FAQ für medatixx-Kundinnen und -Kunden zur Cyber-Attacke auf medatixx

Versionierung	Datum / Uhrzeit	Änderung
1.0	08.11.2021 / 12.00 Uhr	-
2.0	12.11.2021 / 13.00 Uhr	Seite 1, Tabelle Versionierung eingefügt Seite 3, Ergänzung bei Frage 5 vorgenommen Seite 6, neue Fragen Nr. 15 und 16 hinzugefügt
3.0	12.11.2021 / 17.00 Uhr	Seite 6, neue Frage Nr. 17 hinzugefügt
4.0	15.11.2021 / 15.00 Uhr	Seite 3, Aktualisierung Frage 5 Seite 6, neue Frage Nr. 18 hinzugefügt
5.0	17.11.2021 / 12.00 Uhr	Inhaltsverzeichnis eingefügt Seite 6, Aktualisierung Frage 17
6.0	24.11.2021 / 17.00 Uhr	Seite 5, Aktualisierung Fragen 13 und 17

Inhaltsverzeichnis

1. **Von wem wurde der Angriff ausgeführt?**

   Es handelt sich um einen kriminellen Angriff. Wir arbeiten eng mit den Ermittlungsbehörden zusammen. Bitte haben Sie Verständnis dafür, dass wir uns derzeit nicht zu Details äußern.

2. **Wie sind Sie auf den Angriff aufmerksam geworden?**

   Wir haben am 3. November 2021 ungewöhnlichen Verkehr (Traffic) zwischen den Servern der medatixx und fremden IP-Adressen festgestellt. Daraufhin wurden erst durch unsere interne IT sowie unter Hinzuziehung unserer externen Partner die Ursache untersucht und unverzüglich Forensiker eingeschaltet. Es stellte sich heraus, dass es sich um einen Ransomware-Angriff handelt.

3. **Welche Sicherheitsvorkehrungen hatten Sie?**

   medatixx nimmt den Datenschutz und die Datensicherheit sehr ernst. Unser Sicherheitskonzept umfasst sowohl modernste technische als auch prozessuale und verhaltensbezogene Maßnahmen. Die IT-Sicherheit der medatixx wird regelmäßig geprüft und fortlaufend verbessert, auch indem sogenannte Penetrationstests durchgeführt werden.

4. **Haben Sie einen Notfallplan und greift der jetzt wie geplant?**

   Ja, wir haben einen Notfallplan. Dieser wird aktuell von den verschiedenen Fachleuten systematisch abgearbeitet.

   Sobald die Störung vollständig behoben ist, werden wir den gewohnten Geschäftsbetrieb fortsetzen können. Unsere Kunden und Vertriebspartner haben wir unverzüglich kontaktiert und werden sie auch fortlaufend über die Entwicklung weiter informieren.

5. **Wie kann ich Kontakt mit medatixx aufnehmen?**

   In den nächsten Tagen werden wir die unseren Kunden bekannten Rufnummern und Mailadressen der zentralen Services und unserer medatixx-Niederlassungen schrittweise wieder in Betrieb nehmen. Sie erhalten über unsere Website www.medatixx.de fortlaufend Informationen über die weitere Entwicklung.

   Bei dringenden Anliegen rund um Ihre Praxissoftware senden Sie bitte eine Mail an akutservice@medatixx.de mit Angabe Ihres vollständigen Praxisnamens, des Namens Ihrer eingesetzten Praxissoftwarelösung und der Kontaktdaten eines Ansprechpartners, damit wir Sie kontaktieren und Ihre Anfrage dokumentieren können. Wir werden uns schnellstmöglich um Ihr Anliegen kümmern. Die Ihnen bekannten Mobilnummern unserer Mitarbeiter sind unverändert erreichbar. Wenn Sie von einem unserer selbstständigen regionalen Vertriebspartner betreut werden, wenden Sie sich auch weiterhin an diesen; diese sind wie gewohnt erreichbar.

6. **Was ist konkret von der Attacke betroffen?**

   Es handelt sich um einen kriminellen Angriff auf unsere IT-Infrastruktur, bei dem wichtige Teile unseres internen IT-Systems verschlüsselt wurden. Infolgedessen sind derzeit unsere Erreichbarkeit sowie der gesamte Unternehmensbetrieb stark beeinträchtigt.

Die Funktionalität der Systeme in Ihrer Praxis / Ihrem MVZ / Ihrer Ambulanz ist nach heutigem Erkenntnisstand nicht betroffen.

