THREATCLOUD EMULATION SERVICE
NEUE, ZIELGERICHTETE UND ZERO-DAY-ANGRIFFE ERKENNEN

THREATCLOUD

Die Vorteile

- Erkennung neuer Malware, die sich in Adobe PDF-, Microsoft Office-, Flash-, ausführbaren und archivierten Dateien sowie Java Applets versteckt
- Emulation von Dateien und Dokumenten für die Bedrohungserkennung in einer sicheren „Sandbox“
- Schutz vor Angriffen auf die verschiedenen Windows-Betriebssystemumgebungen
- Datei-Emulation innerhalb der SSL- und TLS-Kommunikation
- Schutz vor schadhaften Dateien bevor sie in das Unternehmen eindringen können

Die Funktionen

- Cloudbasierender Dienst: Integration in Ihre bestehende Infrastruktur erfordert kein zusätzliches Equipment
- Integration in Exchange: die Überwachung aller E-Mail-Anhänge wehrt E-Mail-Bedrohungen zuverlässig ab
- keine Beeinträchtigung des Geschäftsbetriebs: das Netzwerk ist abgesichert – ohne fälschliche Kategorisierungen von Inhalten (Zero-False-Positives)
- Steigerung des Sicherheitsniveaus: Informationen zu neuen Bedrohungen werden automatisch an die ThreatCloud weitergeleitet

DIE HERAUSFORDERUNG

Cyber-Bedrohungen werden immer raffinierter und komplexer und zielgerichtete Angriffe nutzen Software-Schwachstellen in Download-Dateien und E-Mail-Anhängen aus.

Diese Bedrohungen umfassen neue Exploits oder auch Varianten bekannter Exploits, die nahezu täglich auftreten und für die es keine Signaturen gibt. Es gibt keine Standard-Lösung für die Erkennung dieser Exploit-Varianten. Neue oder unerkannte Bedrohungen erfordern neue Lösungsansätze, die über die Signaturen bekannter Bedrohungen hinausgehen.

DIE LÖSUNG

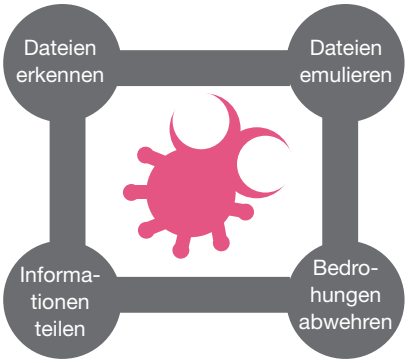
Check Point ThreatCloud Emulation verhindert die Infizierung durch unerkannte Exploits, zielgerichtete oder Zero-Day-Angriffe. Diese innovative Lösung überprüft sehr schnell alle Dateien und überführt diese in eine virtuelle „Sandbox“, um schadhaftes Verhalten erkennen zu können. So kann die erkannte Malware nicht in das Unternehmensnetzwerk eindringen. ThreatCloud Emulation gibt diese Informationen an den ThreatCloud™ Service weiter und teilt so diese neuen Informationen zu erkannten Bedrohungen mit anderen Check Point-Kunden.

Herkömmliche Lösungen legen den Fokus auf die Erkennung von Bedrohungen und die Benachrichtigung nachdem diese in das Netzwerk eingedrungen sind. Mit Check Point ThreatCloud Emulation können Unternehmen neue Bedrohungen abwehren bevor es zu einer Infizierung kommt.

DIE FUNKTIONSWEISE

So erkennen Sie verdächtige Dateien sofort

- Erkennung von Dateien in E-Mail-Anhängen oder Web-Downloads
- Verdächtige Dateien werden an den ThreatCloud Emulation Service gesendet
- Unterstützung durch den Agent für Exchange Server (ohne eine Check Point-Infrastruktur)
- Unterstützung für bestehende Security Gateways mit R77



Datei-Emulation

- Ausführung der Dateien in einer virtuellen Sandbox-Umgebung
- Untersuchung des Dateiverhaltens in verschiedenen Betriebssystemumgebungen und mit verschiedenen Office-Versionen
- Überwachung des File-Systems, der Registry, der Prozesse und der Netzwerkverbindungen
- Verdächtige Aktivitäten der Dateien werden gekennzeichnet und ein Algorithmus ermittelt, ob von diesen Dateien schadhafte Aktivitäten zu erwarten sind
- Erstellung eines detaillierten Berichts, der genaue Informationen zu der untersuchten Datei, zu anormalen Aktivitäten sowie Screenshots aus der Sandbox-Umgebung, in der die Datei ausgeführt wurde, umfasst

Schützen Sie Ihr Unternehmen vor schadhaften Dateien

- Eingehende schadhafte Dateien werden abgewehrt bevor sie in das Unternehmensnetzwerk eindringen können

Informationen zu schadhaftem Code in der ThreatCloud teilen

- Unmittelbare Aktualisierung der ThreatCloud, um neu entdeckte Malware in Dateien daran zu hindern, in andere Unternehmen einzudringen

DIE FUNKTIONEN VON CHECK POINT THREATCLOUD EMULATION

ThreatCloud Emulation Service

ThreatCloud Emulation Service ist eine kosteneffiziente und cloudbasierende Lösung, die die bestehende Infrastruktur eines Unternehmens nutzt. Dateien können für die Emulation von einem bestehenden Security-Gateway oder von dem Agent des Exchange Servers an die ThreatCloud gesendet werden. Der ThreatCloud Emulation Service ermöglicht ein zentrales Management und schafft Transparenz: Unternehmen erhalten sowohl Informationen zu Bedrohungen als auch zur Nutzung des Services.

