VERHOOG UW CYBERWEERBAARHEID MET SECURA'S

PENTESTING DIENSTEN

Bevat uw systeem, netwerk of cloudconfiguratie zwakke plekken? U wilt dit weten voordat een aanvaller deze tegen u gebruikt. Wij kunnen u helpen bij het beoordelen en testen van uw digitale beveiliging. De afgelopen twintig jaar hebben onze klanten ons gevraagd security tests uit te voeren op vrijwel elk denkbaar doelwit.

DEZE PENTESTING DIENSTEN HELPEN U:

Ken uw kwetsbaarheden

U krijgt inzicht in potentiële entry points voor cyberaanvallen en in kwetsbaarheden.

Versterk uw verdediging

U krijgt concrete aanbevelingen, zodat u uw systemen kunt beschermen.

Blijf aanvallers voor

Onze specialisten hebben up-to-date kennis van aanvalstactieken, zodat u een voorsprong heeft.

HOE PENTESTING HELPT OM UW ORGANISATIE TE BESCHERMEN

Zelfs de meest robuuste systemen lopen het risico achterop te raken. Aanvallers ontwikkelen hun methoden voortdurend en gebruiken zowel legacyproblemen als de nieuwste kwetsbaarheden waar uw verdedigers misschien nog niet eens van op de hoogte zijn. Uw organisatie heeft waarschijnlijk veel geïnvesteerd in beveiligingsmaatregelen, maar penetratietests (pentesting) gaan een stap verder. Ze onderzoeken actief of uw technische verdedigingsmechanismen effectief zijn. Via gesimuleerde cyberaanvallen identificeren onze ethische hackers potentiële zwakke plekken voordat kwaadwillenden deze kunnen gebruiken.

Onze pentesting diensten combineren Vulnerability Assessments en Penetration Testing (VA/PT). Met een **vulnerability assessment** identificeren onze specialisten zoveel mogelijk kwetsbaarheden, zonder deze te exploiteren. Bij een **penetratietest** (pentest) simuleren onze testers een aanval, juist om kwetsbaarheden te exploiteren. De combinatie van deze brede en diepe methoden geven een grondig security overzicht.

Secura is opgericht in 2001 als technisch pentesting bedrijf. Ons team heeft dus al twintig jaar ervaring met Tactics, Techniques and Procedures (TTP's) van dreigingsactoren. Onze specialisten beschikken over dezelfde capaciteiten als actoren van nationale staten. Zij gebruiken deze kennis om u te helpen uw cyberweerbaarheid te versterken.

WELKE SYSTEMEN TESTEN WIJ?

Uw organisatie is uniek, net als uw beveiligingsbehoeften. Daarom bieden we assessments en tests op maat voor een breed scala aan systemen en infrastructuren, van IT tot OT en IoT. Of u nu de verdediging van een kritieke **webapplicatie**, een **interne infrastructuur**, een **connected apparaat** of een **OT-netwerk** wilt valideren, wij hebben de specialisten om u te helpen. Waar mogelijk volgen we internationaal erkende standaarden en kaders.

IT security testing

Het doel van een penetratietest is om zo duidelijk mogelijk te laten zien wat de gevolgen kunnen zijn van een bepaald probleem met uw IT-beveiliging, en wat dat voor uw organisatie zou betekenen. Veel organisaties kiezen naar aanleiding van een dergelijke test voor een structurele aanpak van hun IT-beveiliging. We kunnen een breed scala aan IT-testen en assessments uitvoeren, van applicatie tot mobiel en tot cloud. Als u meerdere systemen of applicaties heeft, raden we u aan de testprioriteit te bepalen met een Threat Modeling-sessie.

