CYBERSEC-NG
Swiss Cybersecurity

IT-Vulnerability Scanning Service

KONTINUIERLICHE IT-SICHERHEIT

Im Jahr 2019 wurden in einer der bekanntesten Schwachstellen-datenbanken der Welt (CVE-Details) um die 12'000 Schwachstellen gemeldet. Im Schnitt werden also monatlich ca. 1000 neue Schwachstellen entdeckt. Daraus ergibt sich, dass eine kontinuerliche Überwachung Ihrer IT-Infrastruktur und Applikationen unabdingbar geworden ist.

NETZWERKSCHUTZ

Unser Service ermöglicht es Ihnen Schwachstellen in Ihrem Perimeter zu erkennen und zu beheben bevor diese von Cyberkriminellen ausgenutzt werden.

WEBSEITENSCHUTZ

Web Applikationen werden durch den Einsatz moderner Technologien zunehmend komplexer. Komplexität führt zu einer grösseren Angriffsfläche und entsprechend zu mehr Schwachstellen. Häufig werden kritische, verwundbare Web Applikationen in der Praxis durch eine Web Application Firewall (WAF) geschützt. Problematisch bei diesem Ansatz ist, dass die WAF einen Single Point of Failure darstellt. Miskonfigurationen oder gar der Ausfall einer WAF führt dazu, dass die Web Applikation exponiert und angreifbar wird. Unser Service hilft Ihnen Schwachstellen in Ihren Web Applikationen aufzufinden, diese zu härten und die Abhängigkeit von WAF's zu reduzieren.

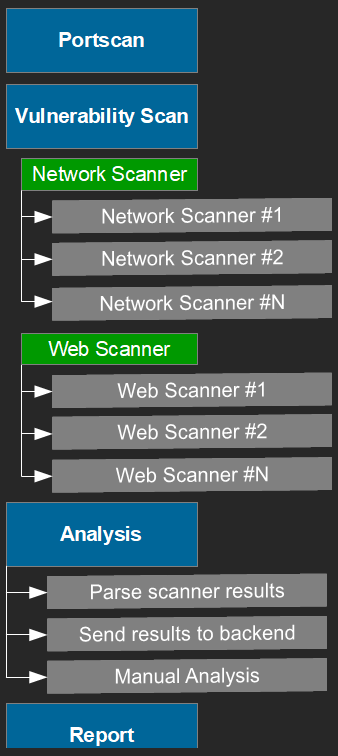
Unser Vulnerability Scanning Service basiert auf Cutting-Edge Technologien und integriert eine Vielzahl von Schwachstellenscannern und eigenentwickelten Tools zu einer Multivendor Scanning Plattform. Er ermöglicht Ihnen die kontinuierliche Überwachung Ihrer exponierten Web Applikationen und Netzwerk Services (VPN, SSH, FTP, SMTP, etc.) im Bezug auf Sicherheitsschwachstellen und erreicht eine bisher ungesehene Breite und Tiefe bei der automatisierten Auffindung von Sicherheitsschwachstellen.

Next Gen. Scanning Engine

Der klassische Ansatz bei der Durchführung eines Schwachstellenscans besteht darin, die Zielsysteme und/oder Applikationen mithilfe **eines** kommerziell verfügbaren Schwachstellenscanners (häfuig Nessus) zu überprüfen. Problematisch hierbei ist, dass jeder Schwachstellenscanner seine Vor- und Nachteile hat, einige Schwachstellen besser – andere schlechter findet. In der Praxis führt dies häufig dazu, dass auch offensichtliche Schwachstellen übersehen werden.

Uns hat sich die Frage gestellt, wie wir die höchstmögliche Abdeckung bei der automatisierten Suche nach Sicherheitsschwachstellen erreichen können und sind zum Schluss gekommen, dass **ein** Schwachstellenscanner nicht ausreichend ist. Unser Ansatz ist es die Besten kommerziellen- und Opensource Schwachstellenscanner in einer Multivendor Scanning Plattform zu vereinen.

Die untenstehende Grafik zeigt den Ablauf eines Vulnerability Scans.



Portscan

In einem ersten Schritt werden alle verfügbaren Ports gescannt und die dahinterliegenden Services identifiziert.