Virtuelle Sandbox-Umgebung

Check Point Threat Emulation überwacht und filtert eingehende Dateien, führt diese in einer virtuellen Umgebung aus und kennzeichnet diejenigen, von denen verdächtiges oder schadhaftes Verhalten zu erwarten ist. Hierbei handelt es sich üblicherweise um Malware, die beispielsweise die Registry oder Netzwerkverbindungen verändert oder neue Dateien erzeugt. Sobald eine neue Bedrohung erkannt ist, wird die Dateisignatur an die Check Point ThreatCloud gesendet, um aus neu entdeckter Malware eine bekannte und dokumentierte Bedrohung zu machen, die sich abwehren lässt.

Unterstützung verschiedener Betriebssystemumgebungen für die Emulation

Check Point ThreatCloud Emulation nutzt verschiedene Umgebungen für die Datei-Simulation: Windows XP, Windows 7, Microsoft Office und Adobe.

Detaillierte Reports zur ThreatCloud Emulation

Es wird ein detaillierter Bericht über die Datei-Emulation erstellt. Dieser leicht verständliche Report umfasst ausführliche Informationen zu allen schadhaften Angriffsversuchen, die durch die untersuchten Dateien entstehen können. Der Bericht bietet darüber hinaus Screenshots der jeweiligen Betriebssystemumgebung, in der die Datei ausgeführt wurde.

Verschlüsselte Kommunikation

Dateien, die mit dem SSL- und TLS-Protokoll übermittelt werden, stellen einen Angriffsvektor dar, der viele Industriestandard-Implementierungen umgeht. Check Point ThreatCloud Emulation überprüft auch die SSL- und TLS-Tunnel und die darüber versendeten Dateien, um verdeckte Bedrohungen auch in diesen vermeintlich geschützten Datenströmen zu erkennen.

Schützen Sie Ihr Unternehmen vor schadhaften Dateien

Der ThreatCloud Emulation Service schickt Dateien mit detaillierten Informationen über deren Aktivitäten an das Security-Gateway oder den Exchange Agent zurück. Schadhafte Dateien können somit die Mitarbeiter nicht erreichen und schützen Unternehmen davor, infiziert zu werden.

Das ThreatCloud-Ökosystem

Neu entdeckte Bedrohungen werden an die ThreatCloud gesendet, sodass auch andere verbundene Gateways geschützt werden können. Jede neu entdeckte Bedrohungssignatur wird an die anderen Gateways gesendet, um Bedrohungen abzuwehren bevor diese die Möglichkeit haben, sich weiter zu verteilen. ThreatCloud ist dank dieses Zusammenspiels das innovativste und modernste Netzwerk für die Bedrohungsanalyse und -abwehr.

Einfache und flexible Bereitstellung in Ihrem Unternehmen

Die Dateien können an den ThreatCloud Emulation Service oder an die Private Cloud Emulation Appliance gesendet werden. Jedes Security-Gateway mit R77 oder höher und jeder Server mit einem Agent für Exchange kann die eingehenden Dateien überwachen und verdächtige Dateien für eine Emulation weiterleiten.

TECHNISCHE SPEZIFIKATIONEN

ThreatCloud Emulation Service

Der cloudbasierende Dienst ermöglicht es, die Volume-Anforderungen für die Datei-Emulation pro Gateway zu definieren und so die Bedürfnisse eines Unternehmens flexibel umzusetzen.

Private Cloud Emulation Appliances

Unternehmen können zwischen zwei Varianten wählen: Appliances für bis zu 3.000 User und Appliances für Unternehmen mit mehr als 3.000 Usern.

Technische Spezifikationen für die Emulation	
Unterstützte Dateiformate für die Überprüfung	Adobe PDF, Microsoft Office, EXE, archivierte Dateien , Flash und Java Applets
Unterstützte Emulationsumgebungen	Microsoft Windows XP, Microsoft Windows 7; Microsoft Office; Adobe Reader

Technische Spezifikationen für das Security Gateway Erkennung der Dateien und Weiterleitung an den ThreatCloud Emulation	
Unterstützte Plattformen	Check Point Appliances: 2000, 4000, 12000, 13000, und 21000, die R77 oder höher nutzen; andere Appliances und Open Server mit gleichwertiger Leistung im Vergleich zu den oben genannten Modellen
Betriebsumgebungen	SecurePlatform or GAiA

KONTAKTIEREN SIE UNS Check Point Software Technologies GmbH | Zeppelinstr. 1 | 85399 Hallbergmoos
Tel: +49-811 99821-0 | E-Mail: contact-germany@checkpoint.de