cryptware
secure your way

Vorteile der Lösung:

- Tägliche Schwachstellen-Scans Ihrer online Systeme
- 100 % Abdeckung Ihrer öffentlichen Systeme und fortlaufende Erweiterung möglich
- Sofortige Benachrichtigung bei kritischen (CVSS) Schwachstellen
- Detaillierte Informationen zum Beheben der jeweiligen Schwachstellen
- Zusätzlich monatliche Übersichtsreports mit allen Ergebnissen
- Kein Zugang zu Ihrem Netzwerk nötig
- Kann ohne Anpassung sofort gestartet werden
- 365 Tage im Jahr als Abo
- Für Industrie und Mittelstand

Tägliche Cyber Schwachstellen-Scans aller online Assets

Täglich wird das gesamte Internet von Kriminellen nach verwundbaren Assets durchsucht und angegriffen. Diese missbrauchen mehr als 10.000 neue Schwachstellen jährlich in Standardsoftware und Betriebssystemen. Früher oder später ist dadurch jedes Asset betroffen.
Über 10 % dieser Schwachstellen sind, nach der Definition des Industriestandards CVSS, kritisch. Kritische Schwachstellen erlauben Angreifern beispielsweise die komplette Kontrolle Ihres Systems zu übernehmen und erheblichen Schaden anzurichten.

Kenntnis darüber zu haben, ob die eigenen Systeme von kritischen Schwachstellen betroffen sind, ist essentiell. In solchen Fällen ist schnelles Handeln notwendig, um die Schwachstellen zu beheben bevor sie ausgenutzt werden.
Unsere täglichen Schwachstellen-Überprüfungen durch die innoSec GmbH helfen Ihnen den Angreifern voraus zu sein. Sie werden sofort benachrichtigt, wenn Ihre Assets von kritischen Schwachstellen betroffen sind. Zusätzlich erhalten Sie alle notwendigen technischen Details, um diese schnell zu beheben.

Täglich prüfen wir Ihre Systeme auf Schwachstellen

Tägliche Überprüfungen all Ihrer öffentlichen Systeme im Internet, wie beispielsweise Cloud-Lösungen, Firewall und Proxy, Web- und Mail-Server, VPN, DNS, SIP, IoT, Homeoffice etc. durch marktfüh-

365 Tage/Jahr

Scan aller online Assets

Sofortige Alarmierung

renden Industriestandard Schwachstellen-Scanner. Es können Konfigurationsfehler, unzureichende Patch-Stände, unsichere Dienste etc. erkannt werden. Die Schwachstellen werden klassifiziert, beurteilt und genau beschrieben.

Vergessene Systeme, die durch die Zeit verwundbar werden, gehören der Vergangenheit an. Genauso wie übersehene Patches und andere vermeidbare Fehler, die vielen Unternehmen bereits spürbare Schäden verursacht haben.

Leistungsumfang

Tägliche unabhängige Überprüfung Ihrer öffentlich erreichbaren Assets (per IP-Adresse oder FQDN) nach Schwachstellen. Die Überprüfung wird mit einem marktführenden professionellen Industrie Schwachstellen-Scanner durchgeführt. Bei der Entdeckung kritischer Schwachstellen, werden Sie sofort per E-Mail benachrichtigt. Die Benachrichtigung beinhaltet Informationen zu der jeweiligen Schwachstelle, dessen Risikopotential und entsprechenden Handlungsempfehlungen zum Beheben. Zusätzlich wird einmal pro Monat ein kompletter Bericht aller überprüften Assets zugestellt, welcher auch weniger kritische Schwachstellen beinhaltet.

Leistungsumfang

- Einrichtungskosten inkl.
- Initiales scannen aller Assets und Erstellung eines gesamten Berichtes mit allen Findings
- Tägliches scannen aller Assets
- Monatlicher Bericht aller gefundenen Schwachstellen
- Sofortige E-Mail-Benachrichtigung bei Entdeckung kritischer Schwachstellen:
  - Benennung des betroffenen Assets (IP oder Domain)
  - Beschreibung der kritischen Schwachstelle
  - Referenzen zur kritischen Schwachstelle (sofern vorhanden, z.B. CVE)
  - Handlungsempfehlungen (sofern möglich, z.B. Patch Download Link)

Optional (Aufpreis auf Anfrage)

- Coverage: Zyklischer Abgleich Ihrer DNS Daten mit den zu scannenden Assets
- Dedicated Scan Engines: Z.B. bei individuellen Cloud-Anbindungen
- Remediate: Beheben der kritischen Lücken

innoSec

cryptware
secure your way

CryptWare IT Security GmbH
Frankfurter Str. 2
65549 Limburg

Phone: +49 (0) 6431 977790 - 0
Fax: +49 (0) 6431 977790 - 22
info@cryptware.eu

www.cryptware.eu