Gefahrenpotenzial VPN

VPN (Virtual Private Network) Konzeptionen werden eingesetzt, um Datenübertragungen über das öffentliche Netz (Internet) abzusichern. Aufgrund der Vielzahl von möglichen Angriffen (siehe weiter unten) sowie in regelmäßigen Abständen auftretenden Sicherheitslücken in VPN Applikationen und der Konfigurationskomplexität von IPSec, sind VPN`s fehleranfälliger als gemeinhin bekannt.

Es gibt keinen Grund anzunehmen, dass VPN-Produkte weniger Sicherheitslücken enthalten als andere Programme. Oft sind es ganz triviale Methoden bzw. Ereignisse, die Sicherheitslücken verursachen und Angriffspunkte in VPN-Produkten ermöglichen.

VPN Sicherheitsanforderung

- ✓ Datenvertraulichkeit
- ✓ Datenintegrität
- ✓ Datenauthentizität

Hier unterscheidet man drei Bereiche von Bedrohungen

- ✓ Abhören von Daten
- ✓ Manipulieren von Daten
- ✓ Verhindern von Diensten

Angriffsformen auf VPN

- ✓ *Man-in-the-Middle Angriff:* Der Angreifer steht dabei entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.
- ✓ *Wiretrapping:* Netzverkehr abhören, um Informationen zu erhalten.
- ✓ *Spoofing:* vortäuschen einer falschen Identität, z.B. verändern der IP-Adresse.
- ✓ *ICMP/ARP Angriff:* gefälschte Statusmeldungen versenden, um Pakete umzuleiten.
- ✓ *Denial of Service:* Überlastung eines Dienstes durch SYN-Flooding.
- ✓ *TCP Sequenznummer:* Manipulation der Sequenznummern bei bestehenden Verbindungen.
- ✓ *Replay:* Pakete aufzeichnen, um sie später wieder einspielen zu können.

- ✓ *Schwächen in Applikationen:* Buffer Overflows/ Stack Exploits.
- ✓ *Web-Spoofing Methode:* URL-Rewriting + Java-Script (Umgeht auch SSL/TLS).
- ✓ *Offline Cracking Attack:* Passwort und Usernamen entwenden.
- ✓ *Client Attack:* Computer auf dem sich der VPN-Client befindet, wird übernommen.
- ✓ *Smurf Attack:* ist das Ausnutzen eines Mangels im TCP/IP , um einen Internet-Teilnehmer mit Paketen zu überfluten.
- ✓ *Der Bleichenbacher Angriff:* ist darauf ausgerichtet, den geheimen Schlüssel eines Servers mittels einer Schwachstelle in der PKCS#1 zu finden.
- ✓ *Key-Exchange-Alogorithm-Rollback-Angriff:* Dieser Angriff beruht darauf, dass der Angreifer dem Client als Server vorspiegelt, RSA zu benutzen, während dem Server vorgemacht wird, der Client wolle Diffie-Hellman benutzen.

Die hier geschilderten Angriffsformen lassen sich größtenteils vermeiden, indem man auf Preshared Keys komplett verzichtet und stattdessen Smartcards, HardwareTokens und X.509-Zertifikate einsetzt. Die Konfiguration mittels IPSec ist dementsprechend umfangreich. Wer gezwungen ist, zur Authentifizierung weiterhin PSKs einzusetzen, weil das Netzwerk-Budget nichts anderes hergibt oder der organisatorische Aufwand einer Umstellung zu groß wäre, sollte Alternativen wie z. B. die Navayo SecBox in Erwägung ziehen.

VPN Schwächen

Die IP-Erweiterung IPSec gilt gemeinhin als die sicherste VPN-Technik. Doch auch sie hat ihre Schwachstellen, die sich mit speziellen Tools, wie z. B. IKE-Scan, IKEProbe und Cain & Abel etc. finden und ausnutzen lassen.

Die Komplexität von IPSec kann durchaus selbst zum Sicherheitsrisikio werden. Zur fehlerfreien Konfiguration von IPSec-basierten VPNs ist Know-how und Erfahrung notwendig. In Kombination mit flaschen Default-Einstellungen vieler Geräte beziehungsweise Programme führt das oft zu vermeidbaren Schwachstellen, die gefährliche Angriffpunkte für Hacker schaffen.

73 Prozent der in Großbritanniens Unternehmen vorhandenen virtuellen privaten Netzwerke (VPN) bergen mindestens eine kritische Sicherheitslücke, die Angreifern den unauthorisierten Zugriff auf Daten ermöglicht. Bei der Komplexität eines VPN-Netzwerkes nicht ungewöhnlich.

