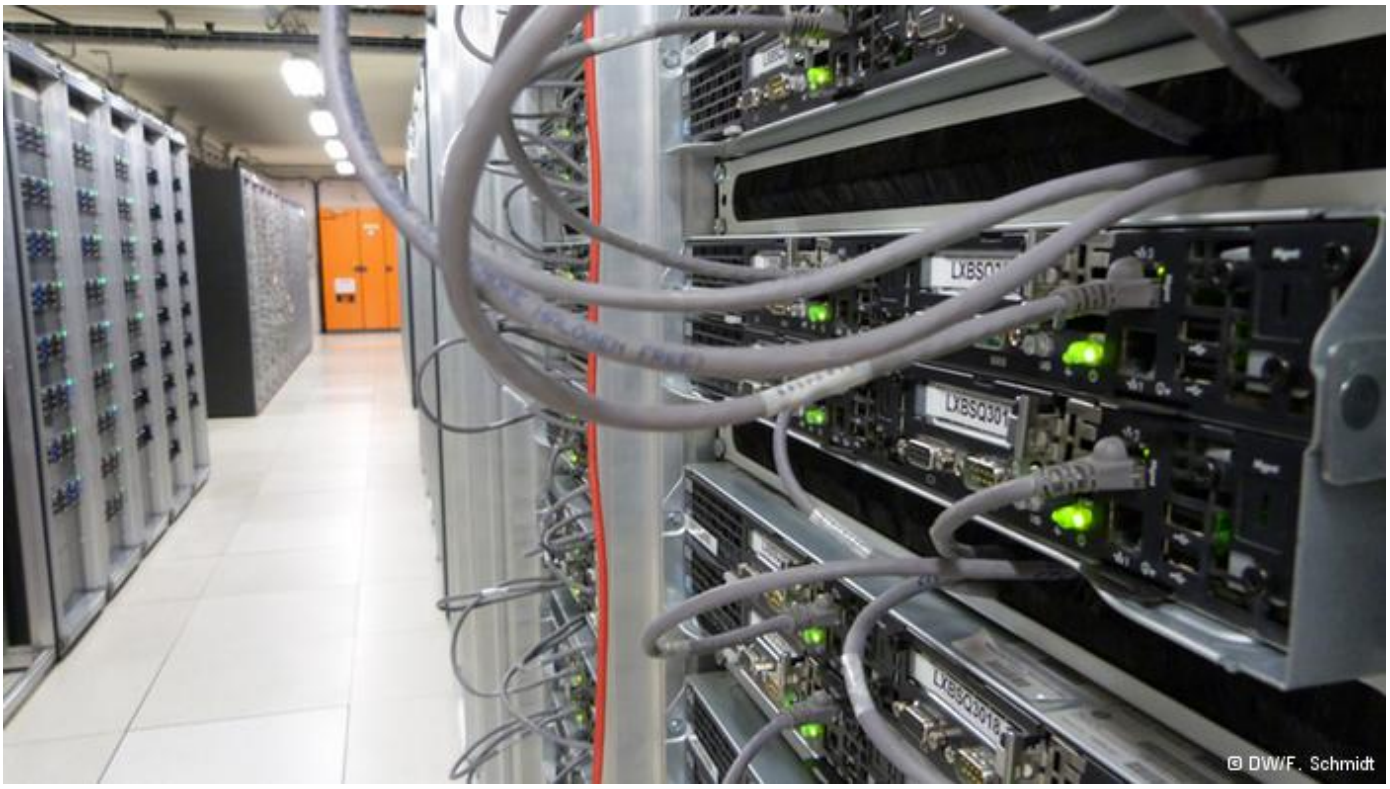
INTERNET

User machen es Hackern leicht

Sicherheitsexperten zeigen auf der IT-Defense Konferenz in Köln wie Hacker mit E-Mails in fremde Computersysteme eindringen können. Dabei ließen sich die meisten erfolgreichen Angriffe mit etwas Vorsicht vermeiden.



