Ressort: Technik

IT-Sicherheitsexperten knacken Verschlüsselung von E-Mails

Münster, 14.05.2018, 13:48 Uhr

GDN - Einem Team aus IT-Sicherheitsforschern ist es gelungen, die Verschlüsselung von E-Mails auszuhebeln. Das berichten die "Süddeutsche Zeitung" (Dienstagsausgabe), NDR und WDR. Betroffen sind demnach die zwei meistverwendeten Verfahren für die Verschlüsselung von E-Mails: S/Mime und PGP. Firmen verwenden in der Regel S/Mime, Aktivisten, Whistleblower und Journalisten hingegen PGP. Das Team hat zwei unterschiedliche Wege gefunden, um die Verschlüsselung von E-Mails auszuhebeln.

Sebastian Schinzel, Professor für Angewandte Kryptografie der FH Münster, hat die Forschung geleitet. "E-Mail ist kein sicheres Kommunikationsmedium mehr", sagte er den drei Medien, die den Prozess über Monate begleiten konnten und mit unabhängigen IT-Sicherheitsexperten redeten, die die Ergebnisse der Forscher bestätigten. Bei verschlüsselten E-Mails werden zwei Schlüssel generiert. Einer ist öffentlich, einer privat. Solange der private Schlüssel gut geschützt wird, so dachte man, ist es egal, ob jemand die E-Mail abfängt. Man bekäme nur Datenwust zu sehen. Die Arbeit der Forscher zeigt, dass die Nachrichten doch entziffert werden können, auch wenn sie jahrealt sind. Im Kern funktioniert das Knacken der Mails so: Die Angreifer wollen einen Firmenchef ausspähen. Sie wollen wissen, über welche Themen sich der Chef in den vergangenen Jahren unterhielt. Die Angreifer besitzen den Ciphertext, also den Datenwust. Diesen präparieren sie und verschicken ihn an den Chef. Der Text der E-Mail kann vollkommen unverfänglich sein, zum Beispiel eine Einladung zum Kaffee. Aber in derselben Mail wird, ohne, dass es für das bloße Auge sichtbar wäre, der Datenwust versteckt. Der Computer öffnet die Botschaft und erkennt den Datenwust und stellt fest, dass er den verschlüsselten Text entziffern kann. Schließlich verfügt er über den Privatschlüssel. Kaum ist der Text entziffert, wird er an eine Seite verschickt, die die Angreifer kontrollieren. Der Angriff der Forscher basiert auf zwei Bedingungen: Erstens, sie besitzen den Ciphertext, also den Datenwust. Zweitens, im E-Mailprogramm wird HTML erlaubt. Nur dank HTML lassen sich zum Beispiel die Links in einer E-Mail anklicken. Die Mail wird so abgeändert, dass sie Elemente nachlädt, also Webseiten besucht, die die Forscher bestimmen können. Ähnliches passiert, wenn in E-Mail-Signaturen zum Beispiel das Firmenlogo auftauchen soll. Das Logo muss erst einmal nachgeladen werden. Durch dieses Nachladen können die E-Mails an die Angreifer verschickt werden. Wird HTML deaktiviert, lässt sich der Angriff stoppen. "Es ist natürlich eine schlimme Sicherheitslücke", sagte Arne Schönbohm, Chef der für IT-Sicherheit zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI), den drei Medien. "Gerade wenn Sie Dinge verschlüsseln, wollen Sie, dass es hier einen hohen Grad der Vertraulichkeit gibt und dass der auch gewahrt bleibt. Durch eine falsche Konfiguration, wenn man bestimmte Sicherheitsmaßnahmen nicht trifft, ist die Vertraulichkeit nicht gewahrt."

Bericht online:
https://www.germandailynews.com/bericht-106069/it-sicherheitsexperten-knacken-verschluesselung-von-e-mails.html

Redaktion und Veranwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV:

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168

Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com