SWS
COMPUTERSYSTEME
Member of ACP Group

DNS SECURITY

Der äußere Schutzwall für Ihr Unternehmen

IT for innovators.

Member of ACP Group

SWS DNS Security – der äußere Schutzwall für Ihr Unternehmen

Herausforderung:

Die Nutzung von Public Cloud Services im Unternehmen führt zu fehlender Übersicht und mangelnder Transparenz. Ein Großteil der Clients arbeitet mobil und ohne VPN. Somit werden sie nicht von der Firmen-IT geschützt. Es entstehen Sicherheitslücken sowie Risiken für Datenverluste durch Schatten-IT.
Das führt zu weiteren Herausforderungen in der ganzheitlichen IT-Sicherheit.

Lösung:

SWS DNS Security ist ein SaaS-Clouddienst. Damit werden im ersten Schritt Domain-Namen in IP-Adressen vor dem Zugriff auf Webseiten aufgelöst. Durch Blockieren der Namensauflösung von Seiten, die in Zusammenhang mit Malware, Ransomware oder Phishing stehen, ist der Benutzer kontinuierlich geschützt, auch außerhalb der Firmen-Umgebung und ohne VPN Verbindung. Somit werden Angriffe abgewehrt, noch bevor sie das Endgerät erreichen.
Selbst wenn das Endgerät schon kompromittiert ist, werden Verbindungen zu Command- und Control-Servern verhindert und die Kommunikation zum Angreifer schlägt fehl.

Leistungsmerkmale:

- Blockieren der Namensauflösung zu Seiten, die durch die Talos Reputation-Datenbank als malicious identifiziert wurden und mit Ransomware, Malware oder Phishing in Zusammenhang stehen
- Schutz der Benutzer innerhalb und außerhalb des Firmennetzwerks
- Blockieren von Verbindungen zu Command & Control Servern
- Domain-Anfragen und IP-Antworten werden auf DNS-Ebene blockiert, über jeden Port und jedes Protokoll
- Echtzeit-Aktivitätssuche und periodische Berichte im monatlichen Zyklus (auf ausdrücklichem Wunsch Berichte auch wöchentlich oder täglich ohne zusätzliche Kosten)
- Filter für mehr als 80 Inhaltskategorien
- Kundenspezifisches Black- und Whitelisting
- Direkte IP-Verbindungen werden auf IP-Ebene blockiert (nur bei Installation des Roaming-Clients)
- Identifikation gezielter Angriffe durch Vergleich lokaler und globaler Verhaltensmuster
- Kontrolle und ggf. Unterbindung von Schatten-IT und Cloud-Nutzung durch Erkennung und Risikobewertung der verwendeten Apps
- Durchsetzung von Richtlinien auf Netzsegment-Ebene sowie durch AD-Benutzer- bzw. Gruppenzugehörigkeiten möglich
- Aufrufe riskanter Domains werden über einen Cloud-Proxy geleitet und auf Schadsoftware geprüft

Ihr Nutzen

- Filter für mehr Inhaltskategorien
- Schutz der Benutzer
- Echtzeit-Aktivitätssuche
- Kundenspezifisches Black- und Whitelisting
- Risikobewertung
- Identifikation gezielter Angriffe

Sie möchten mehr über DNS Security erfahren?
So erreichen Sie uns:

SWS Computersysteme AG
+49 8586 9604 0
vertrieb@sws.de