

Pharming

„Pharming“ beschreibt eine Betrugsmasche im Internet, die mit dem Phishing verwandt ist. Sowohl beim Phishing als auch beim Pharming geht es den Tätern darum, Passwörter und andere vertrauliche Nutzerdaten abzugreifen.

Vorgehensweise

Während beim Phishing ein „Köder“ in Form eines Links in einer gefälschten E-Mail ausgelegt wird, werden die Opfer beim Pharming nicht per E-Mail kontaktiert. Pharming wird deshalb auch als „Phishing ohne Köder“ (engl. phishing without a lure) bezeichnet. Die Voraussetzung für einen erfolgreichen Pharming-Angriff ist stattdessen, dass zuvor unbemerkt ein Schadprogramm (z. B. Trojaner) auf den Rechner des Nutzers geladen wurde. Gibt dieser anschließend eine Internetadresse – etwa die seiner Hausbank oder eines Onlineshops – in seinen Browser ein, landet er auf einer anderen Webseite, als er denkt. Davon merkt er jedoch nichts, da diese betrügerische Webseite optisch der eigentlichen Zielseite nachempfunden ist. Dabei wird auf dem Betriebssystem das DNS-Protokoll, das den Hostnamen der Webseite in eine IP-Adresse umwandelt, manipuliert: Die Schadsoftware ändert nach Eingabe der URL-Adresse im Browser die dazu hinterlegte numerische IP-Adresse in eine andere IP-Adresse um.

Die Folgen

Sobald ein Nutzer persönliche Informationen, wie zum Beispiel seine Kontonummer oder ein Passwort, auf der betrügerischen Webseite eingibt, sind die Täter ebenfalls im Besitz dieser vertraulichen Informationen und können die gestohlenen Daten für ihre Zwecke missbrauchen (Identitätsdiebstahl). So könnten sie beispielweise unbemerkt Kreditkartenabbuchungen durchführen oder auch „im Namen des Opfers“ bei Internetauktionen mitbieten.

DNS Spoofing

Eine besonders gefährliche Variante von Pharming stellt das sogenannte DNS Spoofing dar. Dabei wird über das Schadprogramm ein korrupter DNS-Server angesteuert. Die Täter müssen demnach keine individuellen Host-Dateien auf den Geräten der Opfer kompromittieren. Stattdessen übernimmt der DNS-Server das Vorgehen und kann auf diese Weise viele Nutzer gleichzeitig auf gefälschte und betrügerische Seiten umleiten. Die Folgen sind in diesem Fall besonders dramatisch, da der Identitätsdiebstahl Millionen Nutzer auf einmal betreffen kann.

Schutzmaßnahmen

- Firewall, Antivirenprogramm und Browser immer auf dem neusten Stand halten, d. h. regelmäßig Aktualisierungen durchführen.
- Bevor man Passwörter und vertrauliche Zugangsdaten auf einer Webseite eingibt, prüfen, ob es sich um eine sichere Internetverbindung handelt („https://“ und Schloss-Symbol in der URL).
- Auf gültige Sicherheitszertifikate achten, welche die Echtheit der besuchten Internetseite verifizieren können.

Zurück

© Verlag Deutsche Polizeiliteratur