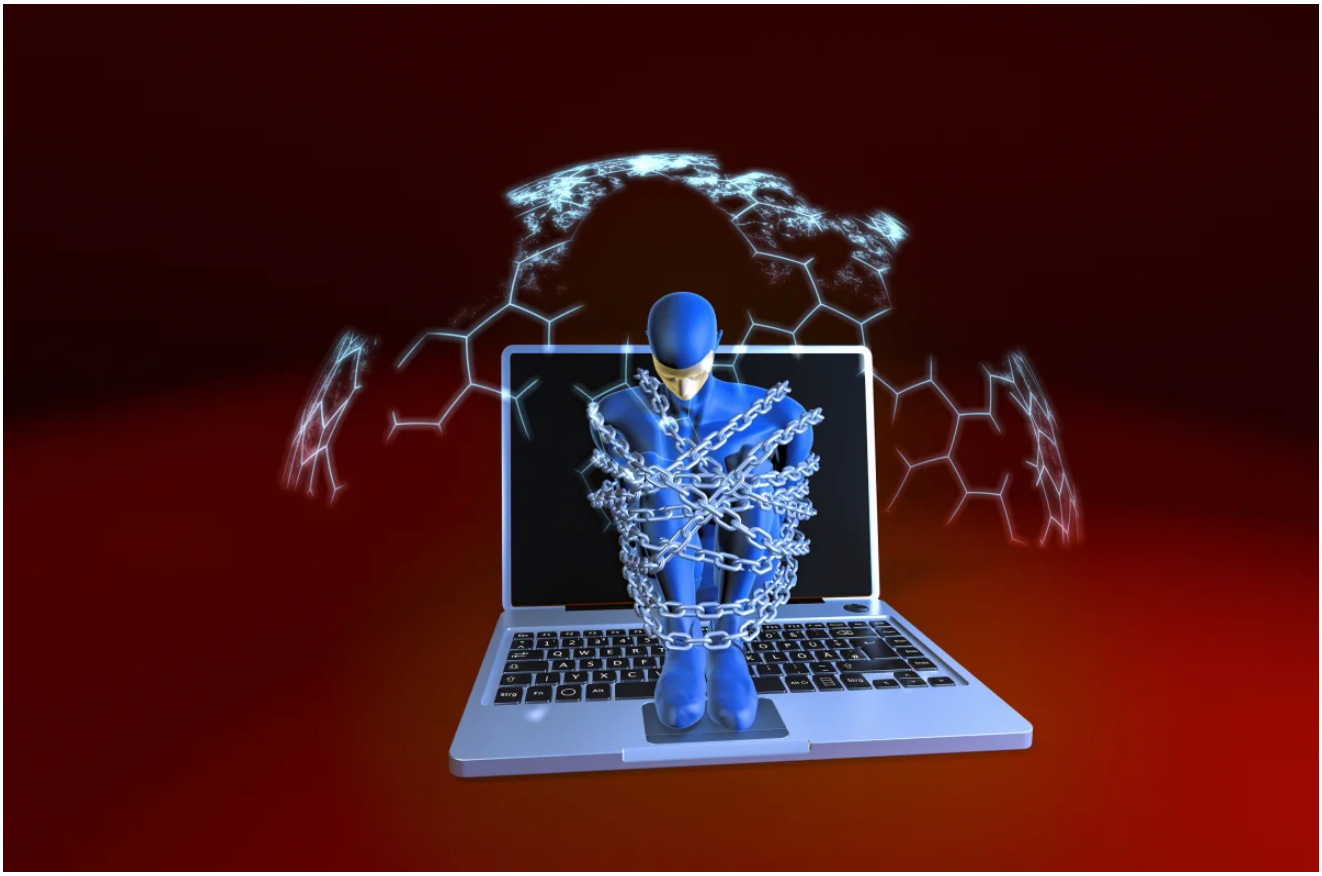
Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen

heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html

Christian Wölbert



WISSEN | HINTERGRUND

Christian Wölbert
02.03.2020
Emotet, Kryptotrojaner, Schadsoftware, Security, Viren

Im niedersächsischen Neustadt am Rübenberge hat der Trojaner Emotet mit voller Wucht zugeschlagen. Nun spricht die Stadtverwaltung offen über das Desaster, damit andere daraus lernen.

