LivingData
SICHER EINE GUTE LÖSUNG

AKDB

IT-Sicherheit

Chronik eines Cyberangriffs

Es passiert immer wieder und immer öfter: Cyberkriminalität gegen Kommunen. Als eine oberbayerische Gemeinde von einem schweren Ransomware-Angriff heimgesucht wurde, schritt das Systemhaus LivingData ein – und rettete die Daten in letzter Minute ...

KUNDENSTORY

Es könnte jeden treffen: Trotz strengster und effektivster Firewalls und Cybersecurity-Maßnahmen schlägt der Verschlüsselungstrojaner zu. Meistens öffnet ein Mitarbeiter einen infizierten Anhang. Dann nimmt das Unheil seinen Lauf - eine Zeit lang unbemerkt. Genau das widerfuhr im Juni 2019 einer oberbayerischen Gemeinde. Das Systemhaus LivingData, ein Tochterunternehmen der AKDB, war sofort an Ort und Stelle. In einer nervenzerreißenden Wochenend-Aktion konnten fast alle Daten gerettet werden. Einmal mehr wurde klar: Es ist ein Irrtum zu denken, dass „sowas immer nur den anderen passiert". Die Gefahr ist real. Sensible Bürgerdaten können unwiederbringlich verloren gehen!

Mittwoch, 19. Juni 2019

Eine Störungs-Mail geht beim System- und Softwarehaus LivingData ein: In einer oberbayerischen Gemeinde funktioniert die Sitzungsdienst-Software Session plötzlich nicht. Die Gemeinde hat einen Systembetreuungs-Vertrag mit der LivingData abgeschlossen. Nach gründlicher Kontrolle steht fest: An der Software liegt es nicht. Ein Mitarbeiter der LivingData schaltet sich per Fernwartung auf den PC auf. Er stellt fest: Ein Verschlüsselungstrojaner hat sich über einen Mail-Anhang Zutritt zum System verschafft. Es werden fünf infizierte PCs gefunden.

Die Mitarbeiter der LivingData werden aktiv. Vom 20. bis 28. Juni werden die Systeme bereinigt, der Domain Controller und die Datenbank wiederhergestellt. Der Systemingenieur Yakup Celik ist am 27. Juni vor Ort, um die fünf betroffenen PCs neu aufzusetzen. Es scheint noch mal gut gegangen zu sein …

»Es ist ein Irrtum zu denken, dass „sowas immer nur den anderen passiert". Die Gefahr ist real.«

Freitag, 28. Juni

9.30 Uhr
Es ist einer der heißesten Tage des Jahres. Das Thermometer zeigt bereits frühmorgens über 20 Grad. Hamed El Rafei, Teamleiter Systemingenieure Süd bei der LivingData, ist um diese Uhrzeit schon lange im Büro. Er hat ein Meeting. Plötzlich platzen die Systemingenieure Nils Gunia und Markus Friedl in den Raum hinein. Die sonst so besonnenen Kollegen klingen besorgt. Irgendetwas stimmt nicht in der Verwaltung der kleinen oberbayerischen Gemeinde. Es scheint einen zweiten Vorfall zu geben. Ein Notebook ist infiziert. Die gesamte IT läuft auf einmal viel zu langsam.

10.30 Uhr
El Rafei schaltet sich per Fernwartung auf die Systeme des Kunden auf. Ihm ist sofort klar: Wir haben ein ernstes Problem! Sämtliche Dokumente und Dateien sind verschlüsselt. Das ist klar erkennbar: Word-Dokumente, PDFs – sie alle tragen statt Dateinamen einen Buchstaben-Nummern-Sonderzeichen-Mix. Ein eindeutiges Zeichen. Was schlimmer ist: Auch das Betriebssystem ist massiv geschädigt. Der Schaden ist gewaltig! Es ist der Domain Controller betroffen, der Mail-Server und – schlimmer noch – der AKDB-Server. Das heißt Einwohnermeldeamt, Finanzwesen, alles ist infiziert.

Auf der Notebook-Oberfläche steht eine Nachricht: Ihre Daten wurden verschlüsselt (…) Sie müssen für die Entschlüsselung in Bitcoins zahlen. Der Preis richtet sich nach der Schnelligkeit, mit der Sie uns zurückschreiben. El Rafei weiß: Viele Opfer zahlen, bekommen ihre Daten aber trotzdem nicht komplett zurück, denn die Ransomware verschlüsselt im Hintergrund alle erreichbaren Dateien und Netzwerklaufwerke weiter. Er muss sich direkt vor Ort ein Bild von der Lage machen! El Rafei springt in seinen Wagen. Gleichzeitig ruft er seinen Mitarbeiter vor Ort, Yakup Celik, an und bittet ihn, das Vor-Ort-Krisenteam zusammenzurufen: Bürgermeister, Kämmerer und Geschäftsleiter. Alle Gemeinde-Mitarbeiter sollen vorerst die Arbeit einstellen.

