



BEVEILIGINGSANALYSE KIEZEN

Een vergelijkingsdocument

Datum

augustus 2026

Aantal pagina's

4

Hulpmiddel: de juiste beveiligingsanalyse kiezen

Wereldwijd worden de digitale dreigingen steeds geavanceerder. Het is daarom van groot belang om je cloudomgeving, apparaten, identiteiten, data en applicaties te voorzien van goede beveiliging. Zo kan iedere medewerker altijd en overal veilig werken.

Hiervoor moet je wel weten waar de kwetsbaarheden in je omgeving zitten. Een beveiligingsanalyse ondersteunt hierbij! Wanneer je overzicht creëert in het huidige beveiligingsniveau van de (online) omgeving, weet je op welke punten je deze kunt verbeteren en welke gerichte maatregelen je kunt treffen. Zo krijg je meer grip op potentiële risico's en til je je (online) beveiliging naar een hoger niveau. Lees meer over het [belang van een beveiligingsanalyse](#).

Verschillende soorten beveiligingsanalyses

- **Kwetsbaarheidsscan:** een automatische analyse over je systemen heen. De scan geeft een algemeen beeld over hoe de IT-beveiliging is geregeld. Algemene kwetsbaarheden zoals veel voorkomende configuratiefouten worden opgespoord en per zwakke plek worden er technische risico-inschattingen gemaakt. De resultaten helpen je om concrete verbetermaatregelen te prioriteren en de digitale weerbaarheid stap voor stap te verhogen.
- **Pentest:** doet bovengenoemde zaken ook, maar geeft een meer gedetailleerd beeld met aandacht voor potentiële kwetsbaarheden. Bij een pentest gaat een ethische hacker zelf op zoek naar kwetsbaarheden in je (web)applicaties, website, IT-infrastructuur, API-koppelingen en mobiele apps.
- **Audit:** een toetsing op basis van een vragenlijst, checklist of gesprekken.
- **Cybercrisis-training:** een training waarin medewerkers oefenen met het herkennen van en handelen bij een cybercrisis.

Daarnaast kun je ervoor kiezen om medewerkers bewust te maken van risico's die ontstaan door hun dagelijkse handelingen. Denk hierbij aan een training of gesimuleerde [phishingaanval](#).

Een oplossing kiezen die past bij je eigen beveiligingsbeleid

Denk eerst na over je wensen, zoals:

- Welke omgeving wil je controleren?
- Hoe vaak wil je deze omgeving controleren?
- Tot welk niveau wil je gaan?
- Wil je medewerkers ook bewustmaken van hun eigen handelingen?
- Bekijk ook [deze vragen](#).

Dit document is een hulpmiddel om een dienst te kiezen. Op de volgende pagina's vergelijken we verschillende oplossingen voor beveiligingsanalyses: MyDigitals Pentest, AvePoint Policies & Insights, SoyCloud en Edufort en de Microsoft 365 APK van APS IT-diensten.

Meer informatie of behoefte aan advies?

Neem bij vragen of voor advies gerust contact op met onze schooladviseur Charles Hunfeld via c.hunfeld@apsitdiensten.nl of 030 - 285 68 21. Hij staat klaar om je te helpen!

Vergelijking oplossingen voor beveiligingsanalyse

	<u>MyDigitals Pentest</u>	<u>AvePoint Policies & Insights</u>	<u>SoyCloud Security audits en pentesting</u>	<u>Edufort Cybersecurity</u>
Manier waarop de risico's en kwetsbaarheden worden getoetst				
Audit: toetsing op basis van vragenlijst, checklist en/of gesprekken	X		X	X
Pentest: legale (ethische) hackers doen onderzoek	X		X	X
Kwetsbaarheidsscan: analyse over systemen heen	X		X	X
Van welke onderdelen worden de risico's in kaart gebracht?				
Identiteiten: (toegangs)rechten en autorisatie	X	X	X	X
Apparaten/werkplekken	X		X	X
Lokale systemen en netwerken zoals servers en het lokale netwerk	X			
Microsoft 365-omgeving	X	X	X	X
Google-omgeving			X	X
Website	X		X	X
Webtoepassingen			X	X
API's			X	X
IP-adressen			X	X

