Das Problem mit Hakuna Matata

Hakuna Matata ist eine Redewendung aus der afrikanischen Sprache Swahili. Wörtlich übersetzt heißt sie: Es gibt keine (Hakuna) Probleme/Schwierigkeiten (Matata) oder freier übersetzt: Alles in bester Ordnung. Lesen Sie in unserer Serie zur Cybersicherheit, warum in einem MVZ in Ober-Ramstadt im März 2017 plötzlich nichts mehr in Ordnung war – und das nicht trotz, sondern wegen Hakuna Matata.

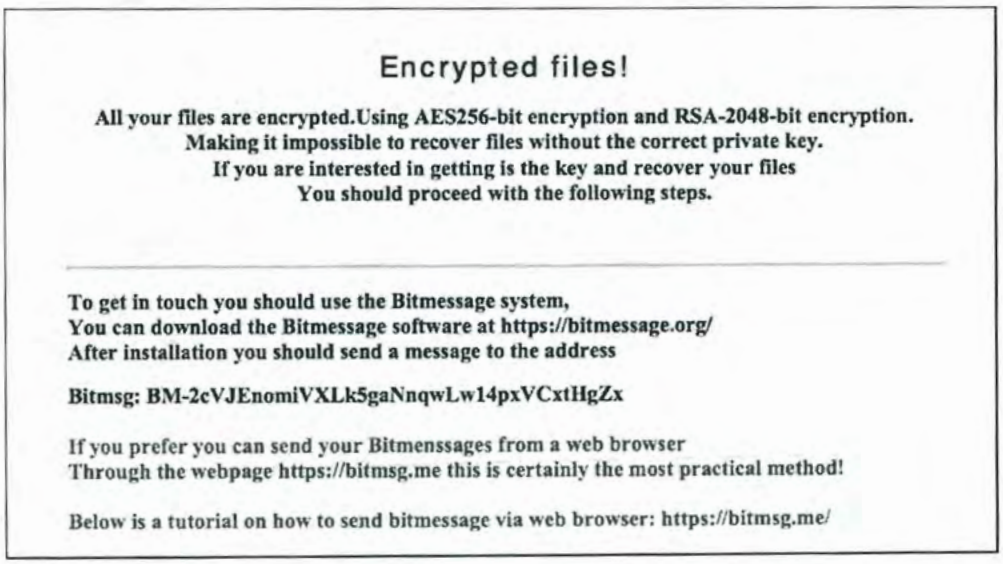
Kann wieder lächeln: MFA Annette Mink bemerkte den Trojaner zuerst.

Es ist Montag, der 27. März 2017, gegen 17.30 Uhr im Hausarzt-MVZ in Ober-Ramstadt. Annette Mink ist MFA, Erstkraft und sitzt zu diesem Zeitpunkt an der Anmeldung. Bislang ist es ein normaler Arbeitstag, keine besonderen Vorkommnisse. Noch eine Stunde, dann ist die Sprechstunde für heute beendet. Doch dann geht's plötzlich los: Auf dem Bildschirm taucht die Meldung auf „All your files are encrypted. Using AES256-bit encryption and RSA-2048-bit encryption … You should proceed with the following steps …" Also: „Alle Daten sind verschlüsselt. Wenn Sie wieder an Ihre Daten gelangen wollen, gehen Sie wie folgt vor." Später wird klar, dass sich hinter AES256-bit ein Trojaner namens Hakuna Matata verbirgt und dass die Täter umgerechnet circa 4.000 Euro Lösegeld in Form von Bitcoins verlangen.

Und tatsächlich – nichts geht mehr. Mink ruft den ärztlichen Leiter Michael Andreas Krist hinzu. „Ich stand ungläubig vor dem PC und musste erstmal realisieren, dass wir komplett ausgeknockt waren", gesteht er. Inzwischen haben auch die Kollegen in den anderen Räumen bemerkt, dass etwas nicht stimmt beziehungsweise dass schlichtweg nichts mehr geht.