Am Morgen des 6. September 2019 bemerkte ein Mitarbeiter der IT-Abteilung der Stadtverwaltung von Neustadt am Rübenberge etwas Seltsames. Sein Monitor zeigte ihm eine extrem hohe Auslastung der Server im Rechenzentrum der Kommune – obwohl keine Tests oder Wartungsarbeiten anstanden. Es könnte Schadsoftware am Werk sein, folgerte der Mitarbeiter. Sicherheitshalber fuhr er die Server sofort herunter.

Doch da war es längst zu spät. Schon am Vorabend oder in der Nacht hatten Unbekannte damit begonnen, die Server der Verwaltung der niedersächsischen 45.000-Einwohner-Stadt zu verschlüsseln. Mails und Formulare, Flächennutzungspläne und Bauzeichnungen, die Hochzeitstermine des Standesamts und Elterngeldanträge – der eingeschleuste Kryptotrojaner machte vor nichts Halt.

c't-Schwerpunkt: Emotet verstehen und abwehren

- Lehrreicher Emotet-Angriff auf Neustadt
- Wie eine Infektion verläuft

- So schützen Sie sich vor Emotet
- Im Notfall richtig reagieren

Ein halbes Jahr später berichtet Maic Schillack, Erster Stadtrat und Stellvertreter des Bürgermeisters, von dem Moment, als seine Mitarbeiter ihn informierten. „Das Schlimmste für mich als Kämmerer war, dass die Daten der Buchhaltungssoftware verschlüsselt wurden“, sagt er. „Darunter 220.000 digitale Steuerakten und 350.000 Adressen von Debitoren und Kreditoren.“

Der Malware-König

Emotet ist eines der zerstörerischsten – man könnte auch sagen: erfolgreichsten – Schadprogramme der IT-Geschichte. Viele Betroffene fahren alle Server und PCs herunter, schicken Mitarbeiter nach Hause, stellen ihre Dienstleistungen oder die Produktion ein. Die Schadenssumme geht dann schnell in die Millionen. Aus Sicht von Arne Schönbohm, Chef des Bundesamts für Sicherheit in der Informationstechnik (BSI), ist Emotet deshalb „der König der Schadsoftware“.

Allein in Deutschland wurden in den vergangenen beiden Jahren Dutzende verheerende Fälle bekannt. Im November 2018 schaltete das Klinikum Fürstenfeldbruck nach einer Emotet-Infektion alle 450 Rechner im Haus ab und meldete sich bei der Rettungsleitstelle ab. Im September 2019 ging das Berliner Kammergericht offline, im Dezember die Uni Gießen. Beide arbeiten immer noch am Neuaufbau ihrer IT. Auch die Medizinische Hochschule Hannover, die Katholische Hochschule Freiburg, die Stadtverwaltung von Frankfurt am Main und viele weitere wurden infiziert.

Die Fälle bei Behörden und Hochschulen bilden nur die Spitze des Eisbergs. Laut BSI wurden allein binnen weniger Tage im September „mehrere tausend E-Mail-Konten von Unternehmen und Bürgern“ durch Emotet kompromittiert und für den Spam-Versand missbraucht. Es hat also auch viele Firmen erwischt – die aber nicht davon berichten, wohl aus Sorge um ihre Reputation und aus Angst vor weiteren Angriffen.

Zu den wenigen Firmen, die ihre Erfahrungen publik gemacht haben, gehört Heise. Im Mai 2019 traf Emotet die Heise Gruppe, das Mutter-Unternehmen des c’t-Verlags Heise Medien. Es ging einigermaßen glimpflich aus: Die Firma wurde nicht komplett lahmgelegt, es wurden keine Daten verschlüsselt [1]. Massivere Schäden richtete Emotet in Neustadt an. Der Fall eignet sich deshalb, um beispielhaft zu erzählen, warum der Trojaner so schwer zu stoppen ist, welche Folgen der Befall haben kann – und welche Lehren sich daraus ziehen lassen.

