ERNW
Enno Rey Netzwerke GmbH

ERNW Newsletter 2 / Juli 2003

Liebe Partner, liebe Kollegen,

willkommen zur zweiten Ausgabe des ERNW-Newsletters, die unter dem Motto
steht: **"Vertrauen ist gut, korrekte Konfiguration ist besser!"**

Die eklatante Verbreitung des Wurms "SQL-Slammer" auch in vermeintlich gut gesicherten Unternehmensnetzen (deren Firewalls den verwendeten Port 1434 sperren sollten) lässt sich vielfach nur durch Infizierung über VPN-Zugänge erklären. Das wirft die Frage auf, ob das VPNs bislang entgegengebrachte Vertrauen sinnvoll und angemessen ist. Ein Problem von VPN-Zugängen möchten wir in dieser Ausgabe erläutern.

Zur Sicherheit von IPsec-basierten VPNs

Die IPsec-Protokollfamilie bildet die Grundlage der meisten in Unternehmen oder Behörden implementierten VPNs. Sie besteht aus dem UDP-basierten "Aushandlungs-Protokoll" IKE (Internet Key Exchange) und den beiden IP-Protokollen ESP und AH zur Verschlüsselung der Nutzdaten (von denen allerdings das zweite kaum eingesetzt wird und möglicherweise in einer zukünftigen Spezifikation entfallen wird).
Ein Design-Ziel von IPsec war unter anderem die Unterstützung einer Vielzahl möglicher Einsatzszenarien bei gleichzeitiger Gewährleistung eines hohen Sicherheits-Grundlevels. Die dafür notwendige Flexibilität wird durch verschiedene Varianten und Erweiterungen des IKE erreicht (dies ist der Grund der für Sysadmins oft beschwerlichen Parameter-Vielfalt und Komplexität des IKE). Der Key Exchange wird in zwei Phasen abgewickelt, die wiederum in verschiedenen Modi stattfinden können.

Die erste Phase (P1) wird üblicherweise im "Main Mode" (mit sechs ausgetauschten Nachrichten) oder im "Aggressive Mode" durchgeführt (beschleunigter Austausch von nur drei Nachrichten mit weniger Sicherheitsfunktionen).

Die Phase 2 (P2) wird standardmässig im "Quick Mode" realisiert.
Eine Aufgabe der Phase 1 ist die Authentifizierung der beiden IPsec-Partner, wofür im allgemeinen sog. "Preshared Keys" (PSKs, dies sind im Grunde Kennwörter) oder Zertifikate eingesetzt werden. Darüber hinaus gibt es den (nicht per RFC spezifizierten) Hybrid Mode, der vor allem von Check Point implementiert ist und meist mit Token-Verfahren auf Client-Seite arbeitet, sowie die P1-Erweiterungen XAuth (zur User-Authentifizierung) und ModeConfig (zur Verteilung von IP-Parametern an Clients), die beide vielfach von Cisco-Komponenten verwendet werden.

Alle IPsec-basierten Implementierungen unterstützen aber in der Phase 1 den Main Mode (der meist bei Gateway/Gateway-Kopplungen von Netzen zum Tragen kommt) und den Aggressive Mode, der für den Zugriff mobiler User vorgesehen ist.

Ein bekanntes jedoch unterschätztes Problem des Aggressive Mode besteht nun darin, dass bereits im ersten vom Gateway an den Client gesendeten Paket der zur Authentifizierung eingesetzte Preshared Key als Hashwert versendet wird, und zwar _ohne_ eine zuvor erfolgte Authentifizierung des Clients. Das IPsec-Gateway händigt also seinen eigenen Preshared Key jedem "interessierten" Client (in gehashter Form) aus.

Speziell für Angriffe dagegen existiert seit einigen Monaten ein Tool namens IKECrack, dessen Wirksamkeit wir bei verschiedener Gelegenheit bereits prüfen konnten. Ein Angreifer initiiert hier (ohne Kenntnis irgendeines Preshared Keys) eine Verbindung zum VPN-Gateway, zeichnet die ausgetauschten Pakete auf und verwendet IKECrack zum Knacken des vom Gateway übermittelten Preshared Keys.