Vulnerability Scan

Die vom Portscan erhaltenen Daten werden automatisiert ausgewertet und an die Network- und Web Vulnerability Scanner weitergegeben. Die verschiedenen Scanner werden anschliessend abhängig von den Zielsystemen parallel oder sequentiell gestartet. Sobald ein Scan abgeschlossen ist, werden die Daten an unser Backend zur manuellen Anlyse gesendet.

Analysis

Die Daten der verschiedenen Scanner (Schwachstellen) werden manuell ausgewertet und zusätzlich auf False-Positives überprüft.

Report

Der Report kann in zwei verschiedenen Formaten ausgegeben werden:

1. Slim

Bei der Slim Variante werden die Rohdaten der Schwachstellen (Risikobewertung, Beschreibung, Gegenmassnahme, etc.) in einem gängigen Format (JSON, XML oder CSV) ausgegeben und können so in bestehende Vulnerability Management Lösungen integriert werden.

2. XL

Bei der XL Variante wird ein klassischer Penetration Testing Report inklusive einem für Nichttechniker verständlichen Management Summary erstellt.

CYBERSEC-NG
Swiss Cybersecurity

IT RISK MANAGEMENT

Sie erkennen aktuelle technische Sicherheitsrisiken, die Ihre IT-Infrastruktur und Applikationen bedrohen und sind in der Lage diese proaktiv zu beheben.

MESSBARKEIT

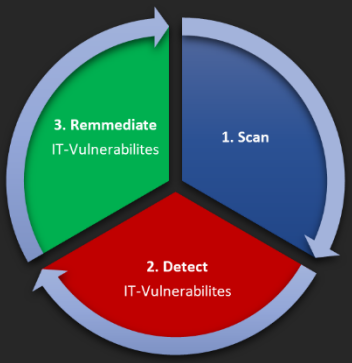
Durch die kontinuierliche Überwachung Ihrer IT-Infrastruktur und Applikationen sind Sie nicht nur gegenüber aktuellen Sicherheitsschwachstellen geschützt sondern können auch die Resultate der Vormonate vergleichen und feststellen ob bereits gemeldete Schwachstellen behoben wurden.

KONTAKT

Cybersec-ng
Grünaustrasse 1
3084 Wabern
078 729 38 39
office@cybersec-ng.ch

Features

Kontinuierliches Schwachstellenmonitoring:
Die Schwachstellenscans können in beliebigen zeitlichen Intervallen (bspw. wöchentlich, monatlich, quartalsweise, jährlich) durchgeführt werden.



Multivendor:
Integration diverser Opensource- und kommerzieller IT-Schwachstellenscanner und eigenentwickelter Tools zu einer einzigartigen, innovativen Plattform.

Präzision:
Durch die Kombination verschiedener, spezialisierter Schwachstellenscanner (Multivendor) erreicht unser Service eine bisher unerreichte Breite und Tiefe bei der automatisierten Auffindung von Sicherheitsschwachstellen.

Skalierbarkeit:
Der Vulnerability Scanning Service basiert auf einer flexiblen Microservice Architektur, die es ermöglicht den Service beliebig zu skalieren und auf die Bedürfnisse von Klein- und Grossbetrieben anzupassen.

Erweiterbarkeit:
Die Integration von zusätzlichen Tools / Schwachstellenscannern ist jederzeit möglich. Der Service wird zudem laufend weiterentwickelt um unseren Kunden ein Maximum an technischer Cybersicherheit zu bieten.

Einsatzgebiete

Health Check
Sie haben Ihre IT-Infrastruktur und/oder Applikationen noch nie auf Schwachstellen untersucht und möchten einen Überblick über den Sicherheitszustand Ihrer exponierten IT-Infrastruktur und/oder Applikationen erhalten.

Kritische Systeme und Applikationen
Sie verfügen über kritische, businessrelevante Systeme und/oder Applikationen (bspw. E-Commerce), die laufend gegenüber aktuellen Sicherheitsschwachstellen geschützt und überwacht werden sollen.

KMU's und Startups
Sie betreiben oder entwickeln Web Applikationen und/oder Netzwerkservices, verfügen aber über ein kleines Budget für IT-Security, können sich ausführliche Penetration Tests oder teure, aufwändig zu integrierende Sicherheitslösungen nicht leisten, möchten aber auf einen Grundschutz nicht verzichten.