Hacker können Hintertüren in Server einbauen, ohne dass es jemand merkt

Wo gibt es Sicherheitslücken in E-Mail-Systemen, die es Angreifern leicht machen, die eigenen Server zu übernehmen - und was kann man dagegen tun? Diese und ähnliche Fragen diskutierten IT-Experten vom 10. bis 14. Februar 2014 in Köln.

Eigentlich ist das Bewusstsein für die Gefahr von Hackerangriffen bei den meisten Menschen schon da: Sie sind misstrauisch, wenn Sie Spam-E-Mails mit irgendwelchen Anhängen bekommen - darin könnten sich ja Viren oder Trojaner verstecken. Aber die wirklich gefährlichen Angriffe erfolgen heutzutage auf anderem Wege, sagt der IT-Sicherheitsberater Ben Williams. Für die Firma NCC-Group führt er sogenannte Penetrationstests an der Software namhafter Hersteller durch - er spielt also die Rolle eines Hackers und versucht einzudringen. Das gelingt ihm übrigens fast immer. Zum Beispiel bei E-Mail-Servern.

Was E-Mails alles preisgeben

"Als Hacker muss ich genau wissen, welches Produkt auf dem Server installiert ist und welche Webadresse das Produkt hat", erläutert der Sicherheitsfachmann. "An diese Informationen kann ich

kommen, wenn ich E-Mails an Nutzer schicke, die es gar nicht gibt. Wenn die E-Mail nämlich bei der Firma ankommt, geht sie zunächst durch alle Filtersysteme hindurch. Vorausgesetzt, sie wird nicht als Gefahr erkannt."

Und auf diesem Wege dringt die falsche E-Mail bis zum internen Mailserver vor. Der Mailserver schickt sie dann an den Absender zurück, weil ja der Empfänger falsch und damit nicht zu ermitteln ist. "Wenn die E-Mail zurückkommt - also 'gebounced' wird - schaue ich mir in den Daten dieser Mail an." Der Trick: Die Nachricht wurde innerhalb des Netzwerkes von Server zu Server weitergeleitet. Und jede Station hat eigene Informationen in der Kopfzeile - dem Header - hinterlassen. "So finde ich heraus, welche Adressen die jeweiligen Firewalls, E-Mail-Filter und so weiter haben, was für Produkte es sind und welche Version installiert ist. All das hilft mir bei der Planung meines Angriffs", sagt Williams.

Hacks sind oft dann erfolgreich, wenn es gelingt, einen internen Administrator zu überlisten

Für betroffene Firmen gibt es allerdings eine Lösung: Die E-Mail mit dem falschen Empfänger darf erst gar nicht die äußere Grenze des Unternehmensnetzwerks passieren. Das geht aber nur, wenn schon dort ein Filter installiert ist, der erkennt, welche Empfänger es auch wirklich gibt, und der keine E-Mails an unbekannte Adressen durchlässt.

Schadprogramme in Webseiten versteckt

Meist ist das allerdings nicht der Fall und Williams kommt an seine Informationen. So kann er seinen Angriff fortsetzen: Als nächstes macht er einen Phishing-Angriff. Er macht sich zunutze, dass die E-Mail-Administratoren heutzutage ihre Mailserver in der Regel von ihrem Arbeitsplatz aus über eine Webseite steuern. Deshalb muss er die Administratoren geschickt täuschen: "Ich muss einen internen Nutzer dazu bringen, auf einen Link in einer E-Mail zu klicken. Den habe ich vorher speziell

für ihn entworfen. Er soll also eine Webseite besuchen, die ich so aufgebaut habe, dass sie hilft, das Produkt anzugreifen."

Hinter der falschen Webseite verbirgt sich ein kleines unsichtbares Programm - ein Skript. Ist der Administrator zufällig gerade auf dem Mailserver eingeloggt, wenn es abläuft, greift das Programm auf den Server zu und baut dort eine Hintertür für den Hacker ein. Aber wie bringt Williams einen von Natur aus skeptischen Systemadministrator dazu, auf den Link zu klicken?

DW.DE

Datenklau schreckt E-Mail-Nutzer auf

Einen solchen Ansturm hat die Webseite des BSI wohl noch nicht erlebt. Als bekannt wurde, dass Online-Kriminelle Millionen E-Mail-Konten geknackt haben, ging der Server des Amtes vor der Menge der Anfragen in die Knie.

