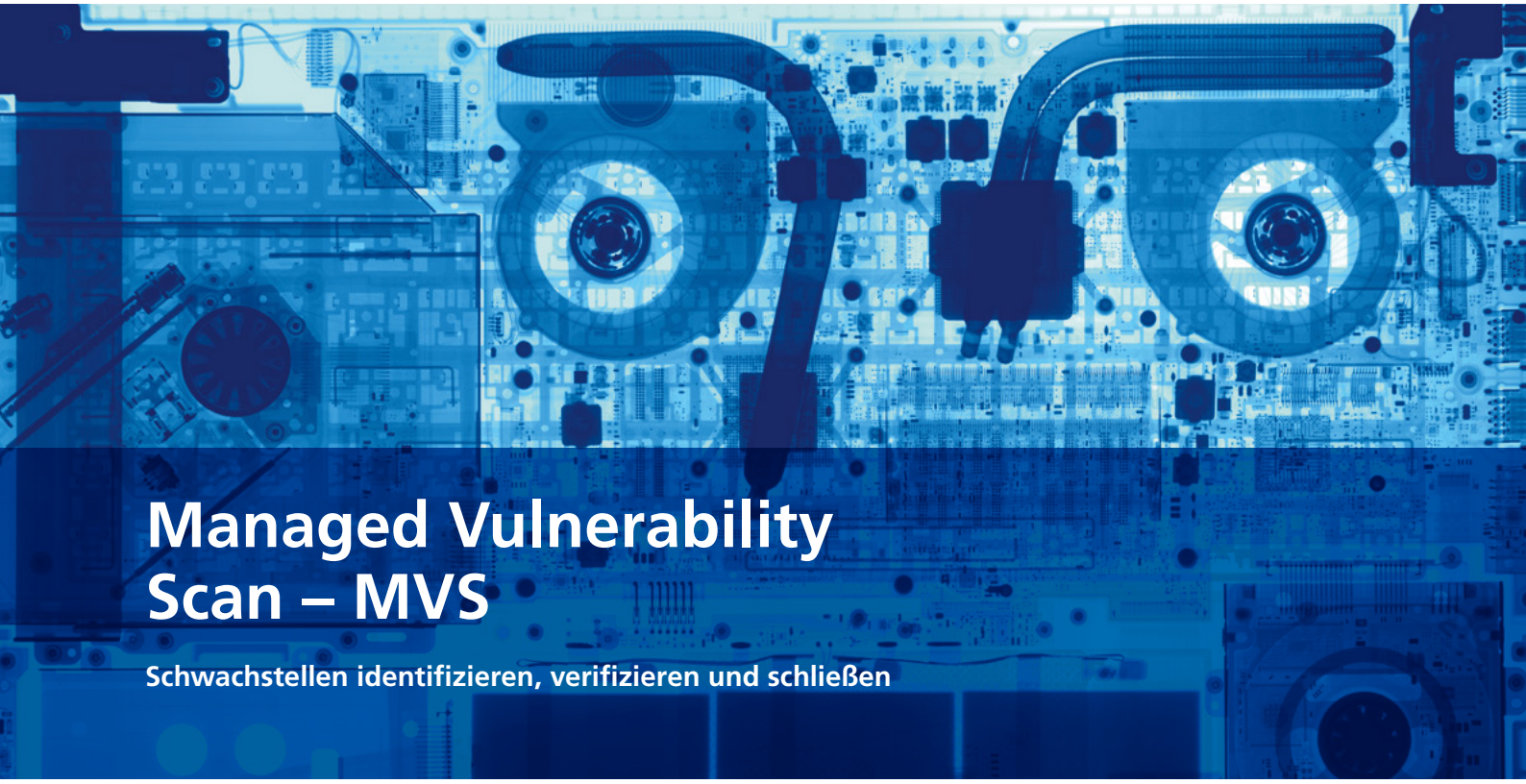

Managed Vulnerability Scan – MVS

Schwachstellen identifizieren, verifizieren und schließen

Software Vulnerabilities sind beliebte Einfallstore für Angreifer. Fehlende Updates, veraltete Softwareversionen oder einfach fehlendes Know-how beim Einrichten oder Absichern von Systemen, bieten Angreifern unzählige Wege in Ihre Infrastruktur.