Der eigentliche Wörterbuch- oder Brute Force-Angriff gegen den PSK des Gateways findet anschliessend auf dem Rechner des Angreifers statt - ohne weitere Verbindungsversuche zum Gateway. Es genügt also ein einziges im Aggressive Mode versendetes Paket des Gateways!

Drei Voraussetzungen müssen für einen erfolgreichen Angriff erfüllt sein:

1.) Das Gateway nimmt Verbindungen von beliebigen IP-Adressen an. Das ist für mobile User eigentlich immer der Fall.
2.) Der initiierende Client kann das Gateway dazu bewegen, die Phase 1 im Aggressive Mode durchzuführen. Das ist bei einigen Devices per default möglich (etwa Cisco-Routern, selbst mit neuesten IOS-Versionen), bei anderen (etwa der Firewall-1) per default ausgeschaltet (aber möglicherweise von manchen Sysadmins im Rahmen verzweifelter Fehlersuche oder einfach aus Unkenntnis aktiviert).
Nicht betroffen sind Systeme, die im Hybrid Mode arbeiten. Systeme mit XAuth sind nur angreifbar, wenn der Angreifer eine Man-in-the-Middle Position zwischen Client und Gateway einnimmt [denkbar etwa beim Zugriff eines Aussendienst-Mitarbeites auf das eigene Unternehmensnetz, während er sich beim Kunden befindet].

3.) Der Hash-Wert wird mit dem Verfahren MD5 gebildet. Diese Beschränkung wird wohl mit der nächsten Version von IKECrack (oder mit einem anderen
Tool) verschwinden.

Alles Weitere hängt vom Umfang des beim Angreifer vorhandenen Wörterbuchs oder der ihm zur Verfügung stehenden Rechenzeit ab. Wir möchten hier nochmals betonen: offline, d.h. ohne weiteren Kontakt zum attackierten Gateway.

Das Problem ist nicht neu, hat aber bisher wenig Beachtung gefunden. Michael Thumann (mthumann@ernw.de) hat darüber ein Paper geschrieben (www.ernw.de/download/pskattack.pdf);
die Antwort von Cisco finden Sie hier:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a008016b57f.shtml

Angesichts der vielen VPNs, die eher unter Funktionalitäts-Gesichtspunkten ("Hauptsache, es läuft irgendwie") als mit umfangreicher Sorgfalt und Fachkunde konfiguriert sind, könnte hier in einigen Organisationen eine Sicherheitslücke bestehen, die Angreifern breiten Zugriff auf schützenswerte Ressourcen gewähren würde. Wir raten daher dringend, die oben genannten Rahmenbedingungen zu prüfen und sie ggf. durch korrekte Konfiguration, Upgrade einer beteiligten Komponente oder Re-Design der VPN-Strukturen zu beseitigen. Natürlich sind wir gerne dabei behilflich.

Wir möchten auch darüber hinaus unser Fachwissen an Sie weitergeben und haben daher eine Schulungsreihe zu speziellen Security-Themen konzipiert. Ab September werden wir bundesweit Seminare durchführen, die jeweils einen Teilbereich der IT Security fokussieren. Dabei haben wir uns ausdrücklich auf Themen beschränkt, die in dieser Form und mit der von uns realisierten fachlichen Tiefe sonst nicht angeboten werden. Die Themen der jeweils dreitägigen Schulungen sind:

Security Management
Know Your Enemy [Fortgeschrittene Angriffs-Techniken, Honeypots & Forensik] Secure Programming Advanced Network Security [Security auf Infrastrukturebene]

Selbstverständlich führen wir die Veranstaltungen auch für unsere Schulungspartner oder inhouse in Ihrem Unternehmen durch. Inhalte, Termine und Preise finden Sie unter www.ernw.de/training.
Wir freuen uns auf Ihren Besuch!

Es grüssen Sie herzlich

Enno Rey & das Team von ERNW

ERNW Enno Rey Netzwerke GmbH - Zaehringerstr. 46 - 69115 Heidelberg
Tel. +49 6221 480390 - Fax 6221 419008 - Mobil +49 173 6745902
www.ernw.de