Zwei Faktoren – Wissen und Besitz – ergänzt um sichere Identitäten

Das D-TRUST-Konzept sieht vor, diese Zwei-Faktoren-Authentifizierung um die Identität des Nutzers zu ergänzen. Dabei wird zusätzlich zu Passwort (Wissen) und Token (Besitz) die digitale Identität mithilfe eines Zertifikats eindeutig sichergestellt. Als akkreditiertes Trustcenter ist D-TRUST berechtigt, elektronische Zertifikate auszustellen, die auf Basis der Personalausweisdaten erstellt werden. Mit der digitalen Identität auf dem Token kann der Nutzer z. B. eine Online-Überweisung bewilligen oder eine digitale Unterschrift leisten.

Nationaler IT-Gipfel 2014 in Hamburg

Der Termin für den nächsten Nationalen IT-Gipfel in Hamburg wird aufgrund nachträglich eingetretener Änderungen der Terminplanungen der Bundesregierung auf den 21. Oktober 2014 vorverlegt.

Zur Vorbereitung des nächsten IT-Gipfels in Hamburg plant das Bundesministerium für Wirtschaft und Energie ein hochrangiges Treffen der zuständigen Mitglieder des neuen Bundeskabinetts mit den führenden Wirtschaftsvertretern des IT-Gipfels im März 2014.

Das Bundesministerium für Wirtschaft und Energie wird auf der Website *www.it-gipfel.de* über die bisherigen Ergebnisse des Jahres 2013 und über den Fortgang der Arbeiten des IT-Gipfels informieren.

Radware Lagebericht: DoS-/DDoS-Attacken unter den aktuell größten Gefahren für die IT-Sicherheit

„Distributed Denial of Service"-Attacken (DDoS) gehören zu den wichtigsten Gefahren für die IT-Sicherheit in diesem Jahr.

Zu diesem Schluss kommt der am 29.01.2014 veröffentlichte Lagebericht zur IT-Sicherheit (Global Application and Network Security Report 2013) von Radware, einem Lösungsanbieter für Anwendungssicherheit und Application Delivery in virtuellen und Cloud-Rechenzentren. DDoS-Angreifer führen demnach ihre Attacken immer gezielter durch, während die ihnen zur Verfügung stehenden Werkzeuge immer ausgeklügelter werden.

Die Ergebnisse des Jahresberichts beruhen auf den Daten und Erfahrungen von Radwares „Emergency Response Team" (ERT), das Angriffe auf Anwendungen und Netzwerke in Echtzeit verfolgt und abwehrt. Die ERT-Sicherheitsexperten beobachteten 2013 eine erhebliche Zunahme von DDoS-Attacken, die sowohl zu kompletten Systemausfällen als auch zu erheblichen Beeinträchtigungen im Betrieb führten – mit der Folge von Umsatzeinbrüchen, sinkender Kundenzufriedenheit und Imageverlusten. Der Radware-Bericht deckt zudem auf, dass die Angreifer selbst neu installierte Abwehrwerkzeuge immer schneller ausschalten können.

Zu den wichtigsten Ergebnissen des Berichts zählen:

Nicht nur Totalausfälle schädigen das Geschäft nachhaltig 60 Prozent der untersuchten Unternehmen verzeichneten im vergangenen Jahr Störungen und Leistungseinbußen in ihrem IT-Betrieb als Folge von Angriffen. Solche Einbußen gelten zwar als nicht so schwerwiegend wie ein Totalstillstand. Doch zeigen gleichzeitig Studien, dass 57 Prozent der Online-Kunden nach mehr als drei Sekunden Ladezeit eine Webseite verlassen und 80 Prozent von ihnen nicht mehr zurückkehren. Für Dienstleistungsunternehmen können also schon Teilausfälle zu sofortigen Umsatzeinbußen führen.

Angreifer schlagen (schnell) zurück

Angreifer sind zunehmend in der Lage, auch frisch aktualisierte Sicherheitssysteme in Unternehmen außer Gefecht zu setzen, indem sie neue Angriffsstrategien verwenden. Zum Beispiel mithilfe des sogenannten „http Floodings" oder Werkzeugen wie „Kill'em All" sind sie teilweise schon nach wenigen Stunden in der Lage, gerade neu installierte Abwehrsysteme zu überwinden.

DoS-/DDoS-Attacken gewinnen an Zerstörungskraft

Mit zerstörerischen Angriffen vor allem in den Jahren 2011 und 2012 haben die Intensität und der Anteil der besonders risikoträchtigen Attacken in den vergangenen Jahren zugenommen. Radwares DoS-/ DDoS-Risikobarometer zufolge stieg die Härte der DDoS-Angriffe im vergangenen Jahr um 20 Prozent.

Immer mehr Branchen im Visier

Neben Regierungsbehörden sind Finanzdienstleister zu den häufigsten Zielen von Cyberangriffen geworden. DDoS-Aktionen hatten nicht nur zerstörerische Motive, wie zum Beispiel bei der Angriffsserie „Operation Ababil" auf US-Finanzinstitute oder bei Attacken auf mehrere Bitcoin-Börsen. Viele sollten zugleich andere Systemeinbrüche verschleiern, die betrügerischen Zwecken dienten. Auch bei Webhosting- und Internet-Dienstleistern stieg 2013 die Zahl der Angriffe.

Neue Angriffsarten

Nach DoS-/DDoS- sind DNS-Attacken die derzeit zweithäufigste Angriffsform. Sie sind für Angreifer interessant, weil sich mit ihnen trotz eingeschränkter Ressourcen massiver Datenverkehr erzeugen lässt und da ihre Mehrebenen-Architektur eine Nachverfolgung der Angreifer fast unmöglich macht. Neben diesen DNS-Attacken tauchten jüngst weitere, für Unternehmen gefährliche Angriffsarten auf. Verschlüsselte anwendungsbasierte Angriffe machten rund 50 Prozent alle Web-Attacken aus, wobei in 15 Prozent aller Fälle Login-Seiten von Internetanwendungen täglich unter Beschuss genommen wurden.

Der komplette Bericht steht als Download zur Verfügung: *www.radware.com/ert-report-2013*

Secusmart erleichtert das Sicherheitsmanagement in Behörden

Über die Hälfte der deutschen Sicherheitsexperten bemängeln das nur wenig ausgereifte Sicherheitsmanagement in Deutschland. Daneben gehen 40% der befragten Experten davon aus, dass über 50 Millionen Deutsche in jeder Branche und in jeder möglichen Funktion bereits belauscht oder Daten abgegriffen wurden. Das unangenehme Ergebnis wurde am 29.01.2014 durch den Report „Secure Mobile Computing" öffentlich. Verantwortlich für die Gemeinschafsstudie ist neben der Secusmart GmbH der Bundesverband IT Sicherheit e.V. (TeleTrusT). „Der Bund hat diese Gefahr bereits verinnerlicht und setzt den hochsicheren und komfortablen Abhörschutz ein. Und das ist gut so: Die politischen Folgen wären kaum messbar, sollten Regierungsgeheimnisse am Telefon abgegriffen werden", so Dr. Hans-Christoph Quelle, Geschäftsführer der Secusmart GmbH.