Barracuda CloudGen Firewall und macmon

Cloud-Generation-Sicherheit mit Advanced Endpoint Security und Erweiterter Zugangskontrolle (NAC)

Advanced Threat Protection & Sandboxing

Barracuda Advanced Threat Protection (BATP) ist ein in die Barracuda CloudGen Firewall integrierter cloud-basierender Service, der herkömmliche Sicherheitstechnologien wie URL-Filter, IPS und Anti-Virus erweitert. BATP besteht aus mehreren aufeinander aufbauenden Schutzschichten mit graduell zunehmendem Aufwand sowie Erhöhung der Erkennungsrate. Angefangen mit Milliarden von digitalen Signaturen, heuristischer Analyse des Code-Verhaltens, statischer Analyse des Codes bis hin zur Live-Detonation in einer Sandbox wird so der beste Schutz auch vor unbekannten Bedrohungen erreicht.

BATP ist einer der schnellsten Services seiner Art im Sicherheitsumfeld, trotzdem kann es in Einzelfällen zu Verzögerungen von wenigen Minuten kommen. Aus diesem Grund bietet die Barracuda CloudGen Firewall die Option “Deliver first, then scan”. Mit Aktivierung dieser Option werden die Inhalte nach URL-Filter, IPS und lokalem Anti-Virus direkt zum Endgerät freigegeben, obwohl die finale Einstufung von BATP noch nicht verfügbar ist. Für den Fall, dass der gerade von der Firewall weitergeleitete Inhalt nachträglich eine Einstufung als “bösartig” erhält, wird durch die macmon-Integration das Endgerät automatisch vom Netz getrennt, in ein Quarantänenetz gestellt und eine Warnung zur Weiterbearbeitung ausgegeben.

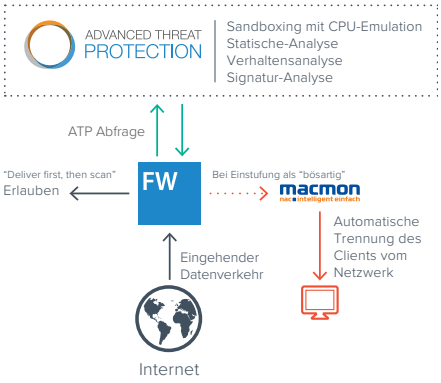

Abbildung 1 - Advanced Threat Protection mit macmon-Integration

Erkennung von Botnet & Spyware

Der Barracuda Advanced Threat Protection Cloud Service analysiert die Ergebnisse von über 50 Millionen Analysepunkten, übergreifend über alle Netzprotokolle und Angriffsvektoren.

Daraus resultiert eine der weltweit größten Datenbanken mit Sicherheitsinformationen über Milliarden von Domains, IP-Adressen und sehr umfangreichen Erkenntnissen, welche Domains oder IP-Adressen als Spyware- und Ransomware-Kontrollinstanzen (sogenannte Command-and-Control-Server) funktionieren.

Erkennt die Barracuda CloudGen Firewall verdächtigen Datenverkehr von Endpunkten aus dem Unternehmensnetz zu einem dieser bekannten Ransomware- oder Spyware-Server, kann der Endpunkt als kompromittiert angesehen werden.

Durch die Zusammenarbeit von Barracuda CloudGen Firewall und macmon NAC wird diese Information automatisch weitergeleitet, das Endgerät vom Netz getrennt, in ein Quarantänenetz gestellt und eine Warnung zur Weiterbearbeitung ausgegeben.

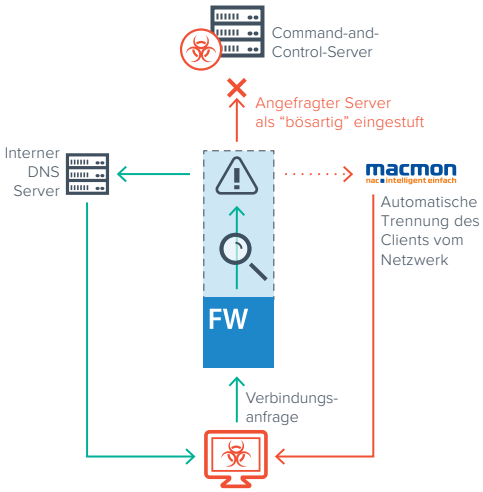

Abbildung 2 - Bot & Spyware Protection mit macmon-Integration

Automatisierte Gruppenkonfiguration

Die Informationen über die Endgeräte im Netzwerk werden aktiv von macmon NAC an die Barracuda CloudGen Firewall übertragen und damit automatisch die passenden Sicherheitsrichtlinien zugewiesen. Die Kommunikationsregeln zwischen zwei getrennten Netzwerksegmenten erfolgen dadurch nicht mehr nur segmentbasiert, sondern auf Basis von Gerätegruppen – die Mitglieder dieser Gruppen werden dabei durch macmon NAC anhand der aktiven Erkennung gepflegt, was stets aktuelle, gerätegenaue Kommunikationsregeln gewährleistet.

