IT-SECURITY

Sicherheit für das Domain Name System

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

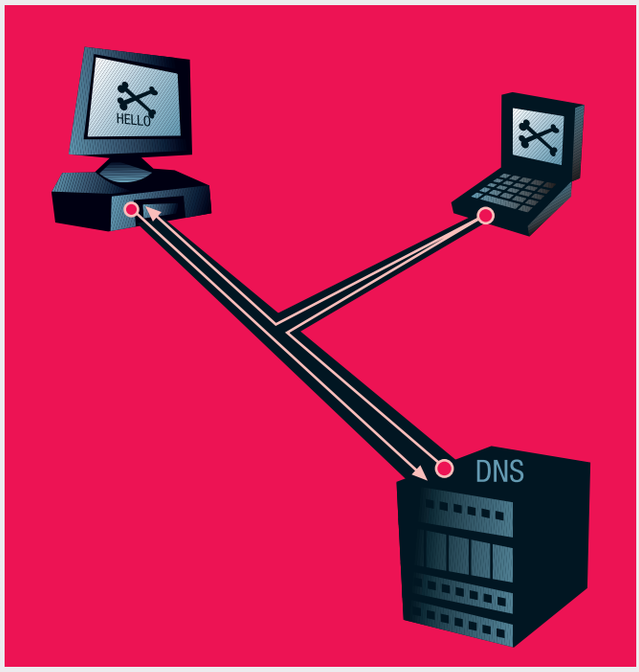

ILLUSTRATION: CW/THÜ

Frage: Wie sieht es mit der Sicherheit des Domain Name Systems (DNS) aus?

Das Domain Name System (DNS) ist einer der bedeutendsten Dienste im Internet, denn es ist verantwortlich für die Namensauflösung, also die Zuordnung der IP-Adresse zu einem Domänennamen. Bei jedem «Surfklick» im Internet wird im Hintergrund DNS verwendet. Auch jedes Mail benötigt DNS, um die IP-Adresse des Empfänger-Mail-Servers zu ermitteln. Die Anzahl der Dienste, die DNS beanspruchen, steigt stetig. Die Einführung von Enum ist nur ein Beispiel der steigenden Bedeutung des DNS-Dienstes. Umso erstaunlicher ist es daher, dass man sich oft nicht viele Gedanken über die DNS-Sicherheit macht. Dabei gibt es sehr viele DNS-Bedrohungen. Einige werden im nachfolgenden Abschnitt kurz skizziert.

Der Verlust der Datenintegrität/-authentizität kann auf verschiedene Arten erfolgen: Die DNS-Anfragen und -Antworten werden im Allgemeinen als unsignierte, unverschlüsselte UDP-Pakete verschickt. Falls ein Angreifer ans gleiche Netz wie der DNS-Client angeschlossen ist, kann er DNS-Anfragen abhören und falsche Antworten generieren. Der Angreifer wartet auf eine DNS-Anfrage des Clients. Auf diese Anfrage erstellt er nun eine Antwortmeldung mit derselben Message ID, aber einem selbst gewählten Inhalt («Resource Records» in der Answer Section). Die gefälschte Antwort wird an den Client gesendet, bevor die richtigen Auflösungsdaten zum Client gelangen können. Jede Netzwerkinfrastruktur, die das Abhören und Einschleusen von lokalem Datenverkehr zulässt, ist dieser Gefährdung ausgesetzt.

Eine Variante dieses Angriffs besteht darin, dass der Angreifer selbst eine Anfrage an den DNS-Server schickt, bei welcher er annimmt, dass der Server sie nicht direkt beantworten kann. Der Rechner leitet diese Anfrage weiter, was dem Angreifer die Möglichkeit gibt, diesen Request selbst zu beantworten. Der Server wird diese falschen Daten speichern. Der Cache des Servers ist korrumpiert. Auf diese Art kann der Angreifer einem Benutzer falsche DNS-Daten unterschieben.

Zu weiteren Bedrohungen der Datenintegrität gehören unter anderem Cache Poisoning, und Pharming: Bei Cache Poisoning schleust ein Angreifer gefälschte Daten in den Cache (temporärer Speicher) ein. Pharming dagegen steht als Oberbegriff für verschiedene Arten von DNS-Angriffen. Das Ziel der Angreifer ist es, die Benutzer heimlich auf gefälschte Webseiten umzuleiten und stellt somit eine Weiterentwicklung des Phishings dar.

Auch bei DNS gibt es eine Reihe von DOS-Angriffen (Denial of Service), welche die Verfügbarkeit des Dienstes beeinträchtigen oder sogar lahm legen.

Zu den DOS-Angriffen gehören beispielsweise die Übernahme respektive Lahmlegung eines Namenservers (durch Flooding, Malware usw.) oder das böswillige Eintragen einer Firma auf eine «Black List». Auch die Distributed-DOS-Angriffe im Jahre 2002, welche 7 von 13 Rootservern bis an den Rand ihrer Kapazität auslasteten, werden in Erinnerung bleiben.

Als Abwehrmassnahme muss eine Netzwerktechnologie aufgebaut werden, die kein Abhören erlaubt. Zusätzliche Sicherheit bietet die Aufteilung des DNS-Dienstes (Split DNS) oder der Einsatz von DNSSEC (DNS Security Extensions). DNSSEC erweitert das DNS-Protokoll, um die Identität des DNS-Servers sicherzustellen und die Verfälschung der Nachrichten während der Übertragung zu verhindern. Das Hinzufügen neuer Resource-Records-Typen sorgt für erhöhte Sicherheit (vergl. RFC 4033, 4034, 4035).

Der Sicherheit des Domain Name Systems muss in Zukunft erhöhte Beachtung geschenkt werden. ■

Der Sicherheit des Domain Name Systems muss in Zukunft erhöhte Beachtung geschenkt werden

Der Autor
Ivan Roman ist Consultant und Trainer bei Roman-Consulting & Engineering in Zürich. www.roman.ch

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch

COM_48_024 24 29.11.2006 16:02:15