Gefahren aus dem Cyberspace

Glasfaserkabel anzapfen - geht das?

"Ich könnte mich zum Beispiel bei ihm beschweren, dass sein System mir zuviel Spam weiterleitet", erklärt der Hacker vom Dienst seine Taktik, "oder ich kann behaupten, dass ich versuche an seine Marketing-Abeilung E-Mails zu schicken, die nicht ankommen. Dann schreibe ich ihm: 'Hier sind weitere Informationen'. Und wenn der Administrator dann auf den Link klickt übernehme ich die Kontrolle seines E-Mailfilters."

Wenn Passwörter irgendwo im Netz herumliegen

Noch einfacher hatten es die LulzSec-Hacker, eine Gruppe, die der Anarchisten-Bewegung Anonymous nahesteht. LulzSec war es 2011 gelungen, in die Rechner zahlreicher Finanz- und Regierungsinstitutionen einzudringen, darunter Rechner des US-Senats und des Auslandsgeheimdienstes CIA.

"In fast jedem Fall, den ich gesehen habe, ging es um die Mehrfachnutzung von Passwörtern. Menschen nutzen denselben Nutzernamen und Passwort an mehreren Webseiten", sagt Michael McAndrews, heute ein privater IT-Sicherheitsberater. McAndrews hatte damals als Spezialagent der Ermittlungsbehörde FBI die LulzSec-Hacker gejagt. Verblüfft hat ihn vor allem, wie leicht es die Nutzer der verschiedenen Computersysteme den Hackern oft gemacht hatten.

Verwendet zum Beispiel ein Polizist dasselbe Passwort für den schlecht geschützten Zugang zum Verabredungs-Forum seines Sportvereins wie für den Zugang zu sensiblen Ermittlungsdaten, macht er es den Hackern leicht. "Leider ist es ein globales Problem, dass die Menschen etwas faul sind", sagt McAndrews. "Es ist leichter, sich ein Passwort einzuprägen als zwölf. Wenn ich für alle Webseiten nur ein Passwort nutze, ist es zwar für mich leichter, aber genauso für die Kriminellen."

Wer liest die E-Mail heimlich mit?

So war es auch für die LulzSec-Hacker. Kaum hatten sie sich eines E-Mail-Servers bemächtigt, nutzten sie eine weitere Schwachstelle. "Die Angreifer haben dem E-Mail-Account den Befehl gegeben: 'Leite alles an diese Adresse weiter'. Sie mussten also gar nicht mehr im System drin bleiben." Die Hacker erhielten jetzt automatisch Kopien aller E-Mails, die an den Betroffenen geschickt wurden. Und so kamen sie auch leicht wieder an neue Passwörter heran. Auf vielen

Australische Polizisten nehmen ein Mitglied der LulzSec-Gruppe fest

Webseiten kann man nämlich unter Angabe der E-Mail-Addresse bestehende Passwörter ändern. "Viele Firmen verlangen deshalb, dass man zusätzlich bestimmte Fragen beantwortet", erklärt der IT-Sicherheitsexperte McAndrews. "Aber leider sind viele dieser Antworten auch für die Hacker leicht zu recherchieren: Wo sind sie aufgewachsen? Mädchenname der Mutter? Name des Haustieres? All das kann gefunden werden, wenn der Nutzer diese Informationen im Internet veröffentlicht."

Auch das ein Grund, weshalb solche Informationen nicht auf Facebook oder ins eigene Familien-Blog gehören. Also ist Vorsicht im Internet oberstes Gebot, meint auch Ben Williams. Illusionen macht er sich aber nicht, denn Menschen seien eben auch nur Menschen, so der Dienst-Hacker: "Bei den Phishing-Angriffen, die ich ausgeführt habe, ist es mir immer wieder gelungen auch Mitglieder des IT-Teams dazu zu bringen, Codes auszuführen - oder sogar Passwörter preiszugeben. Man ist immer wieder überrascht: Nur weil jemand in der IT-Abteilung tätig ist, heißt das nicht, dass er nicht übers Ohr gehauen werden kann."