Jahrelange Forschung, Out-of-the-Box verfügbar

Angriffe auf Unternehmensnetzwerke sind heute praktisch an der Tagesordnung. Viele Angriffe werden stümperhaft mit weit verbreiteten Tools ausgeführt. Andere Angriffe sind hochprofessionell, oft speziell auf ein Unternehmen zugeschnitten. Egal ob dilettantische Angreifer, die interne Daten öffentlich zugänglich machen oder ob Profis Blueprints an die Konkurrenz verkaufen – der Schaden ist enorm.

Benötigt wird eine Lösung, welche beide Arten von Angriffen zuverlässig erkennt und die Reaktion darauf unterstützt.

Funktionsweise

Die Lastline Breach Detection-Plattform setzt sowohl bei der Live-Analyse des Netzwerk-Traffics als auch bei der Analyse von potenziell schädlichen Programmen neue Maßstäbe. Die Analyse von Programmen erfolgt mittels einer Sandbox, welche Erkenntnisse aus jahrelanger universitärer Forschung umsetzt. Im Gegensatz zu anderen Sandbox-Lösungen sieht die von Lastline jede einzelne ausgeführte Instruktion und kann darauf reagieren. Überprüft etwa die Malware, ob ein spezielles Programm (z. B. ein Virenscanner) installiert ist, kann sowohl die Anwesenheit als auch die Abwesenheit dieser Software vorgegaukelt werden. So ist es möglich, unterschiedliche „Ausführungspfade" einer Software zu analysieren, um so schädliches Verhalten zuverlässiger zu erkennen. Vor allem fortgeschrittene Malware versucht mittlerweile, solche Sandbox-Umgebungen zu erkennen und darauf zu reagieren, indem sie sich beispielsweise beendet. Um dies zu verhindern, kommt bei Lastline eine FUSE (Full System Emulation) genannte Technik zum Einsatz. Dabei wird von der virtuellen Umgebung direkt die Hardware selbst und nicht nur das Betriebssystem simuliert. Wird schädliche Software auf alternativen Wegen in ein Unternehmen eingeschleust (z. B. über USB-Sticks), steht die Software selbst nicht zur Verfügung, um analysiert zu werden. Die Anwesenheit schädlicher Software kann aber durch Überwachung des Netzwerkverkehrs erkannt werden. Hierzu prüft Lastline den Netzwerkverkehr auf die Anwesenheit von Indicators of Compromise (IoC), etwa IPs und URLs von bekannten Command and Control Servern oder verdächtige Verhaltensmuster. Die hierfür genutzten Informationen stammen aus einer Vielzahl von Kooperationen mit Partnern und Kunden. Lastline bietet Kunden die Möglichkeit, im eigenen System erkannte IoCs mit anderen Lastline-Kunden zu teilen.

Informationen aus den unterschiedlichen Quellen (Sandbox-Analyse, Netzwerk-Traffic Analyse, Anomalieerkennung) werden korreliert und als Incident an den Benutzer weitergegeben. Ein Incident besteht aus einer Vielzahl kleinerer Events, welche zu der allgemeinen Score (Bewertung der Kritikalität) beitragen. Wird eines dieser Events fälschlicherweise als False-Positive oder False-Negative gewertet, hat dies nur eine relativ geringe Auswirkung auf den Gesamtscore.

Um die Integration in bestehende Security-Infrastruktur so flexibel wie möglich zu gestalten, stellt Lastine eine offene Programmierschnittstelle (API) bereit, welche es erlaubt, Informationen über potenziell schädliche Verbindungsversuche an eine Firewall weiter zu geben. Diese kann dann die passenden Maßnahmen ergreifen.