Vervolgacties bij medewerkers en gedrag <u>Let op:</u> dit zijn optionele diensten die je tegen meerprijs kunt afnemen.				
Training/advies om medewerkers bewust te maken van risico's <i>Bijvoorbeeld: welke externe (web)applicaties gebruiken medewerkers?</i>	X		Mogelijk via externe partner	
OSINT: een techniek om online sporen die op het eerste gezicht verstopt lijken, boven te halen	X		Mogelijk via externe partner	X
Phishing-aanval simuleren bij medewerkers om bewustwording te controleren	X		Mogelijk via externe partner	X
Licentiemodel				
Aantal scans of assessments		Continu	Op basis van aantal mailboxen/ IP-adressen	Dagelijks/ wekelijks
Adviesgesprek			Na resultaten van pentesten	X
Rapportage met samenvatting en aanbevelingen	X	X	X	X
Taal bij toetsingen en/of gesprekken	NL	NL	NL	NL, tool zelf ook NL

Aanvullende diensten:

APS IT-diensten Microsoft 365 APK

De Microsoft 365 APK biedt een gerichte beoordeling van de inrichting en beveiliging van de Microsoft 365-omgeving, waarbij de focus ligt op configuratie, beheer en beveiligingsinstellingen. Tijdens een gezamenlijke werksessie controleert een consultant belangrijke onderdelen zoals identiteitsbeheer, toegangsrechten, e-mailbeveiliging, SharePoint, Teams en Microsoft Defender. De school ontvangt een overzicht met concrete verbeterpunten, adviezen en eventuele direct doorgevoerde instellingen. Daarmee helpt de APK scholen en besturen om beveiligingsrisico's te verkleinen, grip te krijgen op hun Microsoft 365-omgeving en deze volgens actuele beveiligingsrichtlijnen in te richten.

Cybercrisis-training

CCRC is een aanvullende training om organisaties beter voor te bereiden op een cybercrisis. De training gaat breder dan IT-incidenten alleen en besteedt ook aandacht aan communicatie, besluitvorming, rolverdeling, escalatie en continuïteit van onderwijs en bedrijfsvoering. Daarmee helpt de training scholen en besturen om bewuster en gestructureerder te handelen bij digitale verstoringen of crisissituaties.

Edufort AI

Edufort AI is een preventieve beveiligingsoplossing die medewerkers ondersteunt bij veilig gebruik van AI-tools, e-mail en online applicaties. De oplossing voorkomt datalekken en risicovolle handelingen op het moment dat deze plaatsvinden en vormt daarmee een aanvulling op technische beveiligingsanalyses.

Microsoft 365 dashboards en secure score

Microsoft biedt verschillende [vulnerability dashboards](#) aan waarin je zelf actief analyses kunt zien en kwetsbaarheden binnen de omgeving ontdekt. Vervolgens kun je hier actie op ondernemen. Daarnaast heb je de [Secure Score](#): deze geeft aan hoe hoog jullie tenant scoort op beveiliging. Je krijgt direct handige tips om de score te verhogen. [Microsoft Sentinel](#) is ook een mooie oplossing waarmee je een goed overzicht krijgt van de beveiligingsrisico's. De applicatie maakt hier geavanceerde analyses van en neemt je complete infrastructuur hierin mee.

Via Microsoft kun je dus zelf de analyses uitvoeren en inzien. In de vergelijking staan juist analyses die door een externe partij worden uitgevoerd. De verschillende [Microsoft Defender producten](#) kun je vervolgens inzetten om bepaalde risico's te verkleinen.

Disclaimer

De vergelijking tussen deze oplossingen is op hoofdlijnen uitgevoerd. Het is een hulpmiddel bij het maken van een keuze, er kunnen geen rechten aan worden ontleend. Voordat je een keuze maakt, is het daarom belangrijk om als school zelf de productvoorwaarden en -beschrijvingen van de leverancier goed door te nemen. Dat geldt ook voor de andere licentievoorwaarden.