

IT-SECURITY

VPN – So funktioniert ohne Risiko

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

Frage: Wir möchten unseren Mitarbeitern den Remote-Zugriff auf das Firmen-LAN ermöglichen. Wie funktioniert VPN und was gilt es zu beachten?

Das VPN (Virtual Private Network) bietet aus Anwendersicht eine anwenderfreundliche (weil transparente) Möglichkeit, remote auf Firmendaten zuzugreifen. Die Sicherheitsverantwortlichen schätzen bei der VPN-Technologie die Sicherheitsmechanismen um Datendiebstahl, Datenmissbrauch und Datenfälschung während der Kommunikation zu vermeiden. Ein VPN ist ein Tunnel zwischen zwei Endpunkten (Netzwerken), welches ein virtuelles Netzwerk erzeugt. Für die Verschlüsselung der Datenpakete werden kryptografische Verfahren (IPsec, L2TP, PPTP) genutzt. Dieser Artikel beschränkt sich ausschliesslich auf das IPsec-Protokoll.

IPsec ist kein allein stehendes Protokoll, sondern integriert mehrere in einem. IPsec deckt die Sicherheitsziele Vertraulichkeit, Authentizität und Integrität ab und bietet dazu noch Schutz vor Replay-Angriffen. IPsec beinhaltet drei Komponenten, den Au-

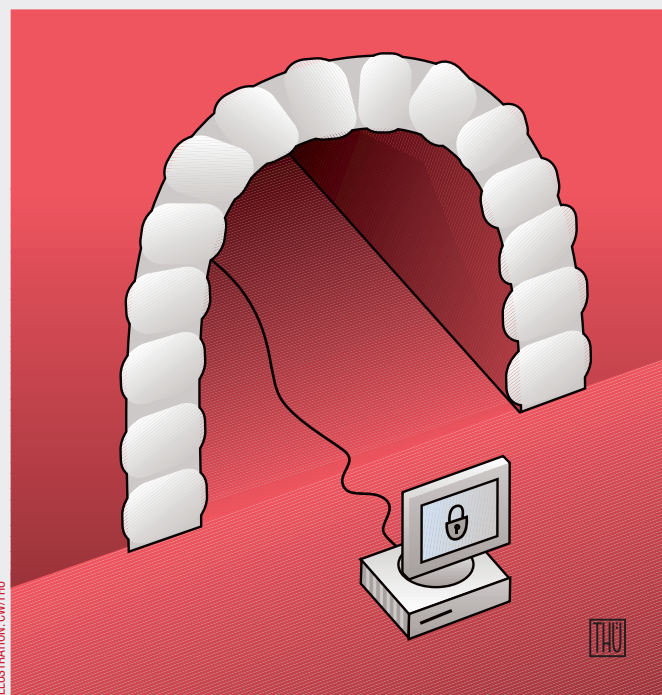
thentication Header (AH), den Encapsulating Security Payload (ESP) und den Internet Key Exchange (IKE).

Der Authentication Header (AH) stellt die Authentizität der übertragenen Pakete und die Authentifikation des Senders sicher. Zudem beinhaltet der AH einen Schutzmechanismus gegen Replay-Angriffe. Die Authentizität wird mittels eines über das gesamte Datenpaket erzeugten Hashwertes (SHA1 oder MD5) sichergestellt.

Der Encapsulating Security Payload (ESP) stellt die Authentifizierung, Integrität und Vertraulichkeit von IP-Paketen sicher. Die Nutzdaten werden beim ESP verschlüsselt (DES oder Triple-DES) übertragen, der IP-Header wird jedoch nicht verschlüsselt.

Das Internet-Key-Exchange-Protokoll (IKE) setzt sich aus drei Protokollen zusammen (ISAKMP, Oakley und SKEME) und dient zur Aushandlung der zu verwendenden Verschlüsselungsprotokolle und zum Austausch von Signaturen oder Schlüsseln.

IKE verwendet zwei Phasen: Als erstes authentifizieren sich beide Endpunkte gegenseitig um eine Vertrauensstellung zwischen einander einzurichten.



Diese Phase kann zwei Methoden nutzen, den «Main Mode» und den «Aggressive Mode».

In einer zweiten Phase werden die Einzelheiten der Sicherheitszuordnung ausgehandelt. Dazu gehört etwa die Art der Signierung oder Verschlüsselung der Datenpakete. Die Signierung dient der Authentizität der Pakete und die Verschlüsselung der Vertraulichkeit der Nutzdaten.

Beim Main Mode werden sechs Datenpakete zwischen den Peers ausgetauscht, die Identitäten sind aber von der ersten Kontaktaufnahme an geschützt, da übertragene IDs oder Zertifikate verschlüsselt werden.

Beim Aggressive Mode werden nur drei Datenpakete zwischen den Peers ausgetauscht. Die Identitäten sind im Gegensatz zum Main Mode aber nicht geschützt, weil keine Verschlüsselung erfolgt. Somit ist der Aggressive Mode unsicherer, da man beispielsweise den Pre-Shared-Key-Hashwert sniffen und diesen danach offline knacken kann.

Dieser Angriff kann mit dem Tool IKE_Scan durchgeführt werden. Weitere Informationen zum IKE-Scan finden sich im Security Blog «Hackertools» der

Computerworld unter: <http://www.computerworld.ch/index.cfm?pid=242>

Anschliessend kann versucht werden, selbst einen unberechtigten Tunnel mit dem Zielsystem aufzubauen, um durch diesen Tunnel direkt die Authentisierungsmechanismen des Ziel-LANs anzugreifen.

Die VPN-Technologie ermöglicht – falls richtig implementiert – die bequeme und sichere Verlängerung des Firmen-LAN an jeden x-beliebigen Ort. Es sollte aber verhindert werden, dass das VPN-Gateway den Aggressive Mode unterstützt. Andernfalls ist es nur eine Frage der Zeit bis sich Unberechtigte an diesem Tor zum LAN zu schaffen machen. ■



Der Autor
Oliver Gruskovjak ist Consultant und OPST bei Oneconsult, Bern.
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