Der Begriff Emotet

Im Jahr 2014 entdeckte die Sicherheitsfirma Trendmicro ein neues Schadprogramm, das sie auf den Namen Emotet taufte. Kriminelle spähten mit der Software damals Bank-Zugangsdaten aus. Mittlerweile dient Emotet jedoch vor allem als „Dropper“, er lädt also weitere Schadprogramme nach. Typischerweise sind das Trickbot und der Verschlüsselungstrojaner Ryuk.

Emotet gelangt in der Regel über Spam-Mails auf Rechner, entweder durch ein Office-Dokument mit Makros im Anhang oder über einen Download-Link. Manchmal wird der Begriff Emotet auch verwendet, um das Gesamtsystem aus Spam-Mails, Anhängen oder Download-Links und dem eigentlichen Schadprogramm zu beschreiben.

Durchschlagskräftige Spam-Mails

Maic Schillack weiß zwar nicht, auf welchem Wege die Stadtverwaltung von Emotet befallen wurde. Wahrscheinlich ist aber, dass ein Mitarbeiter eine gefälschte E-Mail mit einem verseuchten Office-Dokument (z. B. .doc) im Anhang erhalten hat. Das war laut den Analysen von Antiviren-Firmen und Sicherheitsbehörden zumindest bislang die typische Angriffsmethode der Emotet-Gangster. Öffnet jemand das Dokument und folgt der Aufforderung, Makros zu aktivieren, nimmt das Unheil seinen Lauf.

Was Emotet so mächtig macht, ist die perfide Aufmachung der Mails. Sie stammen aus Sicht des Empfängers offenbar von einer tatsächlich existierenden Kontaktperson und zitieren einen realen Mailwechsel zwischen dem Empfänger und dieser Person. Im Fall von Heise wurde ein Mitarbeiter scheinbar von einem Geschäftspartner aufgefordert, Daten in einem angehängten Dokument auf Aktualität zu prüfen. So schafft es Emotet, auch vorsichtige Menschen zum Öffnen des Anhangs zu bewegen.

Die erstaunlich echt wirkenden Mails werden nicht mühsam von Hand gefälscht, sondern automatisch und massenweise. „Emotet ist in der Lage, Outlook-Konversationen (Kontaktbeziehungen und Mailinhalte) auszulesen und so automatisiert sehr authentische Spam-Mails zur Erstinfektion zu generieren“, erklärt das BSI. Emotet verbindet also die Durchschlagskraft von Social Engineering mit der Breitenwirkung einer Spam-Kampagne – Fachleute sprechen von Dynamit-Phishing.

Scanner-Versagen

Ein weiterer wesentlicher Faktor: Virenscanner konnten die Infektionen zumindest bislang oft nicht verhindern. In Neustadt hätten die Scanner zwar – rund sechs Monate vor dem Verschlüsselungs-GAU – auf einigen Arbeitsplatzrechnern Alarm geschlagen, erinnern sich Stadtrat Maic Schillack und der Leiter der IT-Abteilung, Tobias Niemeyer. Nach dem Neuaufsetzen der PCs habe es aber bei mehreren Vollscans keinen Alarm mehr gegeben. Die Antiviren-Software sei stets aktuell gewesen.

Das erinnert an die Vorgänge bei Heise. Hier hatten die Virenwächter an einem Montag zwar einen Angriff gemeldet, nach oberflächlichen Reinigungen schien aber wieder alles in bester Ordnung zu sein – bis Emotet zwei Tage später plötzlich Verbindungen zu Kontrollservern aufbaute. Die AV-Software hatte also anscheinend auf einigen befallenen Systemen nicht angeschlagen oder Teile der Schadsoftware nicht als solche erkannt.

Im Berliner Kammergericht hat AV-Software von McAfee offenbar auf ganzer Linie versagt. „Diese hat Malware, die zum Zeitpunkt der Infektion bereits bekannt war, nicht erkannt“, stellte T-Systems in einer von der Berliner Justiz veröffentlichten Analyse fest.