7. Was ist mit meinen Daten; sind Daten abgeflossen?

Am 3. November 2021 haben wir festgestellt, dass ein Ransomware-Angriff auf die interne IT-Infrastruktur der medatixx stattgefunden hat. Derzeit dauern unsere Untersuchungen noch an. Aktuell können wir weder bestätigen noch ausschließen, dass ggf. einzelne unserer Kunden von einem möglichen Datenabfluss betroffen sein könnten. Sofern wir hierfür belastbare Anhaltspunkte haben und aus dem Datenabfluss Benachrichtigungspflichten erwachsen, werden wir diese selbstverständlich erfüllen. Wir arbeiten eng mit den Ermittlungsbehörden und der Hessischen Datenschutzbehörde zusammen.

8. Wie viele Kunden und Vertriebspartner sind von dem Angriff möglicherweise betroffen?

Unsere Untersuchungen dauern noch an. Fest steht derzeit nur, dass Daten in unserer internen IT-Infrastruktur verschlüsselt wurden. Unsere selbstständigen regionalen Vertriebspartner sind von dem kriminellen Angriff nach aktuellem Kenntnisstand nicht betroffen und weiterhin wie gewohnt erreichbar.

9. Was bedeutet dieser Angriff für mich als Kunden der medatixx und was kann / muss ich tun, um die Sicherheit meiner Daten zu gewährleisten?

Nach jetzigem Stand richtete sich der Angriff gegen medatixx als Unternehmen, nicht gegen unsere Kunden. Die Funktionalität der Systeme in Ihrer Praxis / Ihrem MVZ / Ihrer Ambulanz ist nach heutigem Erkenntnisstand nicht betroffen.

Ob und in welchem Umfang Daten auch entwendet wurden, ist zum heutigen Zeitpunkt nicht bekannt. Es kann daher nicht ausgeschlossen werden, dass bei uns gespeicherte Daten entwendet wurden. Wir empfehlen Ihnen deshalb ausdrücklich, unverzüglich vorsorglich Ihre Passwörter zu ändern. Detaillierte Anleitungen finden Sie auf medatixx.de.

- Ändern Sie die Passwörter für Ihre Praxissoftware. Eine Anleitung finden Sie auf unserer Website www.medatixx.de.
- Ändern Sie die Passwörter Ihrer Windows-Anmeldung an Ihren Arbeitsplätzen und an Ihrem Server und Ihren Firewalls. Eine Anleitung finden Sie ebenfalls auf unserer Website www.medatixx.de.
- Ändern Sie die Passwörter Ihres TI-Konnektors. Eine Anleitung finden Sie auf unserer Website www.medatixx.de.
- Überprüfen Sie die in Ihrer Einrichtung geltenden Regeln zum Umgang mit der Nutzung des Internets und mit E-Mails und sensibilisieren Sie Ihr Team nochmals. Achten Sie insbesondere auf verdächtige Anhänge und Links in E-Mails; auch bei E-Mails, die den Absender „medatixx“ tragen. Hier gilt: Wir werden Sie per Mail niemals um Daten, Kennwörter etc. bitten oder Sie auffordern, Ihre Kennwörter über einen beigefügten Link zu ändern. Empfehlungen zum rechtskonformen und sicheren Umgang mit Daten finden Sie auf den Webseiten der KBV (www.kbv.de; IT-Sicherheitsrichtlinie) und des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.bund.de).

10. Ist mein Zugang zur TI noch sicher? Können Fremde meinen Zugang zur TI benutzen oder übernehmen?

Nach jetzigem Stand richtete sich der Angriff gegen medatixx als Unternehmen, nicht gegen unsere Kunden. Die Funktionalität der Systeme in Ihrer Praxis / Ihrem MVZ / Ihrer Ambulanz ist nach heutigem Erkenntnisstand nicht betroffen.

Ob und in welchem Umfang Daten auch entwendet wurden, ist zum heutigen Zeitpunkt nicht bekannt. Es kann daher nicht ausgeschlossen werden, dass bei uns gespeicherte Daten entwendet wurden. Wir empfehlen Ihnen deshalb ausdrücklich, unverzüglich vorsorglich Ihre Passwörter zu ändern. Detaillierte Anleitungen finden Sie auf medatixx.de.

- Ändern Sie die Passwörter für Ihre Praxissoftware. Eine Anleitung finden Sie auf unserer Website www.medatixx.de.
- Ändern Sie die Passwörter Ihrer Windows-Anmeldung an Ihren Arbeitsplätzen und an Ihrem Server und Ihren Firewalls. Eine Anleitung finden Sie ebenfalls auf unserer Website www.medatixx.de.
- Ändern Sie die Passwörter Ihres TI-Konnektors. Eine Anleitung finden Sie auf unserer Website www.medatixx.de.
- Überprüfen Sie die in Ihrer Einrichtung geltenden Regeln zum Umgang mit der Nutzung des Internets und mit E-Mails und sensibilisieren Sie Ihr Team nochmals. Achten Sie insbesondere auf verdächtige Anhänge und Links in E-Mails; auch bei E-Mails, die den Absender „medatixx“ tragen. Hier gilt: Wir werden Sie per Mail niemals um Daten, Kennwörter etc. bitten oder Sie auffordern, Ihre Kennwörter über einen beigefügten Link zu ändern. Empfehlungen zum rechtskonformen und sicheren Umgang mit Daten finden Sie auf den Webseiten der KBV (www.kbv.de; IT-Sicherheitsrichtlinie) und des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.bund.de).

