-Lösungen wie Bring-your-own-Device und Videokonferenzsysteme vermehrt zum Einsatz kommen. Bei der Implementierung der Lösungen wurde auf Schnelligkeit gesetzt. Die IT- und Datensicherheit standen nicht an erster Stelle. Der Hackerangriff auf die Düsseldorfer Uniklinik stellt einen weiteren traurigen Meilenstein in der Historie der Cyberattacken auf Krankenhäuser dar: Erstmals musste in der Folge eines Angriffs ein Patient sterben.

DER ZUSTAND DER IT-SICHERHEIT DEUTSCHER KLINIKEN IST VERBESSERUNGSWÜRDIG

Es zeigt sich, dass Krankenhäuser zum Teil mit erheblichen Defiziten in punkto IT-Sicherheit zu kämpfen haben. Auch das BSI sieht Handlungsbedarf. Wie schätzen Sie den Status in deutschen Kliniken ein?

Dr. Nicolas Krämer: Weltweit sind etwa 24,3 Millionen gestohlene Patientendatensätze frei im Internet erhältlich. Auch in Deutschland ist die Lage dramatisch. So wurden allein bei einem sicherheitsrelevanten Vorfall im Sommer 2019 mehr als 13.000 hochsensible Patientendatensätze mit mehreren Millionen medizinischen Bildern und personenbezogenen Daten „geleakt" und waren wochenlang ohne Kennwortschutz für alle im Netz verfügbar. Der Zustand der IT-Sicherheit in den deutschen Kliniken kann getrost als verbesserungswürdig bezeichnet werden. Das muss sich umgehend ändern. Die Uniklinik Düsseldorf war nach dem Cyberangriff knapp zwei Wochen von der Notfallversorgung abgemeldet und musste ihren Medizinbetrieb auf eine Minimalversorgung umstellen. Solche Ausfälle können wir uns aktuell in der zweiten Welle der Corona-Pandemie nicht leisten.

Wo liegen Ihrer Ansicht nach die größten Probleme in Krankenhäusern?

Dr. Nicolas Krämer: Medizintechnische Geräte werden häufig mit Windows XP betrieben, einem veralteten und unsicheren Betriebssystem. Und auch die IT-Sicherheitsinfrastruktur ist oft nicht ausreichend, um den mitunter perfiden Angriffstechniken standzuhalten. Eine wichtige Rolle spielt als auch der Faktor Mensch. Das Gegenteil von künstlicher Intelligenz ist menschliche Dummheit. In meinem Vortrag #angriffausderdunkelheit rate ich immer: „Investieren Sie nicht 10.000 Euro in eine weitere Firewall, investieren Sie besser 100.000 Euro in jemanden, der diese vernünftig bedient." Vom amerikanischen Krypto-Experten Bruce Schneier stammt der folgende Leitsatz: „Amateure hacken Systeme, Profis hacken Menschen". Beim Social Engineering werden psychologische Tricks angewendet, um Menschen zu etwas zu bewegen, was sie unter rationalen Umständen nicht tun würden, zum Beispiel ein Kennwort verraten. Auch bei einem leitenden Klinikmitarbeiter kann der Verstand aussetzen, wenn ihm per E-MAIL eine kostenlose VIP-Karte seines Lieblingsclubs angeboten wird. Leider ist die „Awareness" für IT-Sicherheit in den Köpfen vieler Krankenhausmitarbeiter noch nicht fest verankert. Das beginnt mit den Kennwörtern, die häufig leicht geknackt werden können, und hört mit Cyberversicherungen auf, die die meisten Geschäftsführer noch nicht für Ihre Kliniken abgeschlossen haben.

Sehen Sie Unterschiede zwischen großen Kliniken und kleineren Häusern? Was sind die spezifischen Probleme?

Dr. Nicolas Krämer: Die Unternehmensberatung Roland Berger stellte bereits 2017 fest, dass 64 Prozent der knapp 2.000 Krankenhäuser in Deutschland Opfer einer Hackerattacke geworden waren. Die Dunkelziffer dürfte noch höher liegen. Zu den Opfern gehören sowohl größere als auch kleinere Kliniken. Die Awareness hat nichts mit der Bettenanzahl zu tun. Trotzdem haben größere Einheiten und Verbundkrankenhäuser hinsichtlich der Cybersicherheit den Vorteil der Skalierbarkeit und eher die Möglichkeit, einen Mitarbeiter zu beschäftigen, der sich ausschließlich mit IT-sicherheitsrelevanten Fragestellungen auseinandersetzt.

Zu welchen Maßnahmen raten Sie Klinikverantwortlichen, die die Infrastruktur ihrer Häuser besser gegen Cyberangriffe absichern und das IT-Security-Niveau anheben wollen?

Dr. Nicolas Krämer: Quarantäne bewährt sich sowohl beim Verdacht einer Infektion mit COVID-19 als auch mit Computerviren. Neben Quarantänefiltern empfiehlt sich ein Sandbox-System, in dem verdächtige E-Mailanhänge geprüft und gegebenenfalls entschärft werden. Firewalls, Netzwerksegmentierungen und regelmäßige Datensicherungen sowie Patches sorgen

zusätzlich für Sicherheit. Empfehlenswert ist zudem die Beauftragung von sogenannten White-Hat-Hackern. Sie identifizieren im Rahmen von Penetrationstests Schwachstellen, die dann behoben werden können. Aber auch der Faktor Mensch muss in den Fokus genommen werden. Es ist essentiell den Mitarbeitern zu vermitteln, wie sichere Kennwörter aussehen und sie dafür zu sensibilisieren, keine Dienstgeheimnisse in den sozialen Medien zu posten. Diese Maßnahmen leisten einen Beitrag zu mehr Sicherheit.

Einen Impfstoff, der 100prozentig immun gegen Computerviren macht, wird es allerdings nie geben. Cybersicherheit gibt es nicht auf Rezept. Auch darf eine Klinik nicht handlungsunfähig werden, weil sie sich selbst durch ihre Sicherheitsmaßnahmen blockiert. Nehmen wir als Beispiel die Corona-App der Bundesregierung. Sie ist im Kampf gegen die Pandemie nahezu wirkungslos, weil bei ihrer Einführung den Prinzipien des Datenschutzes und der Freiwilligkeit eine höhere Bedeutung beigemessen wurde als der Gesundheit der Menschen.

Wie bewerten Sie das Krankenhauszukunftsgesetz? Inwieweit kann es mit dazu beitragen, dass IT-Sicherheit bei Digitalisierungsprojekten stets mitberücksichtigt wird?

Dr. Nicolas Krämer: Die Tatsache, dass das Gesundheitswesen die am häufigsten von Cyberangriffen betroffene Branche ist, hängt mit mehreren Faktoren zusammen, auch damit, dass Investitionen in IT-Sicherheit gemäß Krankenhausfinanzierungsrecht vom Staat finanziert werden müssen und der Staat dieser Verpflichtung in den letzten Jahren immer weniger nachgekommen ist. Nun stellen Bund und Länder im Rahmen des Krankenhauszukunftsgesetzes insgesamt 4,3 Milliarden Euro zur Verfügung, von denen mindestens 15 Prozent in die IT-Sicherheit der deutschen Kliniken gesteckt werden sollen. Dass bei diesem Gesetz nicht nur die Chancen der Digitalisierung, sondern auch ihre Risiken und Nebenwirkungen berücksichtigt werden, bewerte ich positiv.

Stand: März 2021

welivesecurity by ESET

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200