11.45 Uhr
El Rafei ist in der Gemeinde angekommen. Er wird vom Krisenstab empfangen. Der Bürgermeister gibt ihm völlige Handlungs- und Entscheidungsfreiheit. Er soll tun, was nötig ist, um so viel Daten wie möglich zu retten. Die Experten der LivingData erklären dem Bürgermeister die Vorgehensweise: Sie werden das Netzwerk-Kabel ziehen und sämtliche Server und PCs neu formatieren und einrichten und schauen, wo sich der Trojaner ein-

geschlichen hat. Auch sämtliche iPads und Diensthandys werden ausgeschaltet, da sie ja ebenfalls auf den infizierten Mail-Server zugreifen. In einem zweiten Schritt werden die Backups kontrolliert: Es sollen sämtliche Dateien einzeln einem Screening unterworfen werden. Das sind bei 17 virtuellen Servern jeweils circa 4000 Dateien. Aber dann die Überraschung: Der Backup-Container ist komplett korrupt. Das ist der GAU.

El Rafei beschließt, einen anderen Plan zu verfolgen: Er wird sämtliche Backup-Bänder sichten. Die ersten sortiert El Rafei gleich aus, denn er weiß, dass die erste Attacke mindestens 12 Tage zuvor stattgefunden hat. Es bleiben noch vier Bänder übrig. Er macht das Screening des ersten: korrumpiert. Dann das zweite: auch verseucht. Bei dem dritten steigt eine Hitzewelle in ihm auf: Die Daten sind nicht konsistent. Es bleibt noch ein Tape übrig. Hier sind die Daten vom 8. bis 10. Juni gespeichert. Ihm ist bewusst: Wenn dies auch kaputt ist, sind sämtliche Daten der Gemeinde verloren. Für immer. Unwiederbringlich. Er fängt an leise zu beten ...

Und dann: Das Band ist sauber. Es sind insgesamt 18 Tage an Daten verloren gegangen.

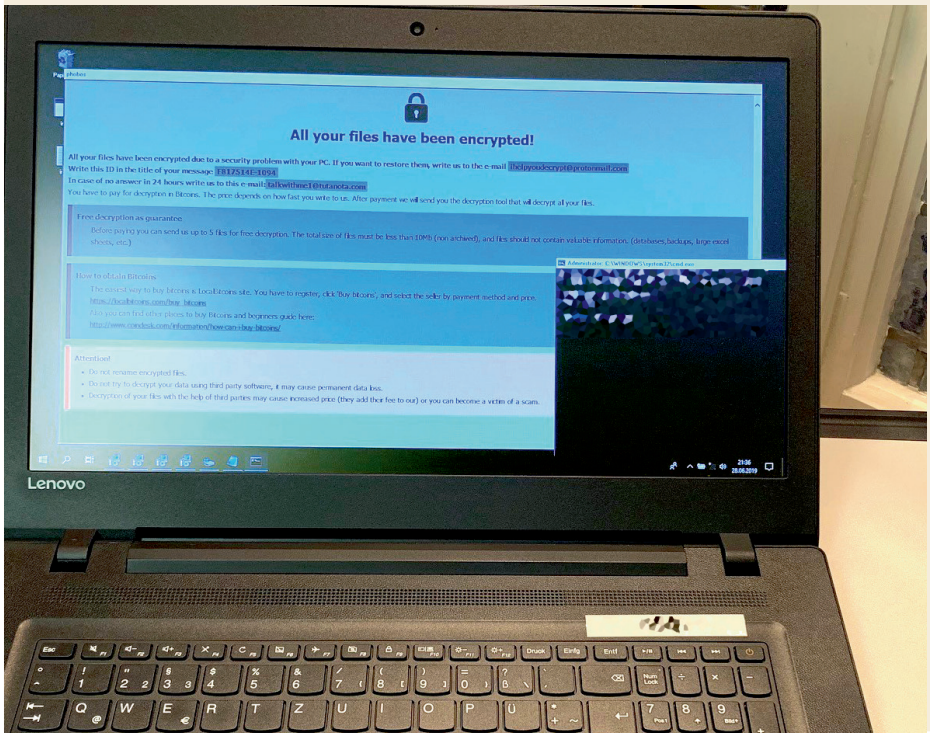
15.00 Uhr
El Rafei schreibt eine Rundmail an seine zwölf Mitarbeiter. Wer gerade Zeit hat, soll bitte alles stehen und liegen lassen und sofort ins Rathaus kommen. Auf freiwilliger Basis. Jetzt geht es darum, sämtliche Server anhand des einen sauberen Tapes wiederherzustellen. Er braucht also Verstärkung. Die Kollegen Julia Pappler, Timo Siegert und Maximilian Mayr melden sich sofort zurück. Sie haben Zeit, obwohl es Freitagnachmittag ist.

