

IT-SECURITY

Protokoll Tunneling: Wolf im Schafspelz

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

Frage: Wie funktioniert Protokoll Tunneling, und wie kann man IT-Infrastrukturen davor schützen?

Das sogenannte «Protokoll Tunneling» bezeichnet eine Technik, mittels welcher Protokolle via ein anderes Protokoll transportiert (getunnelt) werden. Virtual Private Networks (VPNs) nutzen das Protokoll Tunneling zur verschlüsselten Datenübertragung. Dabei handelt es sich um eine vom Unternehmen gewünschte Form von Tunneling.

Leider geht es auch anders: Mittels Protokoll Tunneling ist es möglich, auf unerwünschte Internet-Dienste (z.B. Instant Messaging) zuzugreifen oder mit Malware infizierte PCs remote zu administrieren. Obwohl über jedes Protokoll getunnelt werden kann, führt diese Technik nur zum Erfolg, wenn zum Tunneling Protokolle dienen, die auch für die Policy-konforme Internet-Nutzung benötigt werden. In den meisten Fällen sind dies HTTP, HTTPS und DNS. In der Folge wird auf die gängigen Techniken für diese Protokolle eingegangen:

HTTP-Tunneling: Das HTTP-Tunneling kann über eine Direktverbindung, über einen Proxy Server oder auf Applikationslevel mit API-Funktionen über

den Standard-Browser ablaufen. Webserver im LAN/WAN, in der DMZ oder im Internet können ebenfalls als Proxy missbraucht werden, wenn diese die CONNECT-Methode unterstützen. Die vom Client zu übertragenden Daten können zum Beispiel in der URI oder in Cookies co-

«Auch wenn ein direkter DNS-Zugriff am Perimeter unterbunden ist, können hausinterne DNS-Server genutzt werden.»

diert werden. Die Steuerbefehle des Servers sind am einfachsten im BODY zu platzieren.

Schutzmassnahmen: Filterung von HTTP CONNECT, Protokoll-Analyse auf gültigen HTTP-Verkehr, Anzahl und Timing von Requests auswerten, Überwachung der Verbindungsdauer (normale HTTP-Verbindung meist wenige Minuten, Tunnelverbindungen meist mehrere Stunden), Überwachung auf wiederkehrende Verbindungen in gleichmässigen Intervallen, Überwachung auf Datenmenge (Paketanzahl und -grösse pro Zeiteinheit, Server empfängt z.B. mehr Pakete als Client).

HTTPS-Tunneling: Hierbei ist das Tunneling nicht am Paketinhalt zu erkennen, da die Verbindung

End-to-End verschlüsselt ist. Die CONNECT-Anfrage wird bei jeder indirekten SSL-Sitzung (via Proxy) verwendet, unabhängig davon, ob es sich um normalen oder getunnelten HTTPS-Verkehr handelt.

Schutzmassnahmen: Ein SSL-Proxy baut statt einer verschlüsselten SSL-Verbindung zwischen Client und Zielserver je eine SSL-Verbindung von sich zum Zielserver und eine von sich zum Client auf. Somit ist der

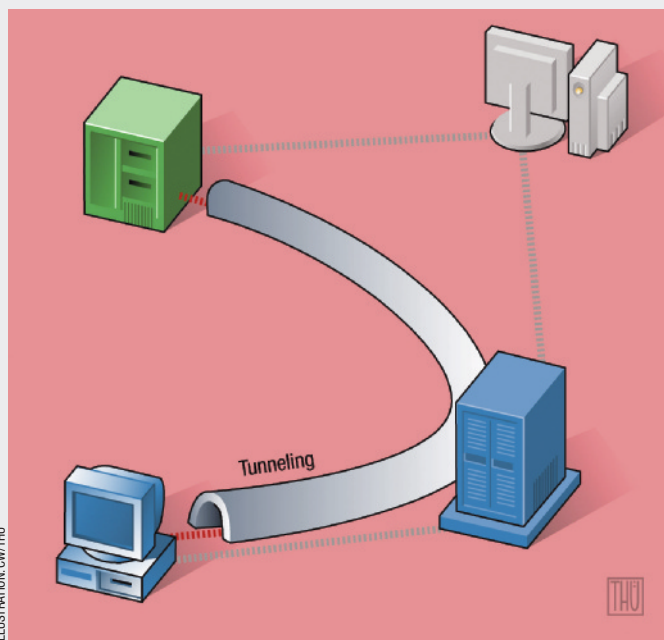
Datenverkehr auf dem SSL-Proxy unverschlüsselt und analysierbar, was jedoch rechtliche Konsequenzen bezüglich Datenschutz hat. Zusätzlich lassen sich Verbindungsdauer, Kommunikationspunkte und Datenmengen überwachen.

DNS-Tunneling: Dies ist die perfideste Tunneling-Variante, weil das DNS für die Zuweisung zwischen Systemnamen und IP-Adressen zwingend benötigt wird. Die Tunneling-Technik basiert darauf, dass die Nutzdaten auf dem Hinweg vom Client als Namensabfragen getarnt und auf dem Rückweg von der Steuerkomponente zum Beispiel in den TXT-Resource-Record-Feldern versteckt werden. Auch wenn ein direkter DNS-Zugriff

am Perimeter unterbunden ist, können hausinterne DNS-Server – welche die Anfragen weiterleiten – genutzt werden. Die Steuerkomponente setzt den TTL (Time-to-live)-Wert auf Null, um sicherzustellen, dass die Antworten (bzw. die Befehle) nirgends zwischengespeichert werden.

Schutzmassnahmen: TXT Records überwachen/filtern, Anzahl Abfragen überwachen/limitieren, Überwachung auf wiederkehrende Verbindungen, Datenmenge, Anzahl und Grösse der Pakete pro Zeiteinheit, Application-Level-Firewalls für Clients.

Fazit: Nicht-Policy-konformes Protokoll Tunneling kann für den Sicherheitsverantwortlichen zum Albtraum werden, doch mit geeigneten Mitteln wird auch der bestgetarnte Wolf im Schafspelz entlarft. ■



Der Autor
Christoph Baumgartner ist CEO der Sicherheitsberaterin One-Consult, Thalwil, www.oneconsult.com

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

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