



**U weet niet of uw vitale bedrijfsapplicaties en IT-systemen bestand zijn tegen hackers of andere kwaadwilligen? Tast u wat betreft veiligheid in het duister? Dan biedt onze *Penetratietest Informatiesystemen (PTI)* uitkomst. Deze 'ethische hack' kan op maat plaatsvinden en geeft antwoorden op uw twijfels en vraagtekens.**

## DE HAMVRAAG ...

“Kan een kwaadwillige vanaf waar dan ook onze systemen overheersen, of zit alles goed dicht? Hoe is het gesteld met veiligheid van bedrijfsapplicaties en IT-systemen?”. Deze en meer vragen staan centraal in het LBVD-dienstproduct *Penetratietest Informatiesystemen*:

- ◆ Zijn onze vitale systemen goed beschermd ('hacker-proof')? Ook intern?
- ◆ Is ongeautoriseerde toegang of misbruik van toegekende rechten mogelijk?
- ◆ Zijn systemen 'gezond' geconfigureerd en voorzien van de laatste security patches?
- ◆ Merkt de organisatie inbraakpogingen op? Zo ja, reageert ze adequaat?

Toetsing is belangrijk. Werkt het? De organisatie loopt onnodig risico wanneer ze niet op de hoogte is van gaten in de beveiliging. Je wilt niet dat kwaadwilligen door tekortkomingen bedrijfskritische webapplicaties of databaseservers kunnen saboteren, vertrouwelijke informatie kunnen inzien of vitale bedrijfsinformatie kunnen wijzigen.

## HET ANTWOORD ...

Via het uitvoeren van een gecontroleerde aanval op een wijze waarop een 'echte' aanvaller dat ook zou doen, brengen de specialisten van LBVD kwetsbaarheden en zwakke plekken grondig en diepgaand in kaart. Zij gaan daarbij gestructureerd te werk, met OSSTMM en ESCA/LPT als leidraad. Onderdelen die LBVD uitvoert zijn onder meer:

- ◆ Afkadering en verdere voorbereiding
- ◆ Informatievergaring
- ◆ Kwetsbaarhedenanalyse en het feitelijke testen
- ◆ Analyse, rapportage en presentatie

LBVD kan het onderzoek in een kort tijdsbestek uitvoeren, waardoor de status van de geteste systemen snel inzichtelijk is voor de organisatie. Verschillende varianten zijn mogelijk, afhankelijk van het perspectief van waaruit u wilt dat LBVD test: vanaf internet of het interne netwerk, bedraad of draadloos, blackbox, greybox of crystalbox, intrusief of niet, et cetera. Ook een combinatie met het LBVD-dienstproduct *MysteryGuest* behoort tot de mogelijkheden.

## HET RESULTAAT ...

Via analyse en interpretatie werken de (gecertificeerde) ethische hackers van LBVD de verkregen bevindingen en statusinformatie uit tot een helder en leesbaar statusrapport, compleet met conclusies én aanbevelingen. Daarnaast is voorzien in een terugkoppelsessie met de opdrachtgever.

Met de verkregen inzichten kan de organisatie bewuster omgaan met risico's en werken aan structurele verbetering van de beveiliging van haar vitale informatiesystemen. Het onderzoek leent zich uitstekend als nul-meting. In die hoedanigheid zijn de resultaten bijvoorbeeld zeer bruikbaar als startpunt van een verbetertraject.

### LBVD HELPT!

LBVD BESCHIKT OVER DE KENNIS,  
ERVARING EN MIDDELEN OM  
PENETRATIE-TESTEN IN UITEENLOPENDE  
VARIANTEN TE VERZORGEN

PENETRATIE-TESTEN VERGT EEN  
GESTRUCTUREERDE AANPAK MET ALS  
BASIS DOORONTWIKKELDE  
TESTMETHODES

### LBVD HELPT!

VAN DIT PRODUCT IS TEVENS EEN  
UITGEBREIDE DIENSTBESCHRIJVING  
VOORHANDEN.  
ONZE SALES IHELPT U GRAAG.