- ✓ **Sicherheitsrisiko Zertifikate**
  Zertifikate werden auf einem Benutzerkonto gespeichert und können auch kopiert werden. Dies hat zur Folge, dass man auf das Zertifikat genauso sorgsam aufpassen muss, wie auf alle anderen Anmeldedaten auch. Wenn das Zertifikat fest im Rechner integriert ist und dieser entwendet wird (Notebooks auf Messen sind ein beliebtes Ziel), dann ist es genauso unsicher, wie ein einfacher Name

und ein leeres Kennwort. Eine Verringerung dieser Gefahr lässt sich über Smartcards erreichen. Natürlich muss man jetzt auf diese Smartcard wiederum genauso aufpassen wie auf alle anderen Daten. Der Kreis ist endlos.

- ✓ **Informationsbeschaffung durch VPN Sicherheitslücken**
  Wenn neue Sicherheitslücken in VPN Produkten bekannt werden und nicht Zeitnah reagiert wird, haben Angreifer die Möglichkeit den Verkehr unverschlüsselt mitzuschneiden oder ins Netzwerk einzudringen.

- ✓ **Private Schlüssel**
  Der vollständige Private Schlüssel wird normalerweise von einer einzigen Person eingegeben. Damit ist aber der Schlüssel allgemein bekannt und somit ein potenzielles Sicherheitsrisiko. Die Speicherung und der (freie) Zugang zum Schlüssel wird zum häufig vergessenen Sicherheits-Aspekt. Stichwort White-Box Pentest.

- ✓ **Daten Rekonstruktion**
  Modernisiert ein Unternehmen seine IT-Infrastruktur z. B. neue PC`s, Server und Notebooks, kann es bei unsachgemäßer Entsorgung (löschen der Festplatte) vorkommen, dass die Daten auf der Festplatte von Dritten wieder rekonstruiert werden können.

VPN Konfigurationsschwierigkeiten

- ✓ Software Clients sind schwierig zu installieren. Schlüssel müssen generiert werden, etc.
- ✓ Software Clients können den Zugriff auf den privaten Schlüssel nicht blockieren, und stellen somit ein Sicherheitsrisiko dar.
- ✓ Software Clients sind system- und versionsabhängig, und damit auch abhängig von der Systemsicherheit.
- ✓ VPN Appliances besitzen typischerweise keinen Hardware Schlüsselschutz.
- ✓ VPN Appliances unterstützen normalerweise kein Remote Management über verschlüsselte Kanäle.
- ✓ VPN Produkte erfordern spezielle Firewall Einstellungen sowohl für ankommende als auch für abgehende Verbindungen.

Sicherheitsprobleme von VPN Produkten

- ✓ Der Primär-Schlüssel ist in der Host Software oder in der Appliance gespeichert. Damit ist der Schlüssel leicht angreifbar und zu hacken.
- ✓ Der Host oder die Appliance basieren typischerweise auf PC Hardware und Standard PC Software, und sind damit ebenfalls leicht zu hacken.

- ✓ IPsec ist schwierig zu installieren und für die vorhandene Firewall passierbar zu machen. Daraus resultiert häufig ein fehlerhaftes Setup.
- ✓ VPN verlangt ankommende und ausgehende Firewall Regeln. Damit steigt die Komplexität und wird anfällig für Sicherheitslücken.

Fazit

VPN Konzeptionen werden heutzutage in fast allen sicherheitsrelevanten Bereichen eingesetzt. Was eigentlich als kostengünstige Alternative zur Standleitungen gedacht war, wird aufgrund der Komplexität von IPSec plus Administrationsaufwand und damit verbundenen Sicherheitslücken aufgrund der schwierigen Implementierung von IPSec, nicht minder kostengünstig als eine Standleitung. Außerdem führt der Begriff „sichere Verbindung“ den Anwender in die Irre und weckt bei ihm die falsche Vorstellung von garantierter Sicherheit.

Alternativen zu VPN gibt es, siehe Navayo SecBox, jedoch werden diese neuen Technologien heute zu wenig genutzt obwohl Sie im Vergleich zu der Sicherheit, Kosten- und Konfigurationsintensität besser abschneiden als herkömmliche VPN Konzeptionen.

Bei der Auswahl von Schutzmechanismen für das eigene Netzwerk sollte man sich unbedingt davon überzeugen, dass die gewählte Sicherheitsstrategie vollwertigen Schutz vor allen Bedrohungen bietet.

Literatur

1. http://www.nta-monitor.com/ike-scan
2. http://www.ernw.de/download/ikeprobe.zip
3. http://www.oxid.it/cain.html
4. http://www.roesner-it.com/it-security.htm

Rösner-IT ♦ Lönsstr. 16 ♦ 48485 Neuenkirchen
Tel: +49 (0) 5973-90 06 52 ♦ Fax: +49 (0) 5973-90 07 98
E-Mail: info@roesner-it.com ♦ Web: www.roesner-it.com