External Attack Surface Assessment

Criminele hackers proberen toegang te krijgen tot uw netwerk. Het External Attack Surface Assessment (EASA) helpt u om uw zwakke plekken in kaart te brengen, zodat u deze kunt oplossen voordat aanvallers ze tegen u gebruiken.

Een External Attack Surface Assessment geeft u:

Inzicht in bedreigingen

Hoe kan een aanvaller schade aanrichten? We checken dit met scans, dreigingsinfo en tests.

Begrip van risico's

De kans is groot dat er schaduw-IT in uw organisatie is. Dit assessment laat u de risico's hiervan zien.

Acties voor verbetering

Met de resultaten van dit onderzoek kunt u snel actie ondernemen om uw aanvalsoppervlak te beschermen.

Waarom het External Attack Surface Assessment?

Criminele hackers, zoals ransomware-groepen, gebruiken alles wat ze kunnen vinden om u aan te vallen, van gehackte wachtwoorden tot kwetsbaarheden in applicaties. Weet u welke gevoelige informatie over uw organisatie online beschikbaar is voor aanvallers? Of welke van uw assets met internet verbonden zijn?

Een **External Attack Surface Assessment** scant proactief naar zwakke plekken, exposures en kwetsbaarheden rondom uw organisatie. Wij gebruiken zoveel mogelijk bronnen: van softwarerepositories tot dark web marktplaatsen. Zo kunt u actie ondernemen voordat criminelen deze informatie tegen u gebruiken.

Hoe het assessment werkt

1. Onderzoek

Welke van uw assets staan in contact met het internet? We beginnen met dit te scannen en in kaart te brengen. Daarbij nemen we één of meer domeinnamen of entiteitnamen als uitgangspunt.

2. Exposures

Dan volgt een scan van de geïdentificeerde assets en openbare repositories, eventuele exposures en datalekken te ontdekken. Hieronder vallen softwarerepository's, cloudopslag en databases.

3. Inloggegevens

Vervolgens combineren we deze assets met up-to-date dreigingsinformatie, bijvoorbeeld credential dumps en dark web marktplaatsen. We voeren ook password spraying uit, om te zien of we op deze manier toegang tot uw systemen kunnen krijgen.

4. Kwetsbaarheden

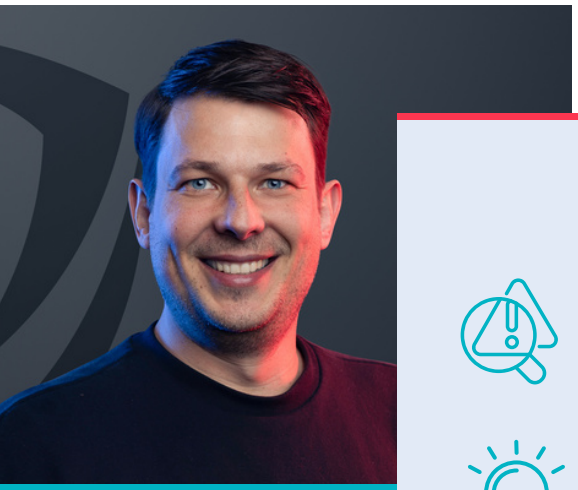
Uw geïdentificeerde assets worden gescand op technische kwetsbaarheden en misconfiguraties. Weinig aanbieders van external attack surface diensten testen dit zo grondig: u hebt nu een compleet beeld.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.



Voorbeeld | Attack Surface Assessment

Welk probleem had de klant?

Een gemeente wilde meer inzicht krijgen in welke van hun systemen verbonden waren met het internet Zij wilden meer controle hierover ervaren.

Resultaat

Tijdens het External Attack Surface Assessment stelden wij vast dat een systeem dat voor beheer werd gebruikt gehackt bleek te zijn en dat inloggegevens voor dit systeem verkocht werden op het dark web. Omdat we wisten welk systeem geraakt was, kon deze gemeente snel maatregelen nemen.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100

secura.com