IT PENTESTING DIENSTEN

- **Internal Penetration Test**
- **Mobile Application Assessment**
- **Web Application Assessment**
- **Cloud Assessment**
- **Endpoint assessment**
- **Domain Name System assessment**
- **Configuration review assessment**
- **Wi-Fi Assessment**
- **Firewall review assessment**
- **External Attack Surface Assessment**
- **IT Threat Modeling**

OT security testing

Veel kritische processen, bijvoorbeeld in industriële omgevingen, zijn afhankelijk van Operationele Technologie (OT). Tegelijkertijd neem de connectie tussen IT en OT toe. Omdat zowel IT- als OT-systemen betrouwbaar moeten zijn, is testen van cruciaal belang voor alle systemen. Voor elke omgeving is echter een andere aanpak nodig. Secura's gespecialiseerde OT-team kan u helpen bij het beoordelen van de beveiliging van uw OT-systemen. Veel van de diensten die we aanbieden voor IT kunnen worden toegepast op OT-omgevingen, met aanpassingen.

SPECIFIEKE OT DIENSTEN

- **OT Vulnerability Assessment en Penetration Testing**
- **OT Threat Modeling**
- **OT Perimeter Assessment:** evalueert de beveiliging van de grens tussen informatietechnologie (IT) en operationele technologiesystemen (OT)
- **ICS Cyber FAT-SAT:** een uitbreiding van de conventionele FAT/SAT met een focus op cyberbeveiliging

IoT security testing

IoT-apparaten worden steeds meer een focus van onze testen. Aanvallers richten zich niet alleen op de netwerkinterfaces, zoals gebruikelijk is in de IT, maar ook op de hardware, firmware, cloud-gebaseerde backends en gerelateerde mobiele applicaties, die vaak onvoldoende worden begrepen. Wij testen deze componenten grondig in ons gespecialiseerde laboratorium voor device assessments. Zo gebruiken we reverse engineering en firmware hacking technieken om potentiële kwetsbaarheden te identificeren. Wij testen slimme kantoorsystemen, logistieke en transportsystemen en IoT apparaten in energie, retail of gezondheidszorg.

IoT PENTESTING SERVICES

- **(Enterprise) IoT Assessment:** eevalueert het beveiligingsniveau van de (I)IoT-apparaten en back-end services (klantisolatie, cloudgebaseerd provisioneringssysteem, enz.)
- **(Enterprise) IoT threat modeling:** helpt bij het identificeren van het meest geschikte veilige ontwerp voor apparaten en back-end services
- **Consumer IoT evaluatie en certificering**

INTERNATIONALE NORMEN EN STANDAARDEN

Het is belangrijk dat de diepte en breedte van uw security test eenduidig is. Daarom gebruiken we waar mogelijk internationale normen en standaarden. De standaarden die we gebruiken zijn afhankelijk van het beoordelingsdoel, de te testen omgeving (architectuur, platform, applicatie, et cetera), branche-eisen en regelgeving per land.

De belangrijkste normen die we gebruiken zijn:

- Application Security Validation Standard (ASVS) voor web- en mobiele toepassingen (M-ASVS).
- OWASP Application Security Testing Guide (Gids voor het testen van toepassingsbeveiliging)
- SANS-top 25: de meest voorkomende en gevaarlijkste fouten bij het maken van software
- Sectorgebonden normen zoals PCI-DSS, BIO, DigiD en andere.

HOE WIJ TESTEN: VERSCHILLENDE VORMEN VAN PENTESTING

Security testen kunnen worden onderverdeeld in drie hoofdtypen: black-box, grey-box en crystal-box testen.

Black-box testing simuleert een externe aanvaller zonder voorkennis van het systeem. Het doel is om veel voorkomende kwetsbaarheden te identificeren die een aanvaller kan misbruiken.

Grey-box testing gebruikt credentials om toegangsniveaus en interne kwetsbaarheden te testen. Deze methode is ideaal voor gevoelige datasystemen en is de meest gebruikte testmethode, vaak in combinatie met black-boxtechnieken.

Crystal-box testing gebruikt volledige toegang tot broncode of configuraties, waardoor een meer gedetailleerde analyse van kwetsbaarheden mogelijk is, met name in functies voor beveiliging zoals input validatie en cryptografie.