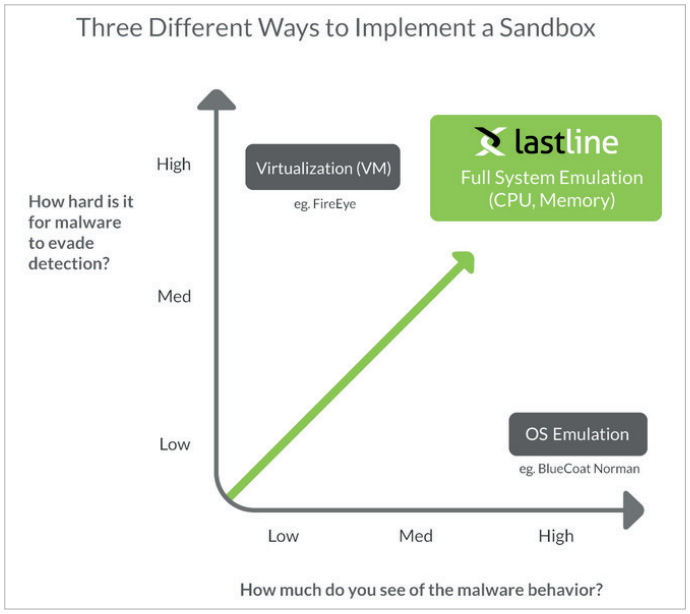

Abbildung 1: Funktionsweise

Architekturmodell

Lastline Enterprise kann in zwei verschiedenen Varianten betrieben werden: „Hosted by iT-CUBE" oder „on-premise".
Bei der von uns betriebenen Variante werden Sensoren im Unternehmensnetzwerk verteilt. Diese Sensoren senden Informationen an ein von iT-CUBE betriebenes Backend. Dieses Modell erlaubt es, die gesamte Leistungsfähigkeit von Lastline zu nutzen, ohne viel Hardware kaufen und das Backend selber betreiben zu müssen.

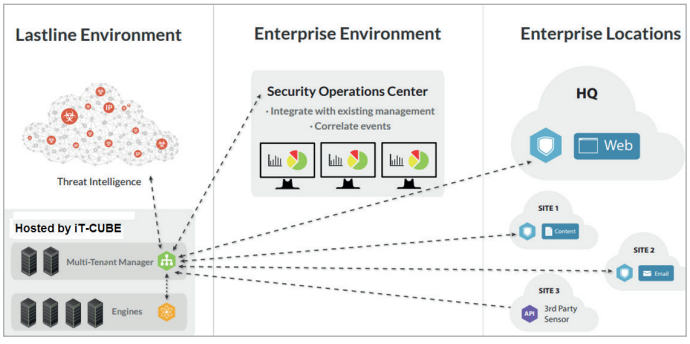

Abbildung 2: Architekturmodell „hosted by iT-CUBE"

Um erhöhten Anforderungen an Datenschutz bzw. Speicherung der Daten gerecht zu werden, kann das Lastline-Backend vollständig im eigenen Unternehmen betrieben werden. Sollen mehrere Standorte gesichert werden, kann das Backend in der Zentrale betrieben werden. Die Außenstellen werden dann nur mit Sensoren ausgestattet.

Üblicherweise erhalten Lastline-Sensoren den Netzwerk-Traffic über Span-Ports oder Netzwerk-TAPs. Es besteht auch die Möglichkeit, Sensoren in-line zu betreiben. In diesem Fall wird aber die Verwendung von sogenannten Fail-Open-Kits empfohlen.

Jede Lastline-Komponente kann auf handelsüblicher Serverhardware betrieben werden. Der Kauf von speziellen Appliances ist nicht nötig, da die Software als Virtual Appliance ausgeliefert wird. Darauf sind bereits alle nötigen Tools vorinstalliert und müssen nur noch minimal konfiguriert werden. Dieses Konzept erlaubt die Kombination aus handelsüblicher Hardware mit dem geringen Betriebsaufwand einer Appliance.

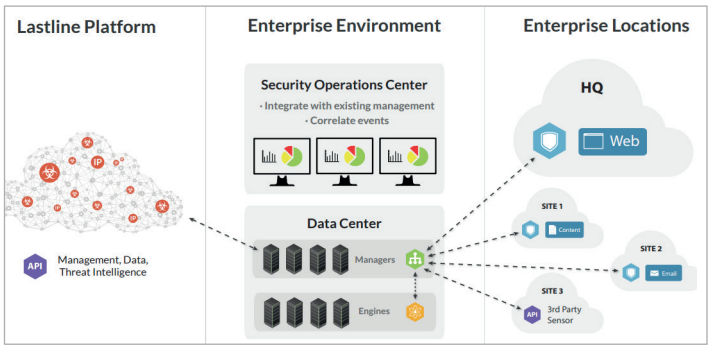

Abbildung 3: Architekturmodell „on-premise“

Leistungen

iT-CUBE hilft Ihnen bei der Planung und Umsetzung der Installation von Lastline. Zusätzlich beraten wir Sie bei der Integration und Auswahl von 3rd-Party-Komponenten und führen die Integration der Lösung in Ihre bestehenden Logmanagement-Systeme (SIEM) durch. Während der Nutzung von Lastline ermitteln wir kontinuierlich neue Use Cases und Prozesse, um auf Alarme optimal reagieren zu können. Gerne betreiben wir Ihr Lastline-Backend als Managed Security Service. Verfügen Sie bereits über ein Security Operation Center, integrieren wir Lastline in dieses.

