runIP | RADAR

Sicherheit und Visibilität für ihre DNS und DHCP Umgebung

In modernen TCP/IP-Netzwerken ist DNS einer der kritischsten Netzwerkdienste, da die Namensauflösung eine zentrale Rolle bei der Konnektivität von Systemen und Anwendungen spielt. DNS gehört daher auch zu den bevorzugten Zielen böswilliger Akteure im Internet. Dies liegt vor allem daran, dass Benutzer durch die Kontrolle eines DNS-Servers gezielt auf Server des Angreifers umgeleitet werden können. Darüber hinaus wird DNS auch für DDoS-Attacken genutzt, vor allem via DNS Amplification. Dabei sendet ein Angreifer kleine DNS-Anfragen mit der gefälschten Adresse seines Opfers an einen DNS Server mit dem Ziel, möglichst große Antworten zu generieren, die der DNS Server dann an das Opfer sendet. Auf diese Weise kann der Angreifer seineAttacke um einen Faktor bis zu 50 verstärken (daher Amplification). Schließlich spielt DNS in vielen weiteren Angriffsszenarien eine Rolle, beispielsweise als Kommunikationskanal für Command & Control Server oder bei der Exfiltration von Daten über DNS-Tunnel - also einem meist unauffälligen Datendiebstahl.

Der Absicherung von DNS kommt vor allem deshalb eine hohe Bedeutung zu, weil eine Kompromittierung dieses Dienstes die Verfügbarkeit nahezu aller Anwendungen erheblich beeinträchtigen kann. DDI-Lösungen vereinfachen zwar den Betrieb von DNS und DHCP, beinhalten aber in der Regel keine gezielten Sicherheitsmaßnahmen, um die Verfügbarkeit der Dienste jederzeit zu gewährleisten. runIP RADAR schließt diese Lücke und ermöglicht eine effiziente und robuste Absicherung der DNS-Infrastruktur.

Features im Detail - Alarmierung und Blockierung

runIP RADAR erlaubt die Definition von Rate Limits, bei deren Überschreitung Clients und/oder Ziele gezielt blockiert werden können. Bei Bedarf kann diese Blockierung auch den Client und die verwendete Domain umfassen. Für einzelne Adressbereiche oder Domains kann ebenfalls eine automatische Entsperrung nach Ablauf definierter Zeiten konfiguriert werden. Auf diese Weise kann man beispielsweise sicherstellen, dass die Adressbereiche von Gäste-WLANs nach einem Sicherheitsvorfall nicht dauerhaft gesperrt werden. Auch Sperrungen, die aufgrund laufender Angriffe gegen die Domain erfolgten, können so nach einer gewissen Sicherheitsfrist ohne manuellen Eingriff wieder aufgehoben werden.

Features im Detail - Logging

runIP RADAR ist in der Lage, den gesamten DNS- und DHCP-Verkehr im Netzwerk dezentral zu loggen und zu protokollieren bzw. zentral an ein bestehendes System beim Kunden weiterzuleiten. Die technischen Attribute, die geloggt werden sollen, sind dabei frei konfigurierbar. Darüber hinaus können auch Ausnahme-Listen, etwa für vertrauenswürdige Netzwerke oder DHCP Probes, definiert werden. Die Möglichkeit der Weiterleitung von Log-Daten an SIEM-Systeme erlaubt die einfache Integration in unternehmensweite Sicherheitslösungen und die Korrelation der aufgezeichneten Daten mit Security-Events, die von anderen Sicherheitslösungen generiert wurden. So können beispielsweise Angriffe auf die DNS-Infrastruktur schnell und zuverlässig erkannt und gemildert bzw. blockiert werden.

Ihr Nutzen

- Vollumfängliche Absicherung Ihrer DNS-Infrastruktur
- Schnelle Erkennung von DNS-Tunneln
- Weitgehende Verhinderung der Daten-Exfiltration über DNS
- Abwehr von DDoS-Attacken gegen die DNS-Infrastruktur
- Unterstützung bei der forensischen Analyse nach Sicherheitsvorfällen
- Enge Integration in die runIP Management Plattform

Integration in die runIP SERVICES PLATFORM

runIP RADAR läuft als Service auf den runIP Appliances von N3K. Es wird über eine separate Weboberfläche verwaltet und konfiguriert. Über den RADAR-Server erfolgt die gesamte Konfiguration von runIP RADAR, die auf alle runIP Appliances innerhalb des Netzwerks repliziert wird.

runIP | RADAR

GUI-basiertes Reporting

Der RADAR Server verfügt über ein intuitiv zu bedienendes GUI, . Über dieses GUI erfolgen Konfiguration und Steuerung des RADAR-Servers und sämtlicher Instanzen von runIP RADAR auf den einzelnen runIP Appliances. Das GUI bietet eine Vielzahl vorgefertigter Reports sowie einfache Möglichkeiten, individuelle Berichte zu erstellen. Zudem bietet das GUI leicht verständliche Statistiken zu Alarmierungen und RPZ-Treffern. Zu den vorgefertigten Berichten zählen:

- Rate-Limit-Überschreitungen, die auf unerwünschten Datenaustausch hindeuten
- Verwendung bereits blockierter DNS-Domains und Client-IPs
- Top-Clients, Top-Domains oder Top-FQDNs einschließlich häufig verwendeter, nicht auflösbarer Namen.

