Hilfe, meine Daten sind verschlüsselt

Plötzlich erscheint auf dem Bildschirm die Meldung «Deine Daten sind verschlüsselt, bezahle eine Anzahl Bitcoins und du kommst wieder an deine Daten». In diesem Moment ist der Schock gross. Oft so, dass es nicht mehr möglich ist, an die eigenen Daten zu kommen. Der Hilfeschrei ist laut: Wie komme ich wieder an meine Daten?

Alleine im Dezember 2019 wurden in zahlreichen Firmen, Städten und Schulen die Daten verschlüsselt. Dazu gehören die Stadt Frankfurt a.M., die Uni Giessen, die Klinik Fürth, der Staat New Orleans und viele weitere. Auch der aktuelle Halbjahresbericht der MELANI (Schweizer Melde- und Analysestelle Informationssicherung) berichtet von zahlreichen Varianten und Angriffen in der Schweiz.

Unbedarft eine E-Mail geöffnet, den Anhang angeschaut und der Schädling kann losschlagen. Dabei werden nicht nur die Daten auf dem eigenen Gerät, sondern alle erreichbaren Daten verschlüsselt, sei dies ein Server-Laufwerk, ein USB-Stick oder das Backup im gleichen Netzwerksegment. Dann sind nicht nur die eigenen Daten auf dem Rechner verloren, sondern auch gleich noch das Backup mit. Nur gegen Bezahlung wird das Kennwort zum Entschlüsseln der Daten herausgegeben. Diese Art von Schädling wird Ransomware genannt. Wer genau hinter diesen Angriffen steht, ist in der Regel nicht nachvollziehbar. Im Internet stehen auch Mietmodelle verfügbar. Eine Ransomware kann für eine bestimmte Zeit gemietet werden, der Betreiber des Netzwerkes verdient an jeder Erpressung eine gewisse Anzahl an Prozenten mit (Ransomware as a Service).

Verschlüsselt mit einem mathematischen Verfahren

Einer der ersten dieser Art war CryptoWall, der zum ersten Mal im September 2013 im Internet entdeckt wurde. Die Verteilung erfolgt über E-Mails und ein Botnet. Ein Botnet sind von Hackern übernommene Rechner, die für die Verteilung des Schädlings genutzt werden. Wird CryptoWall ausgeführt, sucht er bestimmte Dateitypen wie .doc/.docx (Microsoft Word) und verschlüsselt diese mit einem mathematischen Verfahren (RSA, 2048 Bit). Das identische Verschlüsselungsverfahren wird auch für Webseiten genutzt, zum Beispiel, wenn Sie auf Ihr Online-Banking zugreifen. Es gilt somit als sehr sicher oder eben als nicht knackbar, eine Entschlüsselung der Daten ist ohne den dazugehörenden Schlüssel nicht mehr möglich. Der Benutzer wird in der Folge zu einer Webseite gelotst und erhält in einem Fenster die Anweisung, 500 Dollar in Bitcoins (eine virtuelle Währung im Internet, die anonym von einem Ort an einen anderen transferiert werden kann) zu bezahlen.

Ein Counter weist darauf hin, wie lange dies noch möglich ist. Nach Ablauf der Frist verdoppelt sich zwei Mal der Betrag, danach ist eine Entschlüsselung der eigenen Daten nicht mehr möglich, der dazu passende Wiederherstellungsschlüssel wird gelöscht. Verschiedene Quellen berichten, dass einige der betroffenen Personen bezahlen. Unter anderem war in der Tagespresse von einem Spital zu lesen, welches als einzige Lösung aus der Misere bezahlt hat. Je nach Quellen ergibt dies eine stolze Summe, die auch mal über eine Million US-Dollar betragen kann. Dies alleine ist ein grosser Antrieb, weiterhin auf diese Art Geld zu verdienen und eine Reduktion der Angriffe ist nicht zu erwarten. Ich vermute sogar, dass wir im Jahr 2020 richtiggehend mit Ransomware überschwemmt werden. Die Angriffe werden dabei auch gezielt entwickelt. Dies zeigen Varianten, die zuerst überprüfen, wer das Opfer ist. Handelt es sich dabei um eine grössere Firma oder gar um eine Behörde, wird der zu bezahlende Betrag massiv erhöht.

Bild: Archiv

Wie komme ich wieder an meine Daten?

