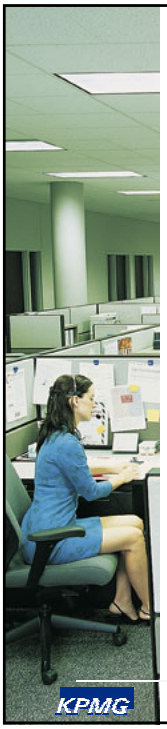

KPMG
INFIORMATION RISK MANAGEMENT
Testen van security
Securityrisico's in hedendaagse systemen
TestNet - 5 april 2006
ADVISORY
AUDIT • TAX • ADVISORY


Visie van KPMG
Organisaties willen aantoonbaar 'in control' zijn over hun interne processen. Niet alleen omdat regelgeving daarom vraagt, maar ook omdat ze daaraan zelf behoefte hebben.
Dit ambitieniveau vraagt om een adequaat ontwerp en implementatie van ICT, evenals controle op naleving van de eisen die aan de ICT worden gesteld. Bijvoorbeeld gebruik van en controle op naleving van baselines; het inregelen, de analyse en opvolging van logging; security scanning en testing.
In onze visie moet het ambitieniveau voor belangrijke ICT-objecten en -processen aantoonbaar 'in control' zijn.
Op basis van het groeimodel kan een organisatie haar eigen ontwikkelstadium en ambitieniveau bepalen.
Proactief
Aantoonbaar
Basis
Individueel
Ad hoc
Geoptimaliseerd
Beheerst en meetbaar
Gedefinieerde processen
Herhaalbare processen
Initieel
Toenemende monitoring inspanning
Cobit Maturity Level
KPMG
© 2006 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie. Alle rechten voorbehouden.
2



Visie van KPMG

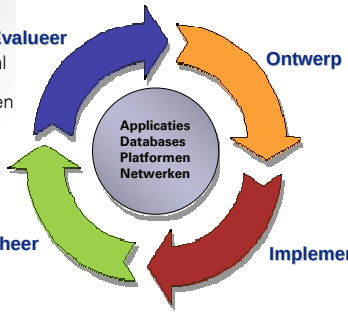
Een organisatie doorloopt voor het borgen van beveiliging de cyclus van Ontwerp, Implementatie, Beheer en Evalueer. Hierbij onderneemt een organisatie doorgaans de volgende activiteiten:

SECURITY COMPLIANCE

- Voer regelmatig beoordelingen uit van de effectiviteit van bestaande maatregelen
- Identificeer en bepaal prioriteit van bestaande zwakheden
- Documenteer verbeterplannen

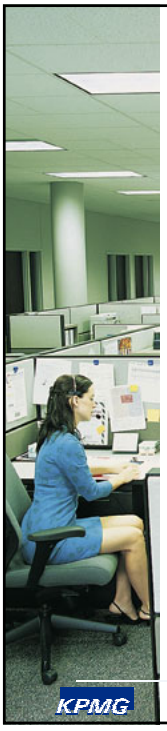
SECURITY TESTING

- Test de ICT-infrastructuur
- Voer trendanalyses uit en bepaal de ontwikkeling van het risicoprofiel