Wenig später ist der aus Groß-Umstadt herbeigerufene MVZ-Manager Alexander Noll vor Ort. Dass er

Hier ging's los. Am PC des Empfangstresens im Ober-Ramstädter MVZ ploppte die Trojanermeldung als Erstes auf: Hakuna Matata – alle Daten verschlüsselt.



Encrypted files!

All your files are encrypted.Using AES256-bit encryption and RSA-2048-bit encryption.
Making it impossible to recover files without the correct private key.
If you are interested in getting is the key and recover your files
You should proceed with the following steps.

To get in touch you should use the Bitmessage system,
You can download the Bitmessage software at https://bitmessage.org/
After installation you should send a message to the address

Bitmsg: BM-2cVJEnomiVXLk5gaNnqwLw14pxVCxtHgZx

If you prefer you can send your Bitmenssages from a web browser
Through the webpage https://bitmsg.me this is certainly the most practical method!

Below is a tutorial on how to send bitmessage via web browser: https://bitmsg.me/

So sah sie aus, die Meldung der Täter. Bei der Beschreibung zur Kontaktaufnahme geben sie sich sogar richtig Mühe und liefern gleich den Link zu einem Tutorial mit. Niemand im MVZ hat aber auch nur eine Sekunde erwogen, das Lösegeld zu zahlen. Kontakt zu den Tätern gab es nicht.

nun mehrere schlaflose Nächte vor sich hat, ahnt er zu diesem Zeitpunkt nicht. „Im Nachhinein – hätte ich das damals schon gewusst: Um Gottes Willen." Von unterwegs hat er bereits mit dem IT-Servicepartner telefoniert. Was tun? Die klare Antwort: Alle Netzwerkstecker ziehen, das System komplett abschalten. Strom aus!

KEIN ZUGRIFF AUF DATEN IST WIE ARBEITEN IN DER STEINZEIT

Gesagt, getan. Gleich am nächsten Morgen ist ein Mitarbeiter des IT-Servicepartners in der Praxis, um das Ausmaß der Systeminfiltrierung zu checken. Gute Nachrichten hat er leider nicht. Sämtliche Daten sind verschlüsselt – null Zugriff auf Terminkalender, Patientenakten, Dokumentationen etc. Mink erinnert sich nur ungern: „Die ersten Tage nach dem Angriff waren schrecklich. Das Arbeiten im normalen Ablauf war überhaupt nicht möglich. Es ging gar nichts. Wir wussten nicht mal, wann welcher Patient bestellt war." Und Krist fügt hinzu: „Die Patienten wurden wie in der Steinzeit behandelt. Rezepte, Überweisungen, alles musste von Hand geschrieben und extra aufgelistet werden, um es später ins System neu einzupflegen."

Der IT-Fachmann isoliert derweil jeden einzelnen Arbeitsplatz. Dann spielt er eine Software auf, um den Trojaner zu entfernen und zu schauen, welche Daten betroffen sind. Doch die Daten lassen sich nicht wiederherstellen. Sollte aber ja kein Problem sein, denn wozu hat man schließlich eine Datensicherung? Die entsprechende Festplatte wird aus dem Safe geholt. Dann der nächste Schock: Das Passwort funktioniert nicht. Auch diese Daten sind verschlüsselt. „Man hat uns das später so erklärt", sagt Noll, „es ist immer ein PC infiziert, vielleicht auch schon jahrelang. Das kann man gar nicht so genau sagen. Und irgendwann läuft ein Zeitcode ab und dann fängt plötzlich dieser Befall an."

Michael Andreas Krist, ärztlicher Leiter, nimmt IT-Fachleute in die Pflicht: „Wir haben gelernt, dass auch IT-Experten, die wissen sollten, was sie machen, es nicht immer richtig machen!"

