Kiteworks

PRODUKTINFORMATION

Kiteworks gehärtete virtuelle Appliance reduziert durch mehrere Sicherheitslayer die Ausnutzung von Sicherheitslücken und das Ausmaß der Auswirkungen drastisch

Die branchenweit am besten gehärtete Appliance für die Kommunikation vertraulicher Inhalte bietet Kunden Sicherheit, indem sie den CVSS-Schweregrad von Schwachstellen wie Log4Shell von 10 auf 4 reduziert.

Kiteworks baut die Sicherheit von Grund auf in das Private Content Network ein, indem es alle seine Komponenten in eine gehärtete virtuelle Appliance einbindet, die die CVSS-Werte (Common Vulnerability Scoring System) für die Ausnutzbarkeit und die Auswirkungen etwaiger Schwachstellen reduziert. Infolgedessen stellen Sicherheitslücken, die in anderen Anwendungen einen hohen oder sogar kritischen Schweregrad haben, für Kiteworks-Kunden ein viel geringeres Risiko dar. Dies bedeutet einen besseren Schutz für vertrauliche Inhalte der Kunden und eine höhere Sicherheit im Hinblick auf komplexe anhaltende Bedrohungen.

Erheblich reduziertes mit der Angreifbarkeit einer Schwachstelle verbundenes Sicherheitsrisiko

Die gehärtete virtuelle Appliance von Kiteworks ist so konzipiert, dass sie die Anzahl der potenziellen Schwachstellen in ihren Bibliotheken reduziert und die zum Ausnutzen dieser Schwachstellen erforderliche Angriffskomplexität erhöht.

- **Eingebettete Netzwerk-Firewall und WAF.** Die gehärtete virtuelle Appliance öffnet in ihrer integrierten Netzwerk-Firewall nur notwendige Ports und schützt Inhalte hinter internen Service-Ebenen mit Zugriffskontrollen und geringstmöglichen Privilegien. Sie überwacht kontinuierlich gefährliche Verbindungen über das eingebettete IPS und riskante Webanfragen über die integrierte WAF und blockiert diese dynamisch.
- **Zero-trust-Least-Privilege-Zugang.** Administratoren haben nur wenige privilegierte Benutzerkonten mit genau definierten Rechten und keinen Zugriff auf das Betriebssystem. Um für Diagnose- und Reparaturzwecke Zugriff auf das Betriebssystem zu erhalten, erhält ein zertifizierter, authentifizierter Kiteworks-Support-Techniker über ein zweistufiges Sicherheitsprotokoll, das die ausdrückliche Zustimmung des Kunden und von Kiteworks erfordert, einen temporären, vollständig protokollierten Zugriff.
- **Minimiert die Angriffsfläche.** Kiteworks fügt nur absolut notwendige Bibliotheken und Treiber zu einem reinen Linux-Betriebssystem (OS) hinzu und deaktiviert nicht benötigte Funktionen und Dienste.

Erheblich reduziertes mit den Auswirkungen eines Angriffs verbundenes Sicherheitsrisiko

Das Private Content Network nutzt auch interne Schutzmechanismen, um die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der Inhalte zu verringern:

- **KI-basierte Erkennung von Anomalien.** Die eingebettete Künstliche Intelligenz (KI) erkennt anomale Datenübertragungen, um Sicherheitsfachkräfte schnell vor einer möglichen Exfiltration zu warnen.
- **Erweiterte Intrusion Detection und Alarmfunktionen.** Kiteworks überwacht das Verhalten aller ausführbaren Dateien, Dateisysteme und den Internetverkehr. Es setzt strenge Richtlinien durch, sendet Warnmeldungen und schaltet unerwartete Aktivitäten ab, bevor ein Cyberkrimineller sensible Inhalte manipulieren oder exfiltrieren kann..
- **Blockieren von Zero-Day-Bedrohungen.** Kiteworks unterbindet den direkten Zugriff eines Exploits auf Inhalte, Metadaten, Netzwerke und andere Ressourcen, indem es Bibliotheken von Drittanbietern innerhalb einer Sandbox auf Betriebssystemebene ausführt (und nicht direkt auf dem Betriebssystem).

Das Ergebnis? Schwerwiegende Sicherheitslücken sind eher ein nebensächliches Übel als ein großes Problem

Als Log4Shell bekannt wurde, haben sich Unternehmen auf der ganzen Welt beeilt, ihre Kunden zu alarmieren und Notfall-Updates für Hunderte oder Tausende von Anwendungen durchzuführen. Die Log4Shell-Schwachstelle (CVE-2021-44228) betrifft ein Open-Source-Protokollierungs-Framework namens Log4j, das in Millionen von Anwendungen zu finden ist. Ihr CVSS-Score ist 10 - der höchstmögliche Schweregrad. Betrachtet man Log4j jedoch durch die Brille des Kiteworks Private Content Network, liegt der CVSS-Score höchstens bei 4. Das liegt daran, dass die angreifbaren APIs von Log4j von Kiteworks deaktiviert werden und die angreifbare Bibliothek eines Drittanbieters streng überwacht wird, während sie in einer Sandbox ausgeführt wird.

Ein weiteres Beispiel aus jüngster Zeit sind die laufenden White-Box-Übungen von Kiteworks, bei denen ein von Kiteworks autorisierter und geschulter Sicherheitsexperte versuchte, eine vierstufige Schwachstellenkette zu erstellen und auszunutzen - eine der schwierigsten Architekturen und eine der folgenreichsten, wenn sie ausgeführt wird. Diese Art von Schwachstelle würde normalerweise die kritischste CVSS-Wertung von 10 erhalten und eine sofortige Behebung erfordern. Die zahlreichen Abwehrmechanismen von Kiteworks reduzierten jedoch die tatsächliche Ausnutzbarkeit und die Auswirkungen auf einen unkritischen Wert, der nur einen kleinen Teil der Implementierungen betrifft.