Eine Erklärung hat Andreas Marx, Chef des Magdeburger Antiviren-Testlabors AV-Test. „Die Macher hinter Emotet & Co. prüfen ihre neuen Kreationen immer gegen alle gängigen Virenscanner“, sagt er. Die Gangster berücksichtigten dabei sowohl die statischen Signaturen der Scanner als auch ihre dynamische Erkennungsmethoden.

Katz- und Maus-Spiel

Haben die Emotet-Macher einen Weg gefunden, populäre Antiviren-Software auszutricksen, feuern sie eine Salve Mails ab. Die Antiviren-Hersteller aktualisieren dann meist binnen weniger Tage ihre Programme – und das Katz- und Maus-Spiel beginnt wieder von vorn. Zum Beispiel verzichteten die Kriminellen im Dezember plötzlich auf Dateianhänge und setzten stattdessen Download-Links in die Mails.

Nach der Infektion lädt Emotet meistens weitere Schadsoftware nach. „Emotet ist nur der Ursprung allen Übels, die enorme Schadenswirkung wird durch ein schrittweises Vorgehen der Täter erreicht“, erklärt das BSI. Typischerweise wird zunächst das Tool Trickbot eingesetzt. Dieses kann unter anderem Zugangsdaten ausspähen und sich weitgehend automatisiert im Opfer-Netzwerk ausbreiten. (Im Artikel ab Seite 18 schildern wir den Prozess detaillierter.)

Im nächsten Schritt schauen die Gangster sich aus der Ferne bei ihrem Opfer um: Um was für eine Organisation handelt es sich? Wie hoch ist der Jahresumsatz? Wo befinden sich die wichtigsten Daten und Backups?

Anschließend entscheiden sie, wie sie das meiste aus ihrer Geisel herausholen. Sie können zum Beispiel Daten verschlüsseln oder mit Veröffentlichungen drohen, um Lösegelder zu erpressen. Sie können aber auch heimlich Kryptowährungen auf den Systemen schürfen – oder den Zugang an andere Kriminelle verkaufen. „Das funktioniert wie bei einem geklauten Auto. Der Dieb kann es eine Weile selbst fahren, es weiterverkaufen oder ausschlachten“, sagt AV-Test-Chef Marx.

Wer steckt hinter Emotet?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist davon überzeugt, dass „die Entwickler von Emotet ihre Software und ihre Infrastruktur an Dritte untervermieten“. Diese setzten dann weitere Schadsoftware wie Trickbot und Ransomware ein, um „ihre eigenen Ziele zu verfolgen“. Die Motivation sei in der Regel finanzieller Natur. Das BSI geht also von Cyberkriminalität aus, nicht von Spionage.

Zur spannenden Frage, aus welchem Land oder aus welchen Ländern die Emotet-Entwickler und die Angreifer kommen, äußert sich das BSI nicht. Auch aus den Strafverfolgungsbehörden sind dazu bislang keine Erkenntnisse nach außen gedrungen. Es kursieren lediglich Gerüchte, in denen von Osteuropa oder Russland die Rede ist. Malware-Experte Andreas Marx von der Firma AV-Test betont jedoch: „Es gibt viele Vermutungen, aber eine Attribution ist nicht seriös möglich.

Gezielte Verschlüsselung

Im Fall von Neustadt haben die Gangster – wie in vielen anderen Fällen – den Verschlüsselungstrojaner Ryuk eingesetzt. Stadtrat Schillack und IT-Mann Niemeyer wissen das, weil am Morgen des 6. September eine HTML-Datei mit dem Schriftzug „Ryuk“ und zwei E-Mail-Adressen auf dem Bildschirm eines Arbeitsplatzrechners erschien, eine Art Bekennerschreiben der Cybergangster.

