GESUNDHEITSDATEN IN GEFAHR !

München, den 10.11.2021

Betrifft: Verschlüsselungstrojaner bei Medatixx - offener Brief

Sehr geehrter Herr Dr. Krombholz,
sehr geehrter Herr Dr. Schmelz,
sehr geehrte Frau Dr. Ritter-Rupp,
sehr geehrte Frau Schindler,

wie Sie sicher erfahren haben, wurde Medatixx mit einem Verschlüsselungstrojaner angegriffen und bezüglich der inneren Abläufe weitgehend ausser Funktion gesetzt. Von nicht erreichbaren Hotlines sind einige Praxen bereits jetzt betroffen. Wie heute bekannt ist, ist die Verschlüsselung in der Regel der Schlusspunkt eines Angriffs, nachdem sich die Hacker bereits Tage oder Wochen vorher auf den Rechnersystemen umgesehen, eingenistet und für sie wertvolle Daten abgegriffen haben.

Die gematik läßt nun verlauten, dass sie die TI nicht in Gefahr sehe und verweist die Praxen auf die Anwendung der IT-Sicherheitsrichtlinie.

Eine dringende Frage: Können Sie uns bitte erläutern, inwiefern die Umsetzung welcher Punkte der IT-Sicherheitsrichtlinie eine Praxis davor schützen könnte, dass Schadsoftware, die von einem gekaperten Softwarehaus ausgeht, auf den Rechnern der Praxen landet - die natürlich Patientendaten enthalten? Den Einsatz von Virenscannern sowie Software- und Hardwarefirewalls setzen wir als selbstverständlich voraus.

In seinem Artikel "Sicher wie die TI-tanic" von Thomas Maus beim Heise Verlag, Januar 2020, beschreibt er genau ein Szenario, in dem der damals noch existente Verschlüsselungstrojaner "Emotet" über Patientendokumente in der ePA in Praxisverwaltungssysteme eingeschleppt wird und sich von da über die gesamte TI potentiell auf alle Teilnehmer der TI ausbreiten kann.

Der Struktur nach handelt es sich um einen vergleichbaren Vorfall, nur dass der Trojaner über das Softwarehaus selbst in die Praxen kommt.

Nach intensiver Rücksprache mit einem unserer Informatiker haben wir folgende Einschätzung sowie Notfall-Maßnahmen für Medatixx-Kunden erhalten:

"Einzig sinnvolle Maßnahme ist sofortige Systemabschaltung, Netzwerktrennung, selektiver Backup am abgeschalteten System, Neuaufbau. Patientendaten sind trotzdem wahrscheinlich schon abgeflossen – eine Inspektion und Archivierung (als Entlastungsbeweis) der Netzwerk-Volumen-Protokolle in Firewall oder DSL-Router wäre dringendst anzuraten.

Handelt es sich um einen sehr aggressiven Angriff und die Medatixx-SW-QS+Test-Prozeduren sind nicht auf höchstem Sicherheitsstand, so haben die Angreifer die Code-Basis infiltriert und alle Medatixx-Praxen, die einen kompromittierten SW-Update erhalten haben, werden demnächst mit sehr schlimmen Folgen zu rechnen haben. Maßnahmenempfehlung wie oben ***plus*** *Außerbetrieblassung des PVS bis zur Erklärung der Sicherheit durch Medatixx."*

Wir vermissen sehr die Herausgabe von Empfehlungen dieser Qualität mit höchster Priorität an die Praxen durch die Länder-KVen und die KBV. So ist mir ein Kollege bekannt, Medatixx-Kunde, der ohne jegliche Maßnahmen weiterarbeitet, weil er ja (noch) nichts Auffälliges bemerkt. Hier zeigt sich erneut verhängnisvoll, dass die meisten Kollegen und Kolleginnen kein Bewußtsein für die

Tiefengefahren einer digitalen Vernetzung haben und mit der Durchführung der oben dargestellten Maßnahmen definitiv überfordert sein dürften. Woher 30 - 40.000 als betroffen einzustufende Praxen zum gleichen Zeitpunkt notfallmäßig die nötigen kompetenten IT-Spezialisten finden könnten, ist noch eine ganz andere Frage.

In der Konsequenz fordern wir die Aussetzung der Anschlusspflicht an die Telematik-Infrastruktur.

Darüber hinaus irritiert uns die Tatsache, dass Medatixx den Vorfall erst eine Woche später den potentiell betroffenen Kunden bekannt gegeben hat. Zudem erinnern wir noch einmal an die Tatsache, dass die gematik zu 51% vom Bund übernommen ist und deshalb keinerlei Veranlassung hat, kompromittierende Tatsachen zügig an die Praxen weiterzugeben, da ja der TI-Anschluss unter allen Umständen dort erste Priorität hat.

In der Presse - z.B. T-online oder Heise-Verlag - wird inzwischen die Gefahr für die gesamte Gesundheitsversorgung in Deutschland als sehr hoch eingeschätzt: *T-Online, 09.11.2021: "Sollten tatsächlich Passwörter zum Zugang entwendet worden sein, wäre das ein erhebliches Risiko für das deutsche Gesundheitssystem."* Wir sind der Auffassung, dass unsere Körperschaften dieses Bedrohungsniveau noch vor der Presse erkennen und entsprechend reagieren sollten.

Mit freundlichen Grüßen

Alexandra Obermeier
Ärztin für Psychiatrie und Psychotherapie
München

für
das Bündnis für Datenschutz und Schweigepflicht (BfDS)