Danach kann alles ganz schnell gehen: sie dringen in sensible Bereiche ein, greifen Geschäftsgeheimnisse ab, verschaffen sich Zugriff auf Kundendaten, übernehmen das Online-Banking und verschlüsseln alle Daten inkl. der Datensicherung. Der wirtschaftliche und der Image-Schaden, könnten nicht größer sein.
Nicht selten können solche Angriffe für geschädigte Unternehmen existenzbedrohend sein. Schützen Sie sich bevor der Ernstfall eintritt! Mit unserem Managed Vulnerability Scan helfen wir Ihnen, Ihre Anwendungen und Systeme vor Bedrohungen zu schützen und die Risiken durch Cyberangriffe effizient zu minimieren.

Was wir Ihnen bieten

Ob einmaliger Scan oder regelmäßiges Sicherheits-Update, der Managed Vulnerability Scan deckt Schwachstellen auf und hilft Ihnen dabei das Sicherheitsniveau Ihrer Infrastruktur nachhaltig und kontinuierlich zu verbessern.

Stellen Sie sich Ihren individuellen Managed Vulnerability Scan zusammen, der zu Ihrer Infrastruktur passt:

Scan-Art

- Scan S – bis 100 IP-Adressen
- Scan M – bis 250 IP-Adressen
- Scan L – bis 1000 IP-Adressen
- Scan XL – über 1000 IP-Adressen

Laufzeit

- 1 Jahr
- 3 Jahre

Reporting

- quartalsweise (Basic)
- monatlich (Standard)
- wöchentlich (Premium)

Wie gehen wir vor?

Im persönlichen Gespräch definieren wir gemeinsam Umfang und Parameter der Scans. Dabei bestimmen Sie Inhalte und Intervalle ganz nach den individuellen Gegebenheiten Ihres Geschäfts. Wir beraten Sie und stehen Ihnen mit Erfahrung und Expertise zur Seite um bestmögliche Ergebnisse zu erzielen.

Schritt für Schritt:

- Festlegung der Targets
- Durchführung des Scans
- Auswertung der Ergebnisse und Erstellung eines Reports
- Beseitigung der gefundenen Schwachstellen (nach Vereinbarung)
- Besprechung konkreter Maßnahmen zur Sicherheitsoptimierung Ihrer Infrastruktur

Sie sind bereits Kunde bei uns und Ihre Infrastruktur läuft in einem unserer Rechenzentren? Perfekt – wir stellen Ihnen eine weitere virtuelle Maschine bereit. Sollte Ihre Infrastruktur bei Ihnen im Rechenzentrum oder Serverraum laufen, erhalten Sie von uns die Medialine Scanbox.

MVS als virtuelle Appliance in der Medialine Cloud

Der virtuelle Server wird nahtlos in Ihr Tenant integriert. Die benötigten Ressourcen des Servers sind inklusive. Der Zugriff auf die virtuelle Appliance und den Scanner erfolgt ausschließlich über SSH und HTTPS.

Die Scanbox

Der Scan wird mit der Medialine Scanbox durchgeführt. Sie bekommen die Scanbox in einem verschlossenen Transportkoffer zugeschickt. Die Scanbox wird dann einfach mit einem oder mehreren Ethernet-Ports in Ihr Netzwerk integriert.

Features der Scanbox:

- Gesicherte SSH-Verbindung über LTE mit IPv6
- Verschlüsselte SD-Karte – Die Ergebnisse und Reports werden sicher auf einer verschlüsselten Speicherkarte abgelegt
- Vier Ethernet-Ports um drei Netzwerke (Netzwerke und auch VLANs) gleichzeitig zu scannen
- Die Scanbox ist versiegelt um Manipulationen auszuschließen

Sie haben ein DMZ-Netzwerk im Einsatz und stellen Dienste wie VPN, Citrix Gateway, oder OWA (Outlook Web Access) bereit? Dann wäre es doch umso wichtiger zu wissen, dass niemand von außen Schwachstellen ausnutzen und sich so Zutritt zu Ihrer Umgebung verschaffen kann!
Wir bieten Ihnen einen täglichen Scan der DMZ mit sofortiger Benachrichtigung, falls eine Schwachstelle gefunden wird. Damit sind Sie tagesaktuell und gegen jede neu entdeckte Schwachstelle geschützt.

Optionen zum MVS:

- Inkl. DDS – Daily DMZ Scan, alle DMZ-Systeme sind inklusive
- Ohne DDS, Einschränkung der Anzahl der IP-Adressen auf 16 IPs

In beiden Varianten ist eine Nessus Professional-Lizenz enthalten. Die Scans und die Reports werden von unseren Security-Zertifizierten-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