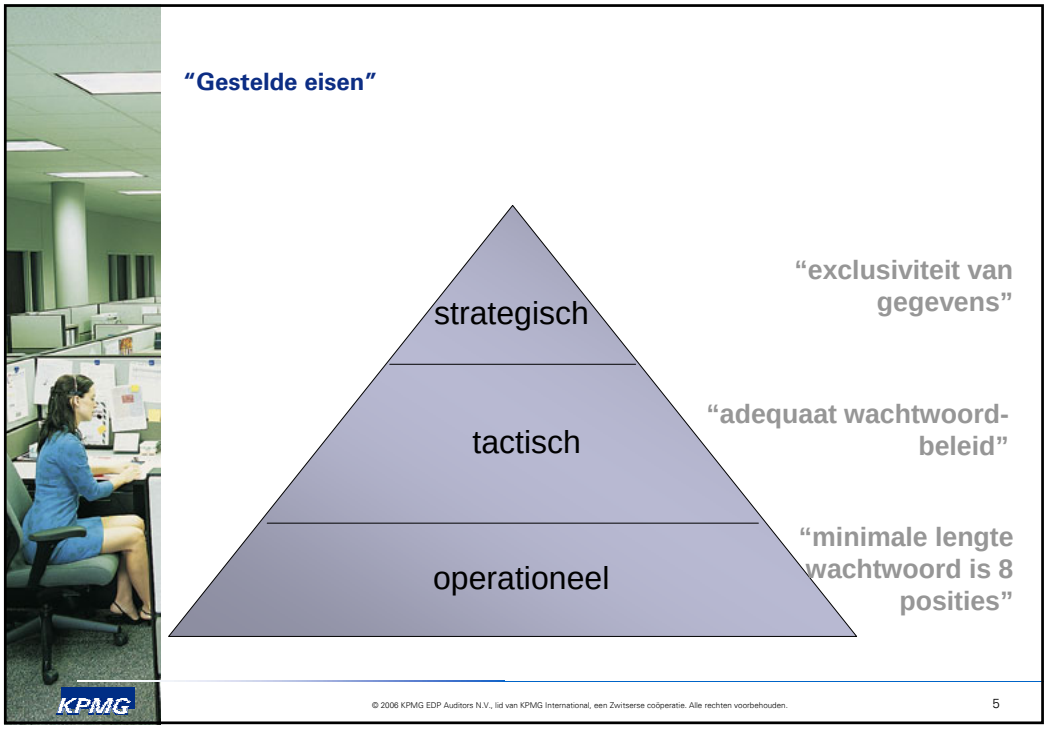
SECURITY ADVIES

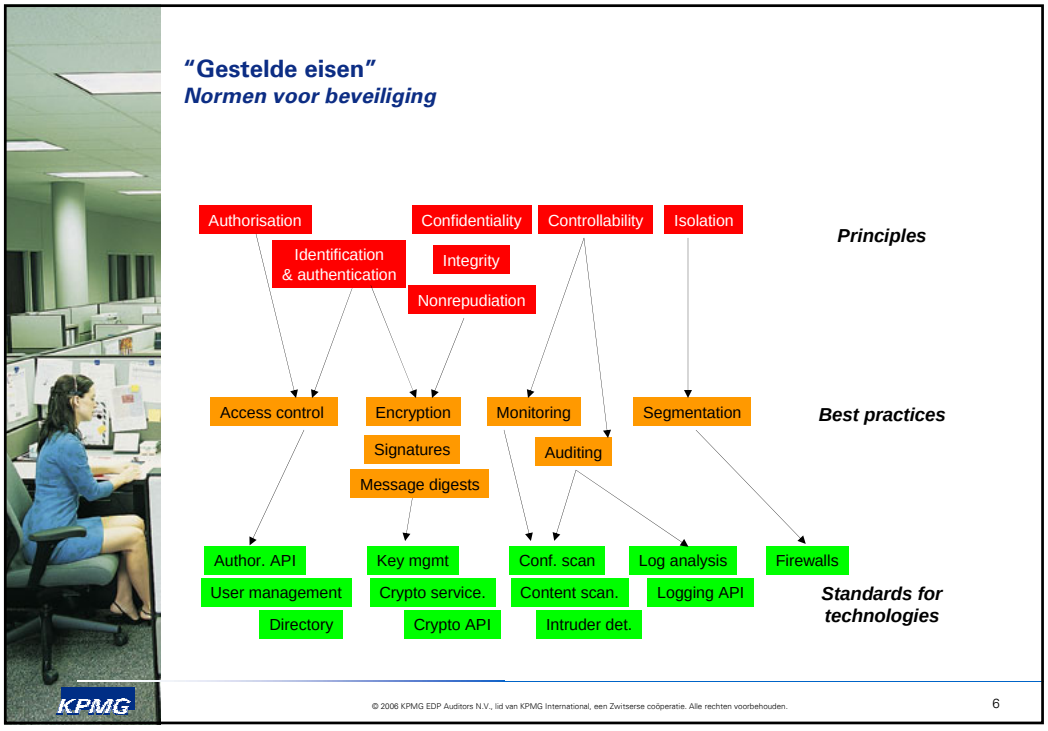
- Ontwerp en implementeer beveiligingsmaatregelen om de bedrijfsprocessen te beschermen
- Tref maatregelen in lijn met wet- en regelgeving
- Implementeer maatregelen op kosteneffectieve wijze
- Gebruik efficiënte technieken

