Sicherheit auf dem Prüfstand:

Wie gut schützt Ihre Firewall?

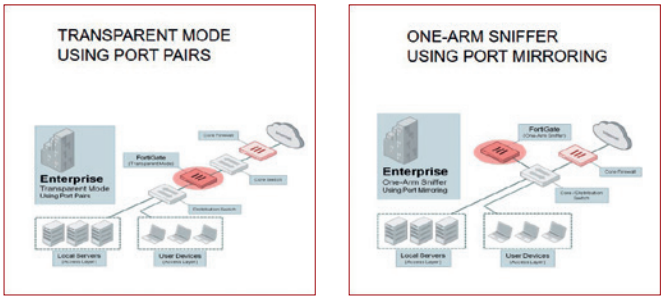
Auch für Firewalls gilt: Vertrauen ist gut, Kontrolle ist besser. Mit dem Cyber Threat Assessment Program (CTAP) von Fortinet haben Sie die Möglichkeit, Ihr Netzwerk im laufenden Betrieb zu analysieren und gleichzeitig zu prüfen, wie gut Ihre Firewall Bedrohungen und Unregelmäßigkeiten erkennt.

Eine Firewall fungiert als „Türsteher“, der ausgehenden und eingehenden Datenverkehr aus dem Internet prüft, unerlaubte Zugriffe verhindert und unerwünschte oder schädliche Inhalte blockiert. Regelmäßige Berichte über Hackerangriffe und Datenlecks sollten niemanden mehr an der Notwendigkeit einer Firewall für jedes Firmennetzwerk zweifeln lassen. Viele unserer kleinen und mittelständischen Kunden scheuen die Kosten und den Aufwand für eine Firewall. Sie vertrauen darauf, zu klein oder zu uninteressant für Hacker zu sein. Dabei spielen Größe oder Branche keine Rolle für das generelle Risiko, Opfer von Schadsoftware und Cyberattacken zu werden. Im Gegenzug aber kann die Folge eines solchen Angriffs für kleine Unternehmen schnell existenzbedrohend sein.

Auch wer das Unternehmen mit einer Firewall schützt, sollte seinem „Türsteher“ gründlich auf die Finger schauen: Erkennt die Firewall wirk-

lich zuverlässig ungebetene Gäste? Und ist sie leistungsfähig genug, um nicht zum Bremsklotz für den Geschäftsbetrieb zu werden?

Eine Firewall ist nur so sicher, wie sie aktuell ist. Hacker werden kreativer und wissen, dass die größte Sicherheitslücke der Endanwender ist – und der beschäftigt sich im Firmennetzwerk nicht unbedingt nur mit seiner Arbeit. Durchschnittlich 25 % des Netzwerkverkehrs entfallen auf das private Surfen in sozialen Medien oder gar aufs Streamen. Das spielt Hackern zusätzlich in die Hände. Es sind nicht mehr nur Phishing-Mails oder Anhänge mit Schadsoftware, die zur Gefahr werden, weil sie immer seriöser und glaubhafter aussehen. Auch Werbeanzeigen im Internet entpuppen sich häufiger als Virus und sind damit ein immer größer werdendes Risiko. Ein falscher Klick kann im schlimmsten Fall das komplette Unternehmen für Tage lahmlegen. Neben dem Sicherheitsrisiko hat der unerwünschte Datenverkehr der Nutzer auch wirtschaftlich Bedeutung, weil er das Netzwerk unnötig belastet und so ggf. die Produktivität senkt. Wer beurteilen will, ob die Bandbreite des Netzwerks ausreicht, muss daher wissen, wofür die Anwender das Netzwerk nutzen.



Das Cyber Threat Assessment kann auf zwei verschiedene Arten durchgeführt werden.

ARROW | Security

FORTINET

Enterprise Computing Solutions – Deutschland

Lassen Sie Ihr Netzwerk analysieren – schnell & unkompliziert

Im Rahmen des **Fortinet Cyber Threat Assessment Program (kurz: CTAP)** können Sie Ihr Netzwerk innerhalb von nur sieben Tagen auf Bedrohungen, Nutzerverhalten und Bandbreitennutzung analysieren lassen.

Was ist CTAP?
Die Analyse Ihres Netzwerks läuft beim CTAP über eine FortiGate, unsere Next Generation Firewall. Die FortiGate wird dabei als Teststellung ca. sieben Tage in Ihr Netzwerk integriert.

Am Ende der Teststellung steht ein Report, der folgende Bereiche Ihres Netzwerks beleuchtet:

Angriffe und Bedrohungen
Wie effektiv ist die momentan eingesetzte Security-Lösung?

Nutzerverhalten
Welche Websites und Webanwendungen werden genutzt?

