



Daily DMZ Scan – DDS

Schwachstellen systematisch erkennen und beheben

Prüfen Sie täglich Ihre Server, die eine direkte Verbindung ins Internet haben auf Schwachstellen, um sich effektiv und zeitnah gegen Gefahren zu schützen? Der Medialine DMZ Scan gibt Ihnen tagesaktuelle Sicherheit, dass Ihre Systeme keine Schwachstellen aufweisen. Werden potentielle Einfallstore erkannt, können Sie sich schnell und effektiv gegen möglich Angriffe absichern – so sind Sie Angreifern immer einen Schritt voraus.

Was wir Ihnen bieten:

- tägliche Scans Ihrer demilitarisierten Zone (DMZ)
- unverzügliche Benachrichtigung über neue Schwachstellen
- tägliche automatisierte Erstellung eines Schwachstellen-Berichts
- variable Service Vertragslaufzeiten von einem oder drei Jahren

Der Schwachstellenscan wird täglich auf bis zu 16 IP-Adressen durchgeführt. Für den Einsatz bei mehr als 16 IP-Adressen in Ihrer DMZ, können mehrere Verträge kombiniert werden. Oder Sie entscheiden sich für ein Upgrade auf unseren Managed Vulnerability Scan (MVS) in Verbindung mit DDS.

Ablauf und Installation: DDS als virtuelle Appliance in der Medialine Cloud

Sie sind bereits Kunde bei uns und Ihre Infrastruktur läuft in einem unserer Rechenzentren? Perfekt – wir stellen Ihnen eine weitere virtuelle Maschine bereit. Der virtuelle Server wird nahtlos in Ihr Tenant integriert. Die benötigten Ressourcen des Servers sind im Angebot inkludiert. Der Zugriff auf die virtuelle Appliance und den Scanner erfolgt ausschließlich über SSH und HTTPS.

Die Scanbox

Sie betreuen Ihre Infrastruktur im eigenen Rechenzentrum oder Serverraum? Dann senden wir Ihnen die Medialine Scanbox zu. Sie bekommen die Scanbox in einem versiegelten Transportkoffer zugeschickt. Die Scanbox wird dann einfach mit einem oder mehreren Ethernet-Ports in Ihr Netzwerk integriert und führt die Scans eigenständig durch.



Features der Scanbox:

- Gesicherte SSH-Verbindung über LTE mit IPv6
- verschlüsselte SD-Karte – Ergebnisse und Reports werden sicher auf einer verschlüsselten Speicherkarte abgelegt
- vier Ethernet-Ports um drei Netzwerke (Netzwerke und auch VLANs) gleichzeitig zu scannen
- versiegelter Versand zum Schutz vor Manipulationen

In beiden Varianten ist eine Nessus Professional-Lizenz enthalten.
Die Scans und die Reports werden von sicherheitszertifizierten Mitarbeitern durchgeführt.

Schützen Sie sich vor Angreifern, indem Sie ihnen keine Plattform bieten.
Identifizieren und beheben Sie Schwachstellen, bevor es ein anderer tut.

Änderungen und Irrtümer vorbehalten. Es gelten unsere allgemeinen Geschäftsbedingungen in der jeweils aktuellen Fassung. Die Produktbeschreibung stellt noch kein verbindliches Angebot dar und dient ausschließlich der Information. Vertragsdetails sind aus Angeboten und Leistungsverzeichnissen zu entnehmen, welche wir gerne für Sie erstellen. Stand: 03/2021