11. Muss ich als Praxisinhaber die Patienten informieren?

Bitte haben Sie Verständnis dafür, dass wir Sie nicht rechtlich beraten dürfen. Wenn Sie einen Datenschutzbeauftragten bestellt haben, sollten Sie diesen einbinden.

12. Muss ich meine KV und andere Instanzen informieren?

Bitte haben Sie Verständnis dafür, dass wir Sie nicht rechtlich beraten dürfen. Von uns wurden die KBV und die KVen mit Verweis auf unsere Website informiert.

13. Ist eine Fernwartung derzeit überhaupt sicher?

medatixx hat die Fernwartungsumgebung neu aufgesetzt. Die bei dem Angriff kompromittierte Umgebung wurde hierbei nicht genutzt. Die Standardlösung für Fernwartungen - Kunden der medatixx - ist Beyond Trust.

14. Ist es sicher, wenn Updates von medatixx kommen, diese zu installieren?

Die Bereitstellung von Updates durch medatixx wird nur dann erfolgen, wenn wir von deren Sicherheit überzeugt sind. Darüber informieren wir Sie vorab mit gesonderten Hinweisen.

15. Ist der TI-Zugang in der Arztpraxis vom Cyberangriff auf die medatixx betroffen?

Nach jetzigem Stand richtete sich der Angriff gegen medatixx als Unternehmen, nicht gegen unsere Kunden oder die Telematikinfrastruktur. Die Funktionalität der Systeme in Praxis / MVZ / Ambulanz sowie der TI-Zugang sind nach heutigem Erkenntnisstand nicht betroffen.

16. Ist durch eine mögliche Kompromittierung des Konnektorpassworts der Zugriff auf die TI von außerhalb der Praxis möglich?

Nach jetzigem Stand richtete sich der Angriff gegen medatixx als Unternehmen, nicht gegen unsere Kunden oder die Telematikinfrastruktur. Die Funktionalität der Systeme in Praxis / MVZ / Ambulanz sowie der TI-Zugang sind nach heutigem Erkenntnisstand nicht betroffen. Der Zugriff aus der Ferne auf den Konnektor ist bei korrekt konfigurierter Firewall nicht möglich. Zudem basiert die TI-Sicherheitsarchitektur auf einer mehrstufigen, auch hardwarebasierten Absicherung Ihres Zuganges. Selbst im Fall eines kompromittierten Passworts würde dies allein noch keinen unbefugten Zugriff ermöglichen. Etwaige Zugriffe auf ihre Firewall können unsere Kunden im KundenCenter der I-Motion in der Rubrik IT-Sicherheit selbst prüfen.

17. Steht die Störung beim KV-Connect-Versand in den Praxissoftwarelösungen von medatixx im Zusammenhang mit dem Cyber-Angriff auf das Unternehmen?

Einen Zusammenhang mit dem Cyber-Angriff auf unser Unternehmen können wir ausschließen. Es handelt sich um einen bekannten Fehler in der Zertifikatsprüfung der Praxissoftware. Unter folgenden Links stehen eine Korrekturdatei sowie die dazugehörige Anleitung für x.isynet, x.comfort und x.concept bereit:
https://arztsoftware.medatixx.de/kundenservice/xisynet
https://arztsoftware.medatixx.de/kundenservice/xcomfort
https://arztsoftware.medatixx.de/kundenservice/xconcept

18. Unsere Praxis erhält unaufgefordert Anrufe von vermeintlichen Microsoft-Supportmitarbeitern. Wie gehen wir damit um?

Achtung: Hierbei handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch von Kriminellen, um an Passwörter oder persönliche Daten zu gelangen oder etwa Schadsoftware auf Ihren Systemen zu installieren.
Man bezeichnet diesen Betrugsversuch auch als „Tech Support Scam“. Bitte beenden Sie das Gespräch sofort. Geben Sie keinerlei Informationen preis. Microsoft führt eigenen Angaben zufolge nie unaufgefordert Telefonanrufe mit Serviceangeboten durch. Nähere Informationen hierzu finden Sie unter anderem bei der Verbraucherzentrale unter diesem Link oder auf den Websites von Microsoft.