Bandbreitennutzung
Wie gestaltet sich die Bandbreitennutzung & wie kann man diese optimieren?

Wie läuft CTAP ab?

1. **Kontaktieren Sie Ihren Fortinet-Vertriebspartner**
2. **Wählen Sie zusammen das passende FortiGate-Modell und die Einsatzart**
   Für CTAP geeignete FortiGate-Modelle sind 60E (Beta), 100D, 300D und 1500D. Die FortiGate kann auf zwei Arten in Ihr Netzwerk integriert werden:
   1) Transparenter Modus
   2) Sniffer-Modus über einen gespiegelten Switch-Port.

   Ihr Fortinet-Partner integriert das FortiGate-Testgerät in Ihr Netzwerk
   Ihr Partner stattet die FortiGate hierfür mit der passenden Firmware und Konfiguration aus. Die FortiGate loggt für die Dauer des CTAP in unseren zentralen FortiAnalyzer, allerdings in eine abgetrennte administrative Domain (ADOM) und SSL-verschlüsselt.
3. **Ihr Fortinet-Partner liefert Ihnen den CTAP Report**
   Nach ca. sieben Tagen beendet Ihr Fortinet-Partner das Logging der FortiGate. Anschließend bespricht er mit Ihnen den CTAP Report und zeigt Ihnen Handlungsempfehlungen auf.

Mit dem Cyber Threat Assessment Program von Fortinet können Unternehmen sieben Tage lang kostenfrei ihren Netzwerkverkehr analysieren und prüfen, ob ihre Firewall Angriffe zuverlässig erkennt.

Das Cyber Threat Assessment

prüft bestehende Sicherheitslösungen und -konfigurationen auf Herz und Nieren,
kann schnell und unkompliziert auf verschiedene Weisen installiert werden,
schränkt den bestehenden Geschäftsbetrieb nicht ein und
beeinflusst das Netzwerk nicht.

Der Ablauf ist simpel. Nachdem die Einsatzart mit uns definiert wurde, wählen wir ein FortiGate-Modell mit passender Firmware aus. Dieses wird bis zu sieben Tage als Teststellung in das System integriert. Die Integration ist über einen gespiegelten Switch-Port oder einen transparenten Modus in wenigen Minuten möglich. Dann läuft die Analyse unsichtbar im Hintergrund und durchleuchtet drei Bereiche:

Allgemeine Sicherheit

Das Programm deckt auf, welche Gefahren und Attacken die Firewall übersieht. Zusätzlich verweist die Analyse auf die gefährdeten Endgeräte.

Nutzerverhalten

Eine zusammenfassende Statistik analysiert das Nutzerverhalten. Außerdem zeigt der Report z. B. welche Social-Media-Kanäle, Instant-Messaging-Programme oder andere Webanwendungen die Mitarbeiter am häufigsten nutzen.

Bandbreitennutzung

Das Programm misst, wann die Durchsatz-, Sitzungs- und Bandbreitennutzung am höchsten ist. Zusätzlich gibt es Aufschluss darüber, zu welchen Zeiten das Netzwerk am ausgelastetsten ist.

Nach der Analyse erhalten Sie einen umfangreichen Analysereport, der Ihnen Infos über die oben genannten Punkte gibt. Im Report werden neben den Schwachstellen auch empfohlene Maßnahmen dokumentiert, die wir gerne mit Ihnen durchgehen. Wichtig hierbei: Die Analyse und der Report sind kostenfrei und verpflichten nicht zum Kauf oder Wechsel zu einer Fortinet-Lösung. Für Unternehmen die optimale Gelegenheit, bestehende Systeme zu überprüfen und bei Bedarf zu optimieren.

Was passiert mit den Daten im Anschluss an das Cyber Threat Assessment Program?

Wir löschen die lokalen Daten vollständig auf der ausgehändigten FortiGate. Sieben Tage nach dem erstellten Report löscht Fortinet automatisch die Log-Daten. Sicherheit setzt Wissen voraus: Mit CTAP schaffen Sie die Basis für eine wohlbegründete Entscheidung in Sachen Firewall. Gern beraten wir Sie ausführlich.

Ihr Ansprechpartner

Thomas Zens
Vertrieb

T +49 228 9080-534
thomas.zens@hug.de

FORTINET SILVER PARTNER

H&G

Warum Fortinet?

Das amerikanische Unternehmen macht seit 2000 mit vollintegrierbaren und leistungsstarken Sicherheitssystemen die gesamte IT-Infrastruktur sicher.

Über 300 veröffentlichte Patente und über 250 ausstehende Patente zu Sicherheitslösungen und -konzepten überzeugen weltweit über 360.000 Kunden. Insbesondere das Konzept der Fortinet Security Fabric hat uns überzeugt. H&G ist Fortinet Silver Partner.