Schillack und seine Mitarbeiter versuchten als Erstes, den Schaden zu begrenzen: Alle Angestellten der Stadt wurden mündlich angewiesen, ihre Rechner herunterzufahren und auf keinen Fall wieder einzuschalten. Gleichzeitig forderte die Verwaltung externe Partner telefonisch auf, keine Mails der Neustädter zu öffnen und selbst nach Schadprogrammen zu suchen. Schillack ließ außerdem die Konten der Stadt sperren und informierte die Polizeibehörden und die Landesbeauftragte für den Datenschutz.

Beamte des Landeskriminalamtes und der Polizei trafen noch am selben Morgen in Neustadt ein und begannen mit der Analyse, um die Schadsoftware zu identifizieren und das Ausmaß der Verschlüsselung einzuschätzen.

Die gute Nachricht: Es gab noch ein unverschlüsseltes, nur 24 Stunden altes Backup der Buchhaltungsdaten. Allerdings erfuhren Schillack und Niemeyer auch viele schlechte Neuigkeiten. Der Trojaner hatte zahlreiche andere Datenbanken sowie einige Backups verschlüsselt. Auf dem zentralen Fileserver der Stadt wurden etwa 550.000 Dateien verschlüsselt, etwa 830.000 blieben verschont.

Alles aus: Systeme herunterfahren

Die Stadtverwaltung musste nun eine weitreichende Entscheidung treffen: Sollte sie die offenkundig verseuchten Rechner und Server reinigen und den Rest weiterlaufen lassen? Oder sollte sie sicherheitshalber alle Systeme herunterfahren und neu aufsetzen?

Schillack und Niemeyer entschieden sich nach Rücksprache mit dem BSI und früheren Emotet-Opfern für die zweite Option. Nur so habe man ausschließen können, dass die Malware sich irgendwo versteckt und erneut ausbreitet, sagen die beiden.

Damit war die Stadtverwaltung von Neustadt mit ihren rund 560 Mitarbeitern weitgehend lahmgelegt. Fast alle Bürgerdienste – von der Ausstellung der Geburtsurkunde über die Ehe-Anmeldung bis zur Übernahme von Bestattungskosten – mussten vorerst eingestellt werden. Die Verwaltung konnte auch keine Zahlungen mehr leisten. Deshalb mussten zum Beispiel Familien vorerst auf Elterngeld und damit auf einen großen Teil ihres Einkommens verzichten.

Auch in anderen Emotet-Fällen haben sich die Verantwortlichen für die Abschaltung und einen weitgehenden Neuaufbau entschieden – zum Beispiel am Kammergericht Berlin. Immer wieder kommt es zum Totalausfall kompletter IT-Infrastrukturen, zu Produktionsstillständen oder der Nichtverfügbarkeit von Dienstleistungen fasst das BSI zusammen.

Zurück auf Los: Neue Infrastruktur

Schillack und Niemeyer versuchten nun, die Ausfallzeit zu minimieren. Für den Neuaufbau rekrutierten sie Verstärkung von einem kommunalen IT-Dienstleister und einem privaten Systemhaus. Zusammen mit eigenen IT-Leuten hatten sie nun etwa 30 ITler vor Ort. Ein Team baute die Infrastruktur neu auf, richtete Server und Netze wieder ein. Das zweite Team lief von Büro zu Büro und setzte die insgesamt rund 300 Arbeitsplatzrechner neu auf.

Es dauerte eine Woche, bis die Verwaltungsmaschinerie langsam wieder in Tritt kam. Zuerst nahmen die Meldebehörde und das Standesamt die Arbeit wieder auf, danach folgten Schritt für Schritt weitere Abteilungen. Die ungeplanten Mehrausgaben für den IT-Neuaufbau schätzt Schillack auf 100.000 bis 150.000 Euro.

„Mittlerweile sind wir zu 95 Prozent wieder einsatzfähig“, sagt er Ende Januar gegenüber c’t. Alle Anwendungen für Bürgerdienste liefen wieder. Viele verschlüsselte Dateien habe man aus sauberen Backups oder von externen Partnern wieder eingespielt. Anderes habe man notgedrungen neu erstellt, etwa die Pläne für ein Neubaugebiet.