In de praktijk gebruiken we vaak een combinatie van deze testvormen, om de tijd optimaal te benutten en om huidige TTP's na te bootsen: een cybercrimineel kan immers credentials hebben gekocht van het dark web. Meestal beginnen we met een black-box benadering om te bepalen of we accounts en verdere toegang kunnen verkrijgen en gaan dan verder met het grey-box post-login gedeelte.

WHAT ONZE KLANTEN ZEGGEN

“Het team ging een stap verder”

“We hebben met Secura samengewerkt voor een cruciaal project op het gebied van productbeveiliging. Het hele team was zeer deskundig en enthousiast om het resultaat te leveren. Het team deed ook meer dan we hadden gevraagd en adviseerde ons om in de loop van het project aanpassingen te doen, wat we erg op prijs stelden.”

MEER DAN EEN SCAN: HOE WIJ HOOGWAARDIGE PENTESTING GARANDEREN

Zeer gespecialiseerde testers

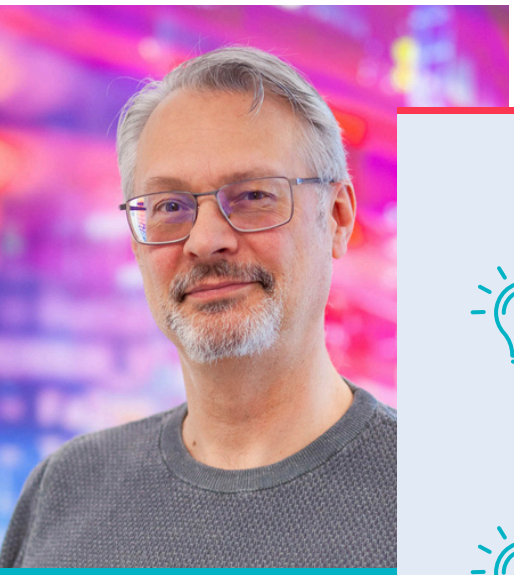
Secura's pentestteam voert elk jaar honderden security tests uit. Alle testers zijn gecertificeerd volgens een minimumstandaard, maar de meeste hebben meerdere certificeringen, zoals OSCP, OVSE, eCPPT, GIAC GPEN. Dit team kan vrijwel elke security test uitvoeren.

Gecertificeerde partner

Secura is geaccrediteerd voor pentesting door CREST en waren het eerste bedrijf dat werd gecertificeerd voor het Nederlandse 'CCV-keurmerk Pentesten'. Ons product security lab is geaccrediteerd door Common Criteria. Secura is een van de weinige bedrijven die door de Nederlandse overheid is geaccrediteerd voor BSPA (Baseline Security Product Assessment).

Kwaliteitsproces

Zelfs als we geen ernstige bevindingen doen, kunt u met ons onderzoeksrapport laten controleren en bevestigen dat alle tests correct zijn uitgevoerd en de testresultaten correct zijn geïnterpreteerd. Ons vier-ogen-principe betekent dat elk rapport door ten minste twee ervaren testers wordt bekeken.



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 CASES | PENTESTING DIENSTEN

Voor een grote online retailer voerde Secura een grey-box applicatietest uit. Wij kwamen erachter dat de content van de website te manipuleren was, op zo'n manier dat sitebezoekers er last van zouden hebben. Daarnaast konden we de betalings-API laten geloven dat er voor artikelen was betaald terwijl dat niet zo was, wat leidde tot een mogelijk fraudescenario. De klant kon deze problemen oplossen terwijl wij nog aan het testen waren.

Voor een internationaal hightechbedrijf voerde Secura een interne penetratietest uit van hun wereldwijde netwerk. Dit leidde tot een volledige compromittering van het Windows-domein, terwijl er al veel mitigerende maatregelen waren genomen. De overige risico's werden vervolgens aangepakt in een verbeterplan. Daarnaast maakten wij SIEM use-cases zodat toekomstige exploits van deze issues zouden worden gedetecteerd.

BUREAU VERITAS 1828

MEER WETEN?

Neem vandaag contact op om uw weerbaarheid te verhogen.

info@secura.com
+31 (0) 88 888 3100
secura.com