DIE FÜNF SCHLIMMSTEN HACKERANGRIFFE

1 Yahoo

2014 wurde die Suchmaschine angegriffen. Rund eine Milliarde Daten (Mailadressen, Telefonnummern, Passwort-Hashes) wurden gestohlen. Zwei Jahre später gelang es den Behörden, das Ausmaß der Attacke aufzudecken. Die Hacker haben aller Wahrscheinlichkeit nach jahrelang auf Yahoo zugegriffen. Es dürften alle Accounts betroffen gewesen sein. Bei dem Hack sollen unter anderem russische Spione verwickelt gewesen sein.

2 Ebay

Im Mai 2014 wurde der Server der Handelsplattform gehackt, 145 Millionen Datensätze wurden abgegriffen. Telefonnummern, Adressen und Geburtsdaten, wohl aber keine Kreditkarten- und Kontoinformationen. Möglich gemacht wurde der Hack durch einige zuvor auf kriminellem Weg erlangte Passwörter, die den Angreifern den Zugriff auf die verschlüsselte Kundendatenbank gewährten.

3 LinkedIn

Im Jahr 2016 wurden mehr als 117 Millionen gehashte Passwörter des sozialen Netzwerks über einen Filehoster zum Verkauf angeboten. Die Daten, die in ihrer Gesamtheit eine 4,5 Gigabyte große Textdatei füllten, sollen im Rahmen eines Hacks bereits im Jahr 2012 geklaut worden sein, bei dem zusätzlich 167 Millionen Nutzerdaten an die Hacker gingen.

4 Heartland Payment Systems

Der Cyberangriff auf einen der weltweit erfolgreichsten Anbieter elektronischer Zahlungsabwicklung schlug 2008 als einer der größten Hackerangriffe der damaligen Zeit hohe Wellen. Die verantwortliche Hackergruppe erbeutete 130 Millionen Kreditkartendaten und verursachte einen Schaden in Höhe von 110 Millionen US-Dollar. Drei Jahre später wurde der mutmaßliche Drahtzieher zu einer Haftstrafe von 20 Jahren verurteilt.

5 JPMorgan

Die US-Großbank wurde 2014 angegriffen. Als Zugang diente das Passwort eines Mitarbeiters des Finanzinstituts, das offenbar zuvor gestohlen wurde. Insgesamt wurden 83 Millionen Datensätze, darunter sieben Millionen Daten, die auf Geschäftskonten zurückgehen, erbeutet. Der Hack hätte mutmaßlich verhindert werden können, wenn JPMorgan jeden Zugang zum Netzwerk mit einer Zwei-Faktor-Authentifizierung geschützt hätte.

DIE FÜNF HÄUFIGSTEN ANGRIFFSMETHODEN

1 Denial-of-Service- (DoS) und Distributed-Denial-of-Service-Angriffe (DDoS)

Bei DoS-Angriffen werden Systeme mit Anfragen geflutet, die nicht mehr bewältigt werden können. Wird ein Angriff von vielen Hostrechnern, auf denen der Angreifer Schadsoftware installiert hat, parallel ausgeführt, ist das ein DDoS-Angriff. Im Gegensatz zu Angriffen, mit denen sich Hacker Zugriff auf ein System verschaffen, sind DoS- und DDoS-Angriffe nicht mit direkten Vorteilen für die Angreifer verbunden.

2 Man-in-the-Middle-Angriffe (MitM)

Bei einem MitM-Angriff schaltet sich ein Hacker in die Kommunikation zwischen einem Client und einem Server. Das kann in Form eines Session-Hijackings passieren, bei dem der Angreifer eine Verbindung zwischen einem vertrauenswürdigen Client und einem Netzwerkserver kapert. Der angreifende Rechner ersetzt dabei die IP-Adresse des vertrauenswürdigen Clients durch seine eigene IP-Adresse.

3 Phishing- und Spear-Phishing-Angriffe

Bei einem Phishing-Angriff werden meist E-Mails aus scheinbar vertrauenswürdigen Quellen mit dem Ziel versendet, persönliche Infos abzugreifen. Die Empfänger werden oft auf eine Website weitergeleitet, auf der sie persönliche Informationen preisgeben. Beim Spear-Phishing befassen sich Angreifer gründlich mit ihren Opfern und senden ihnen Nachrichten, die an sie persönlich gerichtet sind und deren Inhalt für die Opfer relevant ist.

4 Drive-by-Downloads

Drive-by-Downloads sind eine gängige Methode für die Verbreitung von Schadsoftware. Bei diesen Angriffen suchen Hacker nach ungesicherten Websites und schleusen ein schädliches Skript in den HTTP- oder PHP-Code der Seiten ein. Über dieses Skript kann Schadsoftware direkt auf dem Rechner eines Seitenbesuchers installiert werden, oder das Opfer wird auf eine Seite umgeleitet, die vom Hacker kontrolliert wird.

5 Kennwortangriffe

Da zur Kennung von Benutzern eines Systems oft Passworte verwendet werden, ist das Abgreifen dieser Codes eine gängige Angriffsmethode. Zugriff auf Kennwörter erhalten Angreifer, indem sie sich auf dem Schreibtisch des Opfers umsehen, die Netzwerkverbindung „abhören“, um unverschlüsselte Kennwörter abzugreifen, Social-Engineering-Techniken nutzen, sich Zugriff auf eine Kennwortdatenbank verschaffen oder raten.

Quellen: IT-Wegweiser, Netwrix | DERSTANDARD