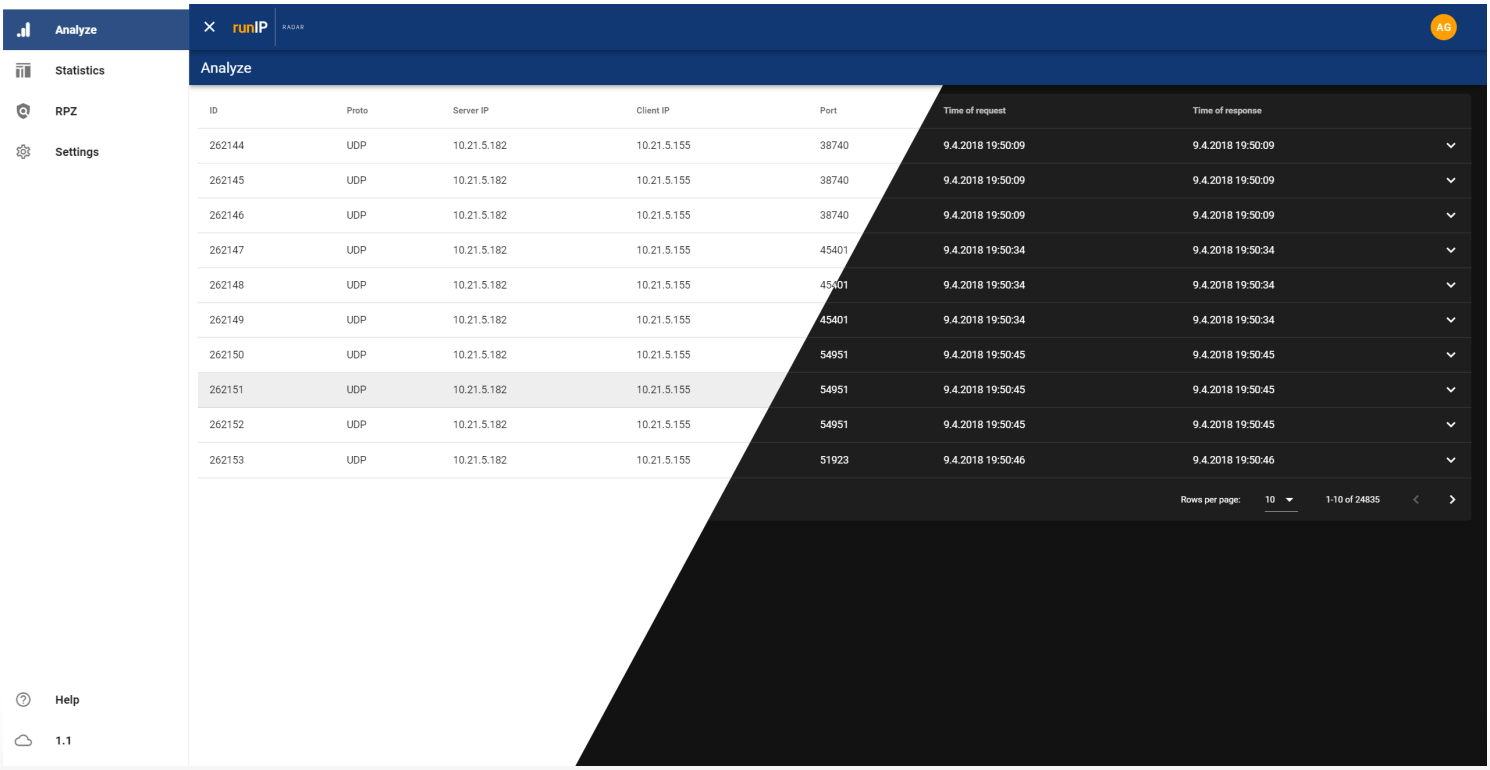
Unabhängig von der DDI-Lösung

runIP RADAR fußt auf der umfassenden DDI-Expertise von N3K und kann aktuell mit allen DDI-Lösungen eingesetzt werden, die von der runIP DDI-PLATFORM unterstützt werden:

- Nokia VitalQIP
- BT Diamond IPControl
- Men & Mice Micetro

Dabei profitiert runIP RADAR von der (optionalen) Hochverfügbarkeit der runIP-Hardware, sodass die DNS-Sicherheit jederzeit gewährleistet werden kann.

In einer späteren Version wird runIP RADAR völlig unabhängig von runIP sein und damit sämtliche DDI-Lösungen auf dem Markt unterstützen.



Über N3K: Schnellwachsende IP-Netzwerke erfordern professionelle Lösungen für die verschiedensten Facetten des Netzwerk-Managements. N3K Network Systems hat sich auf die Gebiete IP Address Management, Privilege Management sowie auf Active Directory Management spezialisiert. So können mit hoher Kompetenz auf die individuellen Anforderungen der Kunden zugeschnittene Lösungen entwickelt werden. N3K unterstützt die Kunden über den gesamten Projektzyklus hinweg bei Bedarfsanalyse, Konzeption, Projektplanung, Implementierung und Schulung. Hinzu kommen umfangreiche Wartungs-Services inklusive weltweitem 7x24-Support und direkter Einwahl beim Kunden. Aufbauend auf dieser einfachen und effektiven Philosophie hat sich N3K als führender Anbieter in Deutschland etabliert. Mehr als 50% der DAX-Unternehmen sind N3K-Kunden. Durch Standorte in den USA und in Singapur können die Leistungen weltweit erbracht werden.

n3K NETWORK SYSTEMS

N3K Network Systems · Ferdinand-Braun-Straße 2/1 · 74074 Heilbronn · Telefon +49 7131 59495 0 · Telefax +49 7131 59495 100 · www.n3k.com · info@n3k.de