RETTUNG MITHILFE DER ALTEN FESTPLATTEN

Ein Glück in diesem Unglück haben sie dann aber doch: Fünf Monate zuvor war der Server ausge-

MVZ-Manager Alexander Noll koordinierte die Behebung des Schadens, sodass Ärzte und MFAs weiter Patienten betreuen konnten. „Man ist nie hundertprozentig sicher, das ist klar. Aber man sollte das Risiko so gut es geht minimieren."

tauscht worden und die Festplatten lagen noch im Safe. Die Daten bis Dezember 2016 konnten auf diese Weise wiederhergestellt werden. „Hätten wir die alten Festplatten nicht mehr gehabt, wäre vermutlich alles weg gewesen", sagt Noll und auch heute noch steht ihm bei dieser Vorstellung der Schrecken ins Gesicht geschrieben.

Was bleibt, ist der Verlust sämtlicher Daten des ersten Quartals 2017, denn unglücklicherweise geschah der Hackerangriff ja kurz vor Quartalsende. Für die Honorarabrechnung eine Katastrophe. Noll zählt auf: „Einmal natürlich die Privatabrechnung. Die machen wir monatlich. Da war dann der März weg, ungefähr 12.000 Euro. Die konnten wir auch nicht mehr retten." Bei der KV-Abrechnung habe das Controlling anhand von Statistiken mit 3.600 Fällen und einem Honorarvolumen von circa 240.000 Euro gerechnet. Nicht auszudenken, wenn das jetzt weg wäre. „Wir hatten damals nur drei Standorte. Aber wenn so eine hohe Summe am größten Standort, eine Viertelmillion, fehlt, dann ist das existenzgefährdend", erzählt Noll.

+++ Newsticker +++

Chronologie des Cyber-Angriffs auf das MVZ Ober-Ramstadt

Montag, 27. März 2017

+++ 17:30 Uhr: MfA Mink bemerkt den Trojanerbefall kurz vor Sprechstundenende +++ Alle angezeigten Daten verschlüsselt, Software lässt sich nicht mehr nutzen, Lösegeldforderung in Höhe von 4.000 € in Bitcoin +++ Alarmierungskette startet (Geschäftsführung, IT-Servicepartner, Landrat, …) +++ IT-Abteilung der Kreiskliniken wird eingeschaltet +++ Sämtliche Rechner und der Server werden abgeschaltet, die Netzwerk- und Stromkabel gezogen +++ Die Prüfung der weiteren MVZ-Standorte auf Systeminfektion ist negativ. +++

Dienstag, 28. März 2017

+++ 10:00 Uhr: Praxis startet im Notbetrieb ohne medizinische Geräte und ohne Terminbuch. IT-Servicepartner säubert System von Schadsoftware. +++ System wird wiederhergestellt. +++ Neuaufspielen der Daten misslingt, weil die Sicherungskopien ebenfalls verschlüsselt sind. +++

Mittwoch, 29. März 2017

+++ Virusattacke wird der KV Hessen gemeldet und eine Fristverlängerung für die Honorarabrechnung Q1/2017 beantragt. +++

Donnerstag, 30. März 2017
+++ MVZ-Manager Noll erstattet Anzeige gegen Unbekannt bei der Staatsanwaltschaft Darmstadt. Die Übergabe der Festplatten erfolgt einige Tage später direkt an das entsprechende Dezernat in Darmstadt. +++

Freitag, 31. März 2017
+++ Quartalsende +++ Neueinrichtung Server, technische Services wieder nutzbar. +++

Samstag/Sonntag, 1./2. April 2017
+++ Verschlüsselte Daten sind nicht rekonstruierbar. +++ Abrechnungsdaten Privathonorar März 2017 und KV-Abrechnung Q1/2017 sind verloren. +++

Ab Montag, 3. April 2017
+++ Eingeschränkter Praxisbetrieb ist wieder möglich und die Daten bis zum 31.12.2016 sind rekonstruiert. +++ Servicepartner geben sich die Klinke in die Hand. +++ Medizintechnik (EKG, Ultraschall etc.) wird schrittweise wieder in Betrieb genommen. +++ Terminvergabe für Mai und Folgemonate ist wieder möglich. +++

