Verschlüsselte Daten bilden Sicherheits-Risiko

Für das Einschleusen von Malware ins Firmennetzwerk setzen Hacker vermehrt auf die verschlüsselte Datenübertragung. Dadurch bleiben Angriffe mehrheitlich unentdeckt. Höchste Zeit, SSL-basierte «blind spots» zu verhindern.

Um Cyber-Attacken zu erkennen und wirksam abzuwehren, muss der gesamte ein- und ausgehende Datenverkehr kontinuierlich auf Schadcode überprüft werden. In Anbetracht dessen sind Firmen in aller Regel bereit, beträchtliche Summen in die IT-Security, in den Schutz von Perimeter und Endpoints, von Systemen und Applikationen zu investieren. Laut aktuellen Studien belaufen sich die weltweiten Ausgaben für UTM-Appliances, Next Generation Firewalls, IPS (Intrusion Prevention System) und weitere für die IT-Security relevante Systeme auf über 70 Mia. USD. Dieser erklecklichen Summe zum Trotz: Viele Firmen bleiben hochgradig verletzbar. Dies vor dem Hintergrund, dass Cyber-Kriminelle vermehrt auf die Übertragung SSL-verschlüsselter Daten setzen. Doch diese werden bei rund 80 Prozent der Firmen nicht überprüft und passieren folglich sämtliche bestehenden Sicherheitsschranken ungehindert.

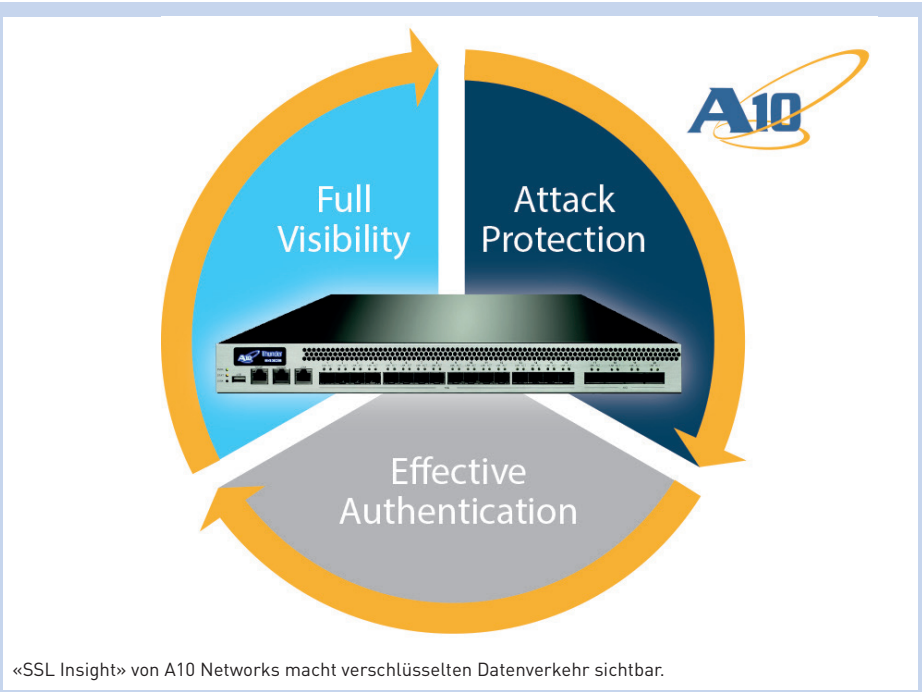
Transparenz schaffen

Um dieser Problematik zu begegnen, sind hoch performante Systeme notwendig, die in der Lage sind, verschlüsselte Daten «on the fly» zu dechiffrieren, verzögerungsfrei auf Schadcode zu überprüfen und schlechten Code zu blockieren. Demgegenüber müssen unproblematische Daten wieder verschlüsselt und an die Zieldestination weitergeleitet werden.

Zwar beinhalten einige am Markt erhältliche Security-Appliances solche mit «SSL Insight», «SSL Interception» oder «SSL forward proxy» bezeichnete Funktionen. Doch der beschriebene Prozess ist derart rechenintensiv, dass klassische Security-Appliances nicht in der Lage sind, die notwendige Performance zur Verfügung zu stellen. Laut einem Bericht von NSS Labs verlieren sie bis zu 87 Prozent ihrer Leistung.

Application Delivery Controller (ADC) mit «SSL Insight»

Um Firmen auch bei der verschlüsselten Datenkommunikation ein Maximum an Sicherheit zu ermöglichen, hat A10 Networks ihre hoch performanten Application Delivery Controller (ADC) der Thunder-Serie mit leistungsfähigen, dedizierten SSL-Security-Prozessoren bestückt. Diese garantieren selbst bei höchsten Datenraten und bei der Verwendung von 4096-Bit-Schlüsseln eine beinahe latenzfreie Entschlüsselung, Überprüfung und Verschlüsselung von SSL-Daten. Die Systeme lassen sich einerseits als eigenständige Gesamtlösung am Firmengateway installieren. Andererseits unterstützen sie ein nahtloses Zusammenspiel mit bestehenden Firewalls und UTM-Appliances. Bei dieser mit «SSL offloading» bezeichneten Integration entlastet die ADC die bestehenden Security-Devices von der leistungshungrigen Entschlüsselung und Verschlüsselung der Daten.



«SSL Insight» von A10 Networks macht verschlüsselten Datenverkehr sichtbar.

Leistungsmerkmale – ein Auszug

Die ADCs der Thunder-Serie von A10 Networks setzen im Bereich «SSL Insight» klare Bestmarken. Zu den herausragenden Features gehören:

- Verzögerungsfreie Entschlüsselung, Überprüfung und Verschlüsselung von SSL-Daten
- Nahtlose Einbindung von Drittprodukten zur Dateninspektion
- SSL offloading zur Entlastung der Firewall-Ressourcen für die Analyse des Netzwerkverkehrs
- Lastverteilung des Netzwerkverkehrs auf mehrere Security-Geräte
- Erstellung von Ausnahmen von «SSL Insight» durch einfache Konfiguration von Website-Kategorien mithilfe des Partners Webroot
- Interoperabilität mit vielen namhaften Security-Herstellern

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Telefon 056 437 60 60
info@boll.ch
www.boll.ch