Ein Statement von Arved Graf von Stackelberg, Managing Director DRACOON

Zum Inkrafttreten der KRITIS-Verordnung im Gesundheitsbereich: Krankenhäuser müssen dringend handeln

Am 30. Juni dieses Jahres ist es soweit: Zahlreiche deutsche Kliniken müssen die KRITIS-Verordnung des BSI (Bundesamt für Sicherheit in der Informationstechnik) bis zu diesem Datum umsetzen. Das Gesetz umfasst insgesamt acht Branchen, die das BSI aufgrund des Betriebs kritischer Infrastrukturen als besonders angriffsrelevant und schützenswert ansieht. Unter den Begriff „Kritische Infrastrukturen" fallen schließlich Organisationen, die eine große Rolle für das staatliche Gemeinwesen spielen.

Wen genau das Gesetz betrifft, regelt die BSI-KRITIS-Verordnung (auch „Korb I" genannt) sowie die erste Änderungsverordnung (bekannt unter „Korb II"). Hier ist anhand transparenter Kriterien festgelegt, für welche Betreiber aus den Bereichen Energie, Wasser, Informationstechnik und Telekommunikation, Ernährung, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr Nachweispflichten gemäß BSI-Gesetz (§ 8a) gegenüber der Behörde bestehen. Für den Gesundheitssektor bedeutet dies konkret, dass Krankenhäuser mit über 30.000 vollstationären Fällen im Jahr als „KRITIS"-Betreiber gelten. Als vollstationär gilt eine Behandlung, wenn der Patient Tag und Nacht im Krankenhaus untergebracht ist und die stationären Leistungen komplett in Anspruch nimmt. Hiervon sind in Deutschland etwa 33 % aller Kliniken betroffen.

Bis zum Stichtag in knapp zwei Wochen müssen eine Reihe von Anforderungen erfüllt sein – zum einen muss alle zwei Jahre ein Nachweis über geeignete Vorkehrungen zur IT-Sicherheit erbracht werden. Zum anderen muss von Seiten des Betriebs eine Kontaktstelle, beziehungsweise ein Funktionspostfach benannt werden, außerdem müssen IT-Störungen dem Amt umgehend gemeldet werden. Auf technischer Ebene muss sichergestellt sein, dass betroffene Healthcare-Unternehmen dem neuesten Stand der Technik entsprechen und den Prüfstandards der Bundesbehörde gerecht werden.

Wie wichtig die neue Verordnung ist, zeigt eine kürzlich erschienene Studie zur IT-Sicherheit im Gesundheitssektor, die vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in Auftrag gegeben wurde. Hier offenbarte etwa ein Test der Mailserver mit dem Analysetool Cysmo, dass Patientendaten in deutschen Kliniken und Arztpraxen häufig nicht sicher aufgehoben sind. Insgesamt wurden neben den IT-Systemen von rund 1.200 niedergelassenen Ärzten auch 250 Kliniken und Apotheken untersucht. Das erschreckende Ergebnis war, dass lediglich 5 % der Kliniken einen sicheren Verschlüsselungsstandard nach Empfehlung des BSI verwendeten. 31 % nutzten die veralteten Standards SSL 2 und SSL 3, etwa 63 %

Arved Graf von Stackelberg, Managing Director DRACOON

die von der Bundesbehörde nicht mehr empfohlenen Standards TLS 1.0 oder TLS 1.1. Besonders erschreckend ist auch die Erkenntnis der Studie, dass E-Mail- und Passwortkombinationen von 60 % der Kliniken im Darknet aufzufinden waren. Angesichts dieser Zahlen überrascht die Tatsache nicht – wie eine vor zwei Jahren erschienene, großangelegte Erhebung von Roland Berger ergab – dass von 500 befragten Kliniken 64 % bereits Opfer eines Hackerangriffs wurden. Diese Zahlen deuten darauf hin, dass das Problem der Mängel in Bezug auf die IT-Sicherheit im Healthcare-Sektor ein strukturelles ist. Kliniken müssen in dieser Hinsicht unbedingt reagieren und sich auf die neuen Herausforderungen einstellen, die mit der fortschreitenden Digitalisierung einhergehen.

Vor allem aber im Hinblick auf den vom BSI geforderten Aspekt des „neuesten Standes der Technik" müssen deutsche Krankenhäuser dringend nachrüsten und eine einheitliche zeitgemäße Lösung einsetzen. Eine große Rolle spielt hier eine lückenlose clientseitige Datenverschlüsselung, mithilfe derer

die Informationen bereits am Endgerät verschlüsselt werden. Dadurch hat nicht einmal der Hersteller der Lösung die Möglichkeit, auf gespeicherte Daten zuzugreifen. Sinnvoll ist es außerdem, eine Softwarelösung „Made & Hosted in Germany" zu wählen. Denn deutsche Anbieter unterliegen den strengen deutschen Datenschutzgesetzen und versichern zugleich, dass die Lösung auch der EU- DSGVO entspricht. Entsprechende Zertifizierungen und Auszeichnungen wie z. B. die ISO27001 untermauern die Konformität zusätzlich. Wichtig ist außerdem, dass sich von autorisierten Personen jederzeit nachvollziehen lässt, wann welche Daten von wem bearbeitet wurden. Nur so lassen sich auch unkontrollierte Datenabflüsse erkennen und vermeiden.

Ein feingranulares Rechtesystem regelt außerdem detailliert, wer auf welche Daten zugreifen und diese bearbeiten darf. Wenn die Lösung zusätzlich noch über einen integrierten Ransomware-Schutz verfügt, mittels dem sich geschädigte Daten zeitnah wiederherstellen lassen, ist ein Maximum an Datensicherheit und -schutz gewährleistet. Klinikbetreiber müssen insgesamt das Risiko ernst nehmen und sich mit der Implementierung einer technisch zeitgemäßen Lösung auseinandersetzen – auf diese Weise sind sie künftig gewappnet im Kampf gegen Cyberkriminelle und vermeiden zudem verheerende Bußgelder im Rahmen der BSI-KRITIS-Verordnung. Auch Patienten können sich somit sicher sein, dass ihre sensiblen Daten in guten Händen sind und nicht kompromittiert werden.

Weitere Infos zu KRITIS erhalten Sie unter https://www.dracoon.com/de/kritis/