Achtstellige Lösegelder

Eventuell wird die Stadtverwaltung sich dann noch mit einem besonders heiklen Thema auseinandersetzen müssen: Die Emotet-Gangster haben Neustadt angeboten, verschlüsselte Daten gegen Lösegeld wieder zu entschlüsseln. Anders gesagt: Sie erpressen die Stadt.

Die Stadtverwaltung verrät nicht, wie die Lösegeldforderung präsentiert wurde, wie hoch die geforderte Summe ist und ob man sie notfalls zahlen würde. Sie erklärt lediglich, dass sie bislang nichts gezahlt habe. Auch das LKA Niedersachsen, das in dem Fall ermittelt, äußert

sich nicht dazu.

Laut BSI passen die Emotet-Macher ihre Lösegeldforderungen an den Wert der verschlüsselten Daten und an die Finanzkraft ihrer Opfer an. „Dabei wurden in Einzelfällen bis zu achtstellige Lösegelder gefordert.“ Auch das ist eine Besonderheit: Bei früheren Ransomware-Kampagnen forderten die Gangster in der Regel von allen Opfern die gleiche Summe.

Neustädter Lehren

Welche Lehren lassen sich nun aus dem verheerenden Cyberangriff auf Neustadt ziehen? Stadtrat Schillack und IT-Chef Niemeyer legen Wert auf die Feststellung, dass die IT-Systeme der Stadt auch vorher „absolut zeitgemäß“ gewesen seien. Nun achte man aber durchaus noch stärker auf Sicherheit.

Auf technischer Ebene habe man zum Beispiel strengere Regeln für Mail-Anhänge eingeführt. Alte Office-Formate wie DOC sowie verschlüsselte ZIP-Dateien würden nicht mehr akzeptiert – was im Alltag immer wieder zu Diskussionen mit anderen Behörden führe, die noch DOC-Dateien versendeten, sagt Niemeyer. Das neue Netzwerk habe man zudem streng segmentiert, um Schädlingen die Ausbreitung zu erschweren. Ein Sicherheitstest durch externe Experten sei geplant.

Außerdem habe man wieder Bandsicherungen eingeführt: Bänder mit essenziellen Daten lägen im feuerfesten Tresor der Stadt und in einem Bankschließfach. Damit könne man nach Notfällen die Grundstruktur der IT schnell wiederherstellen. Hinzu kämen wöchentliche Backups aktueller Daten auf weiteren Bändern. „Diese sind offline, also gibt es keine Angriffsmöglichkeit“, betont Niemeyer.

Niemals wirklich sicher

Mindestens ebenso wichtig wie die Technik ist aus seiner Sicht allerdings das Verhalten der Mitarbeiter. „Das größte Einfallstor in der heutigen Welt ist nicht die Technik, sondern Social Engineering.“ Die Angestellten der Stadt seien nun – durch den verheerenden Emotet-Angriff – schon sehr vorsichtig geworden. „Der letzte September war die ultimative Awareness-Schulung.“ Trotzdem werde man Schulungen durchführen, auch mit externen Experten.

Absolute Sicherheit könne es trotz all dieser Maßnahmen niemals geben, betont Niemeyer. „Die Frage ist nicht, ob man befallen wird, sondern wann.“ Man müsse also auf den Notfall vorbereitet sein – und dann schnell und konsequent handeln. „Jemand muss Entscheidungen fällen, statt um den heißen Brei herumzureden.“

Auch Stadtrat Schillack hofft, dass andere aus solchen Erfahrungen aus Neustadt lernen. Außerdem ruft er betroffene Unternehmen auf, Cyberangriffe bei der Polizei anzuzeigen. Die Ermittler gingen „sehr sensibel“ damit um, betont er, und könnten nur durch Anzeigen das

Verhalten der Angreifer nachvollziehen. „Entscheidend ist für mich die Frage, ob wir durch unseren Vorfall etwas verändern.“ (cwo)

Dieser Artikel stammt aus c't 6/2020.

KOMMENTARE

Kommentare lesen (818 Beiträge)