Mai 2017
+++ MVZ meldet KVH-Abrechnungsabteilung tatsächlichen Datenverlust. +++ Antrag an Vorstand auf Härtefall beziehungsweise Honorarschätzung erfolgt. +++

27.-30. Mai 2017
+++ KVH fordert Nachweise zur Bestätigung des Trojanerbefalls. +++ Verwaltungsapparat rotiert. +++

Mai 2017
+++ Neuanschaffung Hard- und Software, Investitionen in Firewalls von über 25 Tsd. Euro erfolgt. +++

Ende Mai 2017
+++ Praxisbetrieb läuft wieder in Routine. +++

26. September 2017
+++ Staatsanwaltschaft Darmstadt teilt mit, dass Ermittlungen ergebnislos eingestellt wurden. +++ Herkunft des Trojaners aus dem russisch-asiatischen Raum vermutet. +++ Mangels Kooperationsabkommen keine Weiterverfolgung möglich. +++

6. November 2017
+++ MVZ bereitet Widerspruch gegen Honorarschätzung Q1.2017 vor, weil das MVZ auf Wachstumskurs ist und die zugrunde gelegten Vorquartale nicht repräsentativ sind. +++

Dezember 2017
+++ Der Vorfall wirkt sich auf die Erstellung des Jahresabschlusses 2017 aus. +++

April 2019
+++ Einigung mit IT-Dienstleister über Schadensbeteiligung. +++

2014 war das MVZ in Ober-Ramstadt das erste kommunale in Deutschland. Inzwischen gibt es sechs Standorte mit insgesamt 60 Mitarbeitern.

Nachdem klar war, dass die Daten endgültig verloren waren, stellte man beim KV-Vorstand einen Antrag auf Härtefall beziehungsweise Honorarschätzung. „Die KV hat damals eine einstweilige Entscheidung gefällt, dass wir 75 Prozent der durchschnittlichen Honorarsumme aus dem dritten und vierten Quartal 2016 erhalten. Da das erste Quartal leider auch immer das stärkste ist, ergab sich für uns eine Lücke von ca. 60.000 Euro", erläutert Noll, betont in diesem Zusammenhang aber auch die gute Zusammenarbeit mit der KV: „Wir hatten mit dem BeratungsCenter in Darmstadt Kontakt – sehr hilfsbereite Kollegen."

Infobox

Das „Zentrum der medizinischen Versorgung Darmstadt-Dieburg MVZ GmbH" hat heute sieben Standorte, davon fünf als MVZ und zwei als Nebenbetriebsstätte: den größten in Ober-Ramstadt, drei in Groß-Umstadt, einen in Seeheim-Jugenheim, einen in Höchst im Odw. und einen in Traisa. Alle sind Einrichtungen des Landkreises Darmstadt-Dieburg – beim Start 2014 übrigens das erste kommunale MVZ in Deutschland.

Aktuell arbeiten in den Praxen 60 Mitarbeiter, davon 18 angestellte Ärzte. Sie betreuen insgesamt fast 50.000 Fälle pro Jahr.

https://mvz-dadi.de/

NICHT NUR HONORARVERLUSTE, AUCH HOHE KOSTEN

Diesem deutlichen Honorarverlust standen auf der anderen Seite enorme Kosten für die IT-Infrastruktur gegenüber. Einige PCs mussten neu angeschafft werden, so auch der Server. Noll beziffert die Ausgaben auf um die 25.000 Euro. Dazu gehören zum Beispiel auch eine Hardwarefirewall, weitere Schutzmechanismen und Log-in-sticks für die Mitarbeiter. Das seien alles Kosten, die sich über die Jahre nach diesem Angriff ergeben haben.