Dies erfolgt nicht nur für unternehmenseigene Geräte, sondern gilt auch für Gästeautorisierung und BYOD. So können z.B. nur von macmon NAC autorisierte Geräte über die Barracuda CloudGen Firewall auf das Internet oder dedizierte interne Ressourcen zugreifen. Für verschiedene Gruppen werden automatisch verschiedene Sicherheitsrichtlinien aktiviert. Für das Gästenetz können z.B. URL- Filter und Applikationseinschränkungen sehr viel stringenter erfolgen oder aber der Download von Software-Updates auf niedrige Bandbreite eingeschränkt werden. Damit wird verhindert, dass ungewollter Datenverkehr die Produktionsanwendungen negativ beeinflusst.

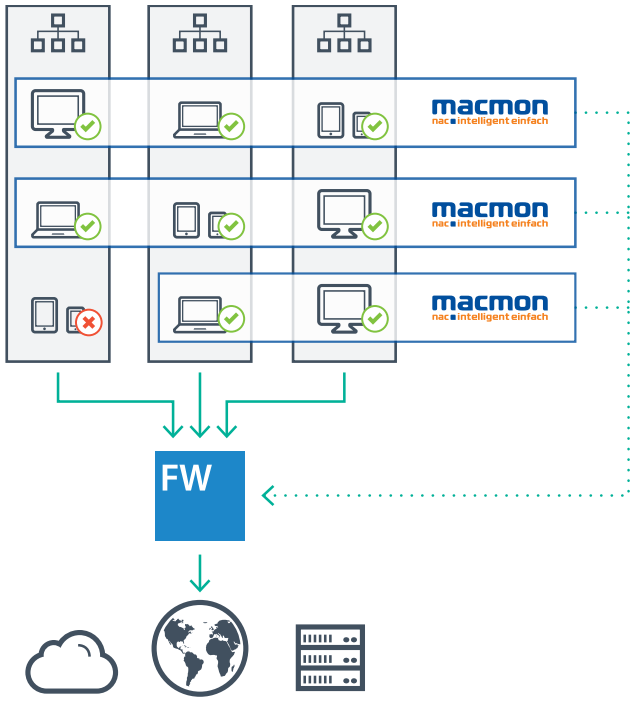

Abbildung 3 - Automatisierte Gruppenkonfiguration

Endgeräteerkennung und Transparenz

Mit Barracuda CloudGen Firewalls und macmon NAC behalten Sie selbst bei großen oder komplizierten Netzen den Überblick. Die Produkte tauschen aktiv Informationen zu IP-, MAC-Adressen und der Netzwerk-Topologie aus. Die Systeminformationen werden durch macmon NAC zueinander korreliert und im Hintergrund abgeglichen, um Adressmanipulationen und andere Angriffsversuche zu unterbinden.

Die grafische Darstellung des Netzwerkes durch macmon NAC erlaubt unter anderem das Filtern nach Hardwaretypen, VLANs und mehr und erlaubt die schnelle Aufdeckung von Konfigurationsfehlern in diesen Bereichen. Endpunkte, die (noch) nicht bekannt sind, werden so schnell erkannt.

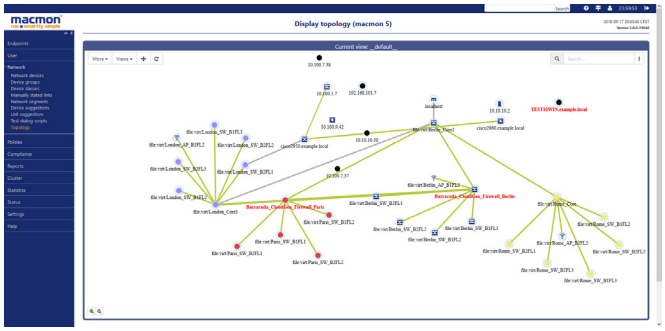

Abbildung 4 - Graphische Netzwerkdarstellung durch macmon NAC

Technisches

Die Anbindung erfordert Barracuda CloudGen Firewall Release 7.2.3 oder neuer und macmon Premium Bundle.

Mehr Informationen

Barracuda Campus:
https://campus.barracuda.com/doc/73718914/

macmon secure GmbH:
https://www.macmon.eu

macmon
nac intelligent einfach

Die macmon secure GmbH beschäftigt sich seit 2003 mit der Entwicklung von Netzwerksicherheitssoftware und hat ihren Firmensitz im Herzen Berlins. Die Network Access Control (NAC) Lösung macmon wird vollständig in Deutschland entwickelt und weltweit eingesetzt, um Netzwerke vor unberechtigten Zugriffen zu schützen. Die Kunden von macmon secure kommen aus diversen Branchen und reichen von mittelständischen Firmen bis hin zu großen internationalen Konzernen. Das Ziel: Jedem Unternehmen eine flexible und effiziente NAC-Lösung anzubieten, die mit geringem Aufwand, aber erheblichem Mehrwert für die Netzwerksicherheit des Unternehmens implementiert werden kann. macmon secure ist Mitglied der Trusted Computing Group und aktiv an verschiedenen Forschungsprojekten beteiligt.

Barracuda
Your journey, secured.