

## Massive Sicherheitslücke bei Google Mail: Filter erlaubt unbemerkten E-Mail-Diebstahl

- Heimliche Weiterleitung zwar komplex, aber möglich
- Abwehr für Firefox-Browser via Erweiterung erhältlich



Googles Webmail-Angebot hat eine Sicherheitslücke, durch die Angreifer unbemerkt sämtliche E-Mails von einem bestimmten Absender stehlen können. Der eigentliche Besitzer des E-Mail-Kontos dagegen bekommt die Nachrichten gar nicht mehr zu sehen. Die Attacke basiert darauf, dass der Angreifer ohne Wissen des Account-Besitzers einen Nachrichtenfilter setzt, wird in einer Konzeptdarstellung auf dem Techblog GeekCondition beschrieben. Der Trick dürfte von Kriminellen genutzt worden sein, um Support-Nachrichten eines Registrars abzufangen und so Domains zu stehlen. "Das ist ein profitabler Grund für solche Tricks", meint Joe Pichlmayr, Geschäftsführer bei Ikarus.

Um einen Nachrichtenfilter für Gmail zu erstellen, wird eine Anfrage-URL mit mehreren Variablen an die Google-Server geschickt. Um einen Gmail-Nutzer anzugreifen, muss ein Hacker zunächst die Variable entsprechend dem User-Namen ermitteln. Das sei zwar kompliziert, doch wie es geht, sei durch intensive Suche im Internet herauszufinden. Ferner muss der Wert einer zweiten Variable gestohlen werden, die einem Authorisierungs-Cookie entspricht. Gelingt das mithilfe einer entsprechend präparierten Webseite, kann der Hacker auch gleich heimlich eine Anfrage an den Google-Server schicken, um einen Nachrichtenfilter zu erstellen. Dieser dient dann dazu, die E-Mails eines bestimmten Absenders direkt an den Cyberkriminellen weiterzuleiten und gleichzeitig aus der Inbox des manipulierten Accounts zu löschen. "Für Angreifer ist das eine interessante Möglichkeit, E-Mails zu stehlen", ist Pichlmayr überzeugt.

Der Trick wurde GeekCondition zufolge von Angreifern genutzt, um eine Reihe von Domains zu stehlen, die beim US-Registrar GoDaddy registriert waren. Als Beispiel eines Opfers wird das Technikblog MakeUseOf angeführt. Mithilfe eines Filters, der E-Mails vom GoDaddy-Support umleitet, ist es möglich, sämtliche erforderlichen Daten zu stehlen, um einen GoDaddy-Account zu übernehmen und dann registrierte Domains zu einem anderen Registrar zu verschieben. Schon früher haben Domain-Diebe Pichlmayr zufolge mit verschiedenen anderen Tricks E-Mails ausspioniert, um an Daten für ihre Machenschaften zu kommen.

### Abhilfe für Firefox-User erhältlich

An Google richtet GeekCondition die Empfehlung, die Gültigkeit der Authorisierungs-Variable auf eine Anfrage statt eine Sitzung zu begrenzen, um so den Angriff zu unterbinden. Nutzer wiederum sollten die Nachrichtenfilter in ihrem Gmail-Account prüfen. Firefox-User können sich mithilfe der Erweiterung NoScript vor gefährlichen Skripten auf präparierten Webseiten schützen. Auch gebührende Vorsicht der Nutzer ist gefordert. "Grundsätzlich sollten keine kritischen Inhalte über Freemail-Dienste verschickt werden", warnt Pichlmayr. (pte/red)