Doch zurück zu den Tagen nach dem Angriff. Im MVZ geben sich inzwischen die Firmen die Klinke in die Hand: für den Ultraschall, für die (Langzeit-) Blutdruckmessung und fürs EKG. Alle Verknüpfungen müssen einzeln wiederhergestellt und die Funktionen getestet werden. Mit Aushängen weist das Praxisteam die Patienten auf eine IT-Störung hin und dass es zu Unannehmlichkeiten kommen könne. Besondere negative Reaktionen von Patienten bleiben aber keinem der Beteiligten in Erinnerung. Das wäre sicher anders gewesen, wenn durch den Hackerangriff tatsächlich Patientendaten abgeschöpft worden wären. Laut Diagnose des IT-Fachmanns war dies aber nicht der Fall. Zum Glück! Nicht auszudenken, wenn sensible Patienten- und Sozialdaten in kriminelle Hände gekommen wären.

Nach gut einer Woche liefen alle Systeme wieder nahezu reibungslos. Was nicht rekonstruiert werden konnte, war der Terminkalender. Die Praxis vergibt im hausärztlichen Bereich Termine vier bis fünf Wochen im Voraus. Da die Terminlücken nicht bekannt waren, konnten sie auch nicht vergeben werden. Heißt: weniger Patienten und nochmals Honorarverlust.

URSACHE BLEIBT UNGEKLÄRT

Wie genau der Trojaner ins System kam, bleibt bis heute ungeklärt. Vielleicht ein E-Mail-Anhang oder ein Datenstick? Keiner weiß es. Das Team um Ärzte, MFAs und Management ist sich aber einig, dass Schuldzuweisungen keinen weiterbringen. Stattdessen ziehen sie an einem Strang und nehmen viele Extrastunden und Mühen in Kauf. „Wenn die Stimmung im Team nicht so gut gewesen wäre, hätten wir die Situation nicht so gut meistern können", sagt Mink stolz.

Neben der Aufrüstung im IT-Bereich wurden in der Folgezeit auch die Dienstanweisungen ergänzt, Schulungen eingeführt beziehungsweise ergänzt und einfach extrem sensibilisiert. Die wahrscheinlich wichtigste Erkenntnis: Es reicht nicht aus, eine Datensicherung durchzuführen, man muss auch überprüfen, ob man an die Daten anschließend wirklich rankommt. „Ich achte sehr darauf, dass die PC-Sicherung zu jeder Zeit einwandfrei stattfindet", sagt Mink.

Das Problem mit Hakuna Matata haben sie mit viel Anstrengung, Zeit und Geld gelöst. „Im Nachhinein kann man natürlich darüber lachen, allein die Ironie", grinst Noll, „es ist uns auch bewusst, was das heißt. Wir benutzen den Begriff bis heute immer mal wieder. Wenn technisch irgendetwas nicht stimmt, dann hat meistens einer den Begriff drauf und sagt: Weißt du noch? Hakuna Matata."

Cornelia Kur

Infobox

Auf den PUNKT.-Serie zur Cybersicherheit

Wie kann ich meine Praxis am besten vor einem Cyberangriff schützen und was ist zu tun, wenn's passiert? Diese und weitere Fragen beantwortete der IT-Experte Mark Peters in seinem Gastbeitrag „Praxishacking: Bedrohung ernst nehmen" in Heft 6/2020.

Dirk Hintermeier, Landeskoordinator Prävention Cybercrime beim Hessischen Landeskriminalamt, ging in seinem Beitrag „Cyberkriminalität – eine zweite Pandemie?" ebenfalls in Heft 6/2020 auf die Zahlen aus der aktuellen polizeilichen Kriminalstatistik und die Vorgehensweise der Täter ein.

Im nächsten Heft (2/2021) gibt Dr. med. Christine Trutt-Ibing, Ärztin und Web-Entwicklerin, wertvolle Tipps für den Umgang mit dem Internet und zur Erhöhung der persönlichen digitalen Kompetenz.

Alle AdP-Artikel aus der Serie zur Cybersicherheit finden Sie unter **www.kvhessen.de/cybersicherheit**