Doch bekommt der Benutzer nun tatsächlich seinen Schlüssel, um die Daten wiederherzustellen? Bei einigen Opfern war dies tatsächlich der Fall, nach wenigen Stunden wurde das überwiesene Geld abgeholt und der Wiederherstellungsschlüssel mitsamt eines Programms übergeben. Damit konnten die Daten wiederhergestellt werden. Doch ob dies immer der Fall ist, ist nicht garantiert. Je nachdem wer hinter dem Schädling steht, kann dies auch ins Leere führen und die Daten sind mitsamt dem Geld für immer verloren. Daher gilt es genau zu überlegen, ob das organisierte Verbrechen mit unterstützt werden soll. Wird niemand mehr bezahlen, stellen sich die Angriffe automatisch wieder ein. Sind nur Windows-Benutzer davon betroffen? Nein, inzwischen sind auch Schädlinge für den Mac im Internet aufgetaucht. Die sicheren Zeiten für Mac-Benutzer sind schon länger vorbei und es ist grosse Vorsicht geboten.

Kann ich mich überhaupt davor schützen?

Doch wie verbreiten sich diese Schädlinge? Oft ist es der Weg via E-Mail. Aus irgendwelchen Quellen, zum Beispiel aus gestohlenen Passwörtern und E-Mail-Adressen oder dem Absuchen von

Webseiten, analog wie dies Google für das Indexieren von Webseiten macht, werden E-Mail-Adressen beschafft. Diese erhalten dann die Aufforderung, eine beiliegende Datei zu öffnen. Immer öfters ist auch von perfekt und fehlerfrei geschriebenen Bewerbungsschreiben, als manipuliertes Word- oder PDF-Dokument getarnt, zu hören. Auch eine E-Mail mit einem Link zu einer Datei auf Dropbox wurde schon entdeckt – die Kreativität der Ransomware-Entwickler ist dabei unerschöpflich, um nicht aufzufallen oder das Antivirenprogramm zu täuschen. Auch werden massenhaft Webseiten infiziert. Durch eine vorhandene Schwachstelle kopiert sich der Schädling auf die Webseite. Besucht nun jemand eine solche verseuchte Webseite, kann es sein, und der Schädling beginnt ohne eigenes Dazutun mit der Verschlüsselung der erreichbaren Daten.

Kann ich mich überhaupt noch davor schützen? Ja, das ist möglich. Beachten Sie einige Punkte, um sich weiterhin vor Malware zu schützen: Halten Sie Ihr System immer auf dem aktuellsten Stand. Installieren Sie die Updates (auch Patches genannt), die Microsoft, Apple und die vielen Software-Entwickler herausgeben. Vergessen Sie dabei nicht die anderen Programme, wie Office, Google Chrome, Firefox, Adobe Reader, Flash usw.

Da sammelt sich doch einiges mit der Zeit an. Eine oft mühsame, aber enorm wichtige Aufgabe. Weiter gilt es, das Antivirenprogramm aktuell zu halten. Trotz dem aktuellen Antivirenprogramm ist Vorsicht geboten, nicht immer werden neue Varianten sofort erkannt! Daher gilt als dritter Punkt: klicken Sie nicht alles an, auch wenn es noch so spannend erscheint. Prüfen Sie jeden Link in einer E-Mail, bevor Sie daraufklicken. Führen Sie die Maus über den Link und verifizieren Sie, wohin die Reise wirklich führt.

Was ist, wenn es doch mal passiert? Da hilft oft nur eines, das Wiederherstellen der Daten aus dem Backup, Restore genannt. Daher gehört aber zu den wichtigsten Vorbereitungsaufgaben das Erstellen von regelmässigen Datensicherungen. Das reine Synchronisieren mit einem Netzwerkspeicher (NAS genannt) hat sich dabei als trügerische Sicherheit erwiesen. Ist dieser Speicher ständig verbunden oder über das Netzwerk erreichbar, verschlüsseln aktuelle Versionen der Schädlinge auch diese Daten. Sie benötigen daher ein Backup an einer externen Stelle. Dies kann zum Beispiel eine Wechselplatte oder ein grosser USB-Stick sein, den Sie wieder vom Rechner entfernen. Sollten Sie den Schädling auf dem Rechner haben, entfernen Sie diesen, bevor Sie die Festplatte anhängen. Erst wenn Sie ganz sicher sind, dass alles in Ordnung ist, spielen Sie Ihre vorher gesicherten Daten zurück.

Fazit

Die Betrüger finden immer neue raffinierte Wege um damit viel Geld zu verdienen. Da es mit den heutigen technischen Möglichkeiten nicht mehr möglich ist, an die verschlüsselten Daten zu kommen, ist es enorm wichtig, im Vorfeld für eine umfassende und geschützte Datensicherung zu sorgen. Im Internet gilt es Vorsicht walten zu lassen, und nicht jedes E-Mail, jeden Anhang oder jede Webseite anzuklicken und im Vorfeld zu überlegen, will ich das wirklich? Nur so können Sie sich optimal vor den aktuellen Gefährdungen schützen.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch