VIPRINET UND SICHERHEIT

China und die USA unterstellen sich heute gegenseitig, zwecks Wirtschaftsspionage mit Hintertüren versehene Routertechnik auf den Markt zu bringen. Dank NSA-Affäre herrscht Gewissheit, dass vertrauliche Daten auch bei den Netzbetreibern nicht sicher sind. Das Vertrauen ist bei Unternehmen wie Bürgern zu Recht erschüttert, der Staat zeigt sich überfordert. Wem können Sie noch vertrauen?

Wir sind Viprinet, ein in Deutschland entwickelnder und produzierender Routerhersteller. Die abhörsichere Ende-zu-Ende-Verschlüsselung unserer VPN-Router ist komplett in Ihrer Hand, und nur Sie haben den Schlüssel. Unsere Produkte sind frei von Backdoors, und wir kooperieren nicht mit Geheimdiensten.

Um Ihre Unternehmensstandorte sicher zu vernetzen, nutzen unsere Router mehrere gebündelte günstige Consumer-Medien wie DSL, UMTS oder LTE. Die Daten werden dabei zerteilt und verschlüsselt übertragen. Durch diese Risikoverteilung auf mehrere Zugangsnetze wird Ihre Standortanbindung daher auch noch hochausfallsicher, bei geringen laufenden Kosten - und das selbst an entlegenen Standorten oder im mobilen Einsatz.

Im Folgenden beschreiben wir im Detail, weshalb Sie uns und unseren Produkten uneingeschränkt vertrauen können:

1. Keine Hintertüren in Viprinet-Produkten

Viprinet verweigert Geheimdiensten jeglicher Gerichtsbarkeit speziellen Zugang zu Viprinet-Produkten.

Sollten ein Geheimdienst oder eine geheime gerichtliche Anordnung versuchen, Viprinet dazu zu zwingen, in irgendeinem Viprinet-Produkt eine Hintertür einzubauen, versprechen wir, alle unsere Kunden im betreffenden Land zu informieren, sofern irgend möglich, unverzüglich jegliche Geschäftsanbahnung im betreffenden Land zu beenden, und uns aus dem betreffenden Land zum frühestmöglichen Zeitpunkt zurückzuziehen.

2. Volle Kontrolle über die Produktkette dank „Made in Germany“

Man muss heute davon ausgehen, dass sowohl in den USA als auch in China produzierte Hardware ab Werk bereits mit Hintertüren geliefert wird. Vorgeblich europäische Hersteller haben die Produktionskette für ihre Produkte nur noch selten komplett in ihrer Hand. Hintertüren können also in Produkten enthalten sein, ohne dass der entsprechende Hersteller selber davon weiß. Bei von US-Herstellern produzierten IT-Sicherheitsprodukten muss nach aktueller Informationslage fest davon ausgegangen werden, dass diese Backdoors der NSA enthalten. Bei Produkten chinesischer Hersteller muss eine Backdoor chinesischer Geheimdienste zumindest vermutet werden.

In Deutschland existierten glücklicherweise keine Geheimgerichte, die Hintertüren in Produkte anordnen könnten. Auch sind keine entsprechenden Bestrebungen von Geheimdiensten bekannt.

Unsere Produkte werden bezüglich ihrer Software vollständig in Deutschland entwickelt. Unsere Quelltexte sind auf fast schon paranoide Art vor Fremdzugriff gesichert. Die Hardware unserer Routerprodukte wird ebenfalls vollständig in Deutschland entwickelt und auch produziert.

3. Paranoide Sicherheitsarchitektur

Unsere Geräte sind vom Design her intern in eine „saubere" und eine „schmutzige" Seite aufgeteilt. Die „schmutzige" Seite ist dabei der Teil, der mit öffentlichen Netzen kommuniziert, also z.B. ADSL-, UMTS- oder LTE-Modems. Diese Komponenten stammen zum Teil auch von Drittherstellern, darunter Herstellern aus Taiwan, China, Korea und den USA. Diesen Teilen wird in unserem Design nicht vertraut, sie werden behandelt wie das unverschlüsselte Internet und nur dazu genutzt, um darüber eine verschlüsselte Verbindung aufzubauen. Der „saubere" Teil der Produkte steht komplett unter unserer Kontrolle. Der „schmutzige" Teil unserer Produkte ist vom „sauberen" sowohl auf Hardware- als auch auf Softwareebene voneinander getrennt.

4. Sichere Verschlüsselung, nicht von der NSA gebrochen

Alle VPN-Produkte von Viprinet verwenden zur Verschlüsselung bekannte Industriestandards, welche von Sicherheitsforschern als sicher und nicht von der NSA gebrochen betrachtet werden.

Dies sind im Einzelnen:

- TLS 1.1
- RSA, Schlüssellänge bis 8/2013 1024 Bit, seitdem 2048 Bit
- AES 256 Bit
- SHA-1

Aufgrund der Enthüllungen von Edward Snowden muss man heute davon ausgehen, dass die NSA möglicherweise versucht, weit verbreitete Verschlüsselungsbibliotheken wie OpenSSL oder auch Hardware-Verschlüsselungschips zu kompromittieren. Es wird vermutet, dass insbesondere das VPN-Protokoll IPSec in Geräten von US-Herstellern mit Hintertüren ausgestattet sein könnte.

Hierzu ist zu sagen: Viprinet verwendet keine ungeprüften Verschlüsselungsengines von Dritten. Unsere Router sind zwar mit Hardware-Verschlüsselungsengines ausgestattet. Diese stammen aber von unterschiedlichen Herstellern aus verschiedenen Regionen der Welt und werden nie exklusiv genutzt – wir verwenden sie immer nur in Kombination mit von uns selbst in der Software implementierten Verschlüsselungssystemen. Unsere Produkte sind daher über keine der bisher bekannt gewordenen Angriffsszenarien der NSA angreifbar, insbesondere nicht über geschwächte Zufallszahlengeneratoren.

Als zusätzlicher Vorteil der Viprinet-Bündelungstechnologie darf gelten, dass bei einem gebündelten VPN über die einzelnen Internetmedien jeweils nur ein Bruchteil der verschlüsselten Daten übertragen wird. Angriffsszenarien in den Netzen der Netzbetreiber, welche laut Presseberichten tatsächlich durchgeführt werden, schlagen bei unserer Technik daher fehl.

5. Tatsächliche Risikobereiche

Viprinet-Produkte verwenden zur Bündelung einen zentralisierten VPN Hub in einem Rechenzentrum. An dieser Stelle laufen also alle verschlüsselten Datenströme zusammen. Ein Angriff auf die Verschlüsselung unserer Produkte ist am ehesten im Netz des Rechenzentrums denkbar. Es sollte daher darauf geachtet werden, dass das Rechenzentrum sicherheitszertifiziert ist. Insbesondere müssen der VPN Hub und benachbarte Netzwerkgeräte (z.B. Switches) gegen physikalischen Zugriff gesichert werden.

Grundsätzlich sind bei der von Viprinet implementierten VPN-Technologie Man-in-the-Middle-Attacken denkbar, wenn über andere Einfallstore (z.B. Social Engineering, Einschleusung von Spionen, Infizierung von Administratoren-PCs) Passwortdaten der Viprinet-Router entwendet werden. Viprinet wird in kommenden Firmware-Releases für seine Produkte auf diese Risiken ein besonderes Augenmerk legen, und in diesem Bereich die Sicherheit und die Erkennbarkeit von Man-in-the-Middle-Attacken deutlich verbessern.