Wir von iT-CUBE sind stets um die Erweiterung und Erstellung von Incident Response-Prozessen und der ganzheitlichen Umsetzung des Security-Konzepts bemüht. Im Falle einer Cyberattacke werten wir die gefundene Malware aus und erstellen eine persönlich auf Sie zugeschnittene Handlungsempfehlung.

Nutzen

Die Experten von iT-CUBE haben bereits zahlreiche Projekte mit verschiedensten Produkten erfolgreich umgesetzt. Wir nutzen diese jahrelange Erfahrung, um Lastline perfekt in Ihre bestehnde Infrastruktur zu integrieren. Firewall-Systeme können, basierend auf Lastline-Alarmen, genutzt werden, um einzelne Systeme oder ganze Abteilunge zu isolieren.

Zu unseren Kunden zählen wir kleine Unternehmen, aber auch zahlreiche international arbeitende Konzerne. Dank dieser Vielfalt an Praxiserfahrung können wir unser Wissen optimal nutzen, um Lastline in jede Umgebung zu integrieren.

Unsere Mitarbeiter stehen im engen Kontakt mit Lastline. So können wir sowohl technische als auch organisatorische Fragen schnell klären. iT-CUBE war von Anfang an dabei. Kurz nachdem Lastline den europäischen Markt erreichte, starteten wir bereits mit den ersten Lastline-Projekten durch.

Dank der Lösung von Lastline kann verdächtiges Verhalten im Netzwerkverkehr entdeckt und verdächtige Software aus E-Mails und dem Netzwerk-Traffic extrahiert und analysiert werden. Noch unbekannte Angriffe können so schnell erkannt werden. Lastline aggregiert Informationen aus verschiedensten Quellen zu einem verlässlichen Alarm. Darüber hinaus wird die Erkennung unterschiedlicher Phasen eines Angriffs ermöglicht. Außerdem erkennt Lastline, ob bestimmte Phasen eines Angriffs (z. B. Data Exfiltration) erfolgreich waren.

Eine Geschichte

Vor etwa drei Monaten wurde die bestehende IT-Security-Infrastruktur eines Unternehmens um die Lastline Enterprise erweitert. Das Backend wird von einem zuverlässigen lokalen Partner betrieben und in jeder der drei Zweigstellen wurde mindestens ein Sensor platziert. Die Logs aller Systeme (Endpoint AntiVirus, ForceScout NAC, …) werden in Splunk indexiert.

Eines Tages zur Mittagszeit erkennt Lastline den Download einer unbekannten Datei. Die Sandbox-Analyse ergibt, dass diese Datei gezielt Benutzernamen/Passwörter heraus filtert und zusätzlich erhebliche Anstrengungen unternimmt, um klassische Analysesysteme auszuhebeln. Der von Lastline generierte Alarm wird in Splunk indexiert. Eigene Splunk-Suchen erkennen in Echtzeit, dass die Endpoint AntiViren-Lösung keine verdächtigen Aktivitäten auf dem betroffenen Endpoint meldet. Daraufhin wird ein Splunk-Alarm generiert und die NAC (Network Access Control)-Lösung wird angewiesen, den Client in ein Quarantäne-V-LAN umzuleiten. Mitarbeiter des Security Operation Center werden alarmiert und entfernen das System.

Die forensische Analyse ergab folgendes: Auf dem betroffenen Endpoint (einem Entwicklungssystem) war seit zwei Monaten ein Dropper installiert. Hierbei handelt es sich um Software, die nichts anderes macht als andere Software nachzuladen. Dieser Dropper hatte erst jetzt versucht, die von Lastline erkannte Software nachzuladen. Es handelte sich tatsächlich um Software zum Diebstahl von Benutzerdaten und wurde zu diesem Zeitpunkt von noch keinem Anti-Viren Programm erkannt. Der Dropper gelangte vermutlich über einen präparierten USB-Stick auf den Server.

Dank der frühzeitigen Erkennung und hervorragender Kooperation verschiedener Systeme konnte der Abfluss von Daten verhindert werden. Die ermittelten IoCs (Hashwerte, involvierte IPs und URLs, …) wurden über die Lastline-Plattform anderen Kunden zugänglich gemacht.

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de