Banking-Trojaner

So schützen Sie Ihre Praxis vor Emotet

Die Erpressersoftware Emotet hat nicht nur Behörden und Privatanwender in Mitleidenschaft gezogen. Auch Praxen und Kliniken sind gefährdet. Doch wie arbeiten die Hacker? Und welche Maßnahmen können einen Angriff abwehren?

Eine Schadsoftware, der zahlreiche Betriebe und Behörden, aber auch Praxen und Krankenhäuser zum Opfer fielen, hat in den vergangenen zwei Jahren zweifelhafte Berühmtheit erlangt: der „Banking-Trojaner" Emotet.

Vorgehen und Ziele der Angreifer sind immer die Gleichen: Nachdem sie potenziellen Opfern per Phishingmail Schadsoftware untergeschoben haben, sehen sie sich zunächst auf den Rechnern in einem Netzwerk um und verschlüsseln dann alle relevanten Daten. Anschließend verlangen sie horrende Lösegelder für die Zusendung des passenden Entschlüsselungswerkzeugs.

Da die Schadsoftware den kompletten Geschäftsbetrieb blockiert, zahlen viele Betroffene stillschweigend – sei es, weil sie zu Recht massive wirtschaftliche und Reputationsschäden befürchten oder weil es, wie im Falle von Krankenhäusern, buchstäblich um Leben und Tod geht.

Wer ist gefährdet?

Obwohl die Auswirkungen einer Emotetattacke durchaus drastisch sind und ein entsprechendes Medienecho verursachen, sind die meisten Anwender nicht darauf vorbereite. Gefährdet sind neben Behörden und Unternehmen wie großen Kliniken und Pharmafirmen auch kleinere Praxen und Privatanwender: Emotet zielt besonders auf Nutzer von Microsofts Betriebssystem Windows und den dazugehörigen Office-Anwendungen, die auf knapp 90 % aller weltweit genutzten PC laufen. Das gilt auch für niedergelassene Ärzte, zumal diese mit besonders sensiblen Patientendaten hantieren und somit leicht zum Ziel von Erpressern werden.

Praxis-IT von Hackern geknackt? Soweit sollte es erst gar nicht kommen.

Wie sieht eine typische Emotetattacke aus?

Der Angriff erfolgt in der Regel in vier Schritten:

- Sie erhalten eine E-Mail, an die ein scheinbar wichtiges Dokument (Rechnung, Vertrag) angehängt ist; meist eine Worddatei, manchmal auch eine Excel-Tabelle oder ein PDF. Beim Öffnen der Datei erscheint eine Aufforderung, das dazu benötigte Programm zu aktivieren. Eine Weiterbearbeitung des Dokuments ist aber nicht möglich. Zusätzlich erscheint auf dem Bildschirm ein gelber Balken mit der Mitteilung, dass „Makros deaktiviert" sind sowie einem Schalter mit der Aufschrift „Inhalte aktivieren". Wer darauf klickt, hat Emotet installiert.
- Nun übermittelt Emotet alle Kontaktdaten aus Outlook sowie alle E-Mails der letzten sechs Monate an einen Server der Angreifer.
- Weitere Komponenten werden nachgeladen. Die Cyberkriminellen können sich nun Zugriff auf Patientendatenbanken, Medikamentenbestellungen oder Finanzdaten verschaffen.
- Haben die Angreifer alle Informationen abgeschöpft, folgt als letzter Schritt die Verschlüsselung und PC-Sperrung samt Lösegeldforderung.

Fünf Maßnahmen gegen Emotet

Selbst für Experten ist es schwierig, sich gegen Emotetangriffe zu schützen. Dennoch können Sie einige grundlegende Maßnahmen treffen, um den Schaden solcher Cyberattacken zu begrenzen:

- Achten Sie auf Sicherheitswarnungen der Softwarehersteller und Browseranbieter. Installieren Sie Sicherheitsupdates spätestens am Tag nach Erscheinen.
- Legen Sie regelmäßig Offlinekopien aller wichtigen Patienten-/Therapiedaten an, halten Sie diese stets aktuell. Speichern Sie diese Kopien auf externen Festplatten oder Bandlaufwerken, die nach dem Kopiervorgang wieder von Firmennetz und Internet getrennt und separat aufbewahrt werden.
- Nutzen Sie Antivirenprogramme und stellen Sie diese so ein, dass sie regelmäßig automatische Updates vom Hersteller bezieht.
- Schulen Sie Ihr Personal: Mails mit unerklärlichen Rechnungen oder unerwarteten Schriftstücken im Anhang können Zeichen für einen Emotetangriff sein. Solche Anhänge dürfen niemals geöffnet werden. Das gilt auch für Mails aus normalerweise vertrauenswürdiger Quelle, da Emotet sich gern in gefälschten Anschreiben von seriösen Unternehmen, Geschäftspartnern oder gar Kollegen versteckt. Im Zweifel klärt ein Rückruf, ob die Mail vom vorgeblichen Absender stammt.
- Unterbinden Sie strikt die Ausführung von Makros. Das funktioniert in Office-Programmen wie folgt: Per Klick gehen Sie auf „Datei", dann „Optionen" und erreichen dort das „Trust Center". Einmal eingestellt, gilt die Regel für alle Office-Anwendungen – von Word bis PowerPoint.

Thomas Böcker