16.30 Uhr Das Rettungsteam trifft ein. Sie sind aus ganz Bayern gekommen – aus Sulzberg bei Kempten, aus Polling bei Mühldorf am Inn, aus München. Krisensitzung. Mittlerweile kocht ein Mitarbeiter der Gemeinde Spaghetti für das Interventionsteam der LivingData: Nudeln mit Tomatensoße und Parmesan.

17.00 Uhr
Die vier LivingData-Kollegen teilen sich in zwei Zweierteams auf. Hamed El Rafei und Maximilian Mayr bringen die Server wieder ans Laufen. Julia Pappler und Timo Siegert formatieren Rechner und Laptops komplett neu und binden sie ins Netzwerk ein. Es sind 27 an der Zahl. Nur das Notebook, das infiziert war, wird nicht angefasst. Es soll der Kriminalpolizei als Beweismaterial übergeben werden. Der Bürgermeister ist mittlerweile nach Hause gegangen, ist aber in ständigem telefonischen Kontakt.

23.00 Uhr
Alle PCs sind neu installiert. Kurz vor 24 Uhr ist der File-Server auch wiederhergestellt. Kurz vor Mitternacht ist auch der Mail-Server wieder am Netz.

Kurz nach Mitternacht: Es trifft die erste Mail ein. Jubel!



Am 28. Juni 2019 entdeckte ein Mitarbeiter der LivingData ein infiziertes Notebook. Darauf stand eine Erpresser-Nachricht.

Samstag, 29. Juni 2019

11.00 Uhr
El Rafei brieft den Bürgermeister telefonisch und rät ihm, eine Anzeige bei der Polizei zu erstatten …

13.00 Uhr
El Rafei trifft mit seinem Team wieder in der Gemeinde ein. Es wird heute zusätzlich durch den Kollegen Tim Seiffert verstärkt. Jetzt muss der AKDB-Server mit den Fachverfahren wiederhergestellt werden. Erst die Software fürs Einwohnermeldewesen OK.EWO, dann die restlichen Programme. Und zwar auf allen 27 PCs. Dabei ist die enge Zusammenarbeit im Team ausschlaggebend für den Erfolg. Die vier rufen sich immer wieder zusammen, um sich auszutauschen, wann welcher Server bereits wiederhergestellt ist. Zusätzlich wird die Firewall installiert und neu konfiguriert.

17.00 Uhr
Das Team gönnt sich eine Pause und geht kurz essen.

23.30 Uhr
Die Arbeit ist fast vollbracht! Am Montag sollen die individuellen Anpassungen gemacht werden.

Montag, 1. Juli 2019

7.20 Uhr
Es werden alle Apps und Tools wieder aufgespielt, die die einzelnen Mitarbeiter genutzt haben: Adobe, Schnittstellen zu Signatur-Tablets, Scanner, Druckertreiber. Um 18 Uhr ist das Team der LivingData fertig.

Dienstag, 2. Juli 2019

9.25 Uhr
Der Bürgermeister ruft bei LivingData an und teilt dem Team mit, dass die Polizei eine heiße Spur hat. Die Staatsanwaltschaft will den Schaden beziffern. Wenn man bedenkt, dass 18 Tage verloren gegangen sind und man das mal 27 Clients nimmt, dann ergibt sich ein Schaden von fast 100.000 Euro.

Und wie ging‘s dann weiter? Bis September kontollierte das Living-Data-Team mehrmals vor Ort, ob alles in Ordnung war. Sicher ist sicher.

i

Die LivingData GmbH, hundertprozentige Tochtergesellschaft der AKDB, plant und realisiert seit 1997 als bayernweit führendes System- und Softwarehaus speziell für Kunden aus dem öffentlichen Bereich maßgeschneiderte Hard-, Software- und IT-Security-Lösungen.
Experten der LivingData und der AKDB übernehmen und verantworten im sogenannten Next Generation Outsourcing-Modell den kompletten IT-Betrieb bayerischer Kommunen.

386_0919

AKDB, Hansastraße 12-16, 80686 München
Telefon 089 5903 0, Telefax 089 5903 1845, E-Mail mailbox@akdb.de, www.akdb.de