

A vertical white banner hanging from a pole on the left side of the building. It features the actabyte logo at the top, followed by the word 'actabyte' in large orange letters, and 'business it' in smaller black letters below it.

ACTABYTE PENTEST AS A SERVICE

EVALUEER JE
CYBERSECURITY
VOORDAT
CYBER
CRIMINELEN DAT
DOEN!



WIJ LEVEN NU IN EEN DIGITALE ECONOMIE

56% VAN AL HET
INTERNETVERKEER IS
CRIMINEEL VAN AARD.

EEN TIJDPERK MET STIJGENDE DATA LEKKEN

2005

157

datalekken

66,9 miljoen

records

blootgesteld

2022

11.476


datalekken

1,66 miljard

records

blootgesteld

Bron: <https://www.idtheftcenter.org/data-breaches/>



61% van kleine en middelgrote bedrijven worden jaarlijks slachtoffer van een cyberaanval. De gemiddelde kosten van een cyberaanval zijn **gestegen tot 4,5 miljoen euro**. Hierdoor is het voor bedrijven extreem moeilijk om te herstellen.

Hoe ontstaan datalekken?

Een datalek vindt plaats wanneer een cybercrimineel een gegevensbron infiltreert en vertrouwelijke informatie buit maakt. Dit kan worden gedaan door toegang te krijgen tot een computer of netwerk om lokale bestanden te stelen of door de netwerkbeveiliging op afstand te omzeilen. De meest voorkomende cyberaanvallen die worden gebruikt bij datalekken worden hieronder beschreven.



RANSOMWARE



MALWARE



PHISHING



DENIAL OF SERVICE (DOS)

De beste verdediging is een goede aanval.



OFFENSIEVE VEILIGHEID

- Vulnerability management
- **Penetratietesten**
- Sociale engineering



DEFENSIEVE BEVEILIGING

- Monitoring & updates
- Beveiligingsbewaking
- Reactie op incidenten

Waarom heeft uw organisatie een penetratietest nodig?

Met penetratietesten kunnen organisaties hun cyberbeveiligingspositie beoordelen op basis van **realistische aanvalsscenario's** , waardoor ze problemen kunnen aanpakken die over het hoofd zouden worden gezien als ze uitsluitend een defensieve aanpak zouden volgen.

**Penetratietesten
brengen cruciale
beveiligingslekken
aan het licht.**



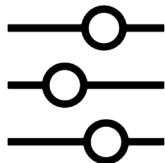
**Ze leggen problemen
bloot die buiten het
bereik van
vulnerability
management vallen.**

Penetratietesten werken

Penetratietesten zijn duidelijk effectief bij het blootleggen van manieren waarop kwaadwillenden uw netwerk kunnen binnendringen en door uw netwerk kunnen bewegen voor:



TOEGANG



MANIPULEREN



SCHADE



VERKOPEN

van waardevolle data en systemen binnen uw organisatie. Alleen focussen op defensieve beveiliging, zoals veel bedrijven doen, is een fundamenteel gebrekkige strategie.



Penetratietesten en het doel ervan

- 01** **Blotleggen van aanwezige risico's** door simulatie van een kwaadaardige cyber aanval
- 02** **Evalueer de huidige** veiligheid detectie- en bewakingscontroles
- 03** **Bied bedrijven** herstelstrategieën om risico's te beperken
- 04** **Begrijp hoe aanvallers zich richten** op de meest vertrouwelijke/gevoelige gegevens

Penetratietesten zijn elke cent waard

Met behulp van de resultaten van een penetratietest kan uw organisatie manieren identificeren om **uw meest waardevolle gegevens te beschermen** door het aantal aanvalsvectoren en toegankelijke paden naar gevoelige bronnen en systemen te verminderen.



Begin 2024 telde Nederland ruim 1,56 miljoen mkb-bedrijven. Het grootste deel hiervan bestaat uit zzp'ers (zelfstandigen zonder personeel), namelijk ruim 1,25 miljoen.

Veel van die bedrijven heeft minder dan 20 werknemers en kan het zich simpelweg niet veroorloven om €5000,- of meer uit te geven aan een jaarlijkse penetratietest.

Daar komen wij om de hoek kijken!

Wij maken penetratietesten **BETAALBAAR**

Wij maken gebruik van de **nieuwste technologie** waarmee ons team penetratietesten efficiënter kan uitvoeren. Deze besparingen realiseren we door u pentesten aan te bieden tegen een betaalbare prijs.

Meer penetratietesten **zonder veel geld uit te geven!**



Wij maken penetratietesten **WAARDEVOLLER**

E-mail- en sms- **meldingen** om op de hoogte te blijven tijdens de penetratietest.

Realtime volgen van aanvallen en bevindingen.

Rapporten zijn binnen 24 uur beschikbaar nadat een penetratietest is voltooid.



Wij maken penetratietesten

REGELMATIGER

Ga verder dan compliance en voldoe aan de beste praktijken in de sector.

Voer een penetratietest uit **wanneer en hoe vaak** u maar wilt.

Blijf op de hoogte in plaats van te hopen op het beste.