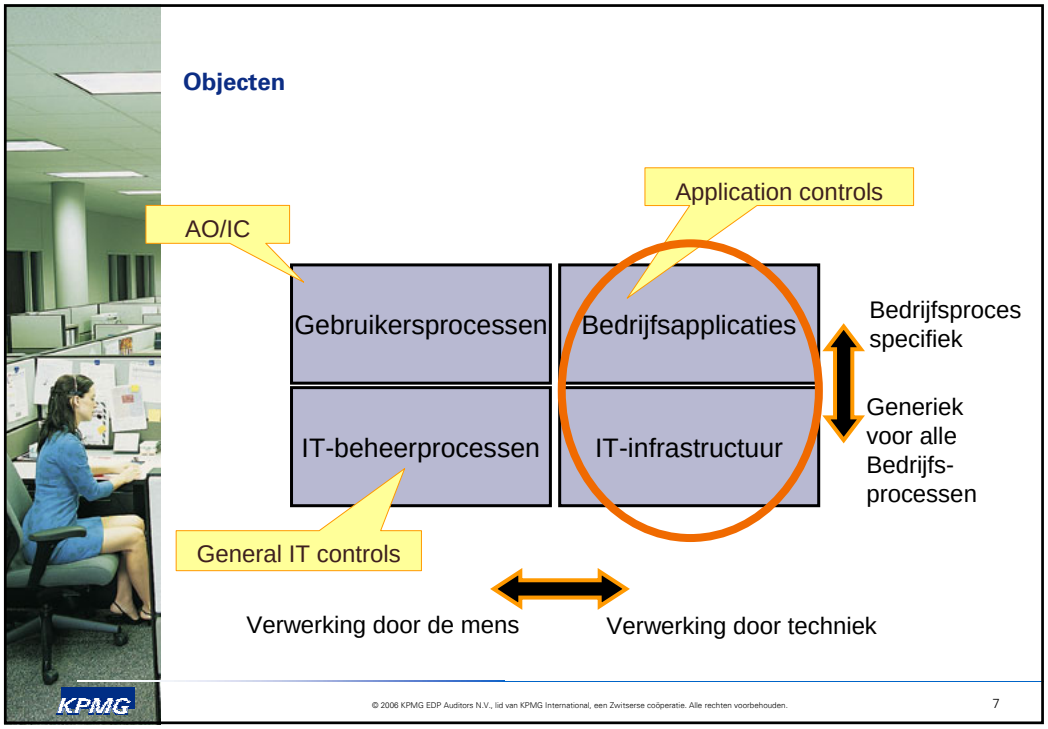


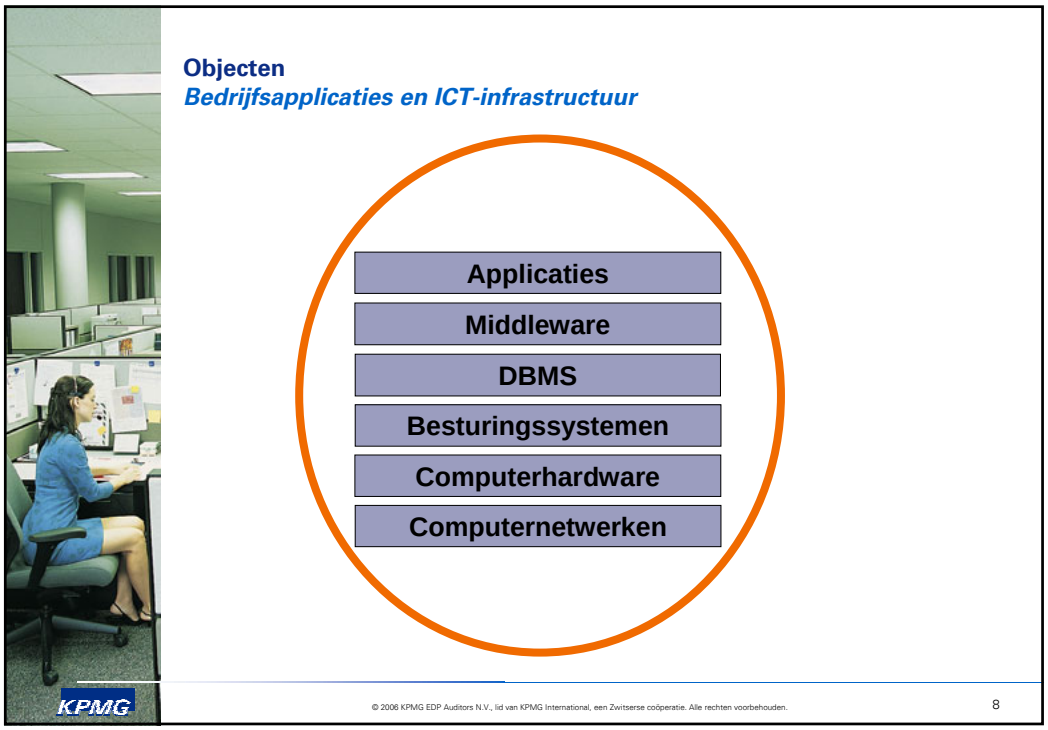
Zekerheid ...

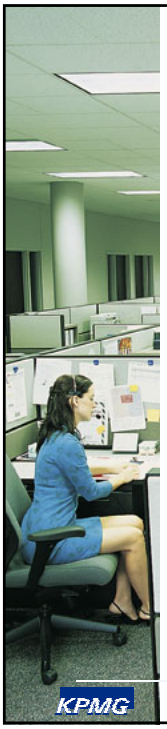
Service	Mate van zekerheid	Uitspraak
e.g. Penetratietest	Comfort	Rapportage van bevindingen
Review	Beperkte zekerheid	Negative assurance Het is KPMG niet object X niet voldoet aan gestelde eisen
Audit	Redelijke mate van zekerheid	Positive assurance Object X voldoet aan de daaraan gestelde eisen


"Gestelde eisen"
strategisch
tactisch
operationeel
"exclusiviteit van gegevens"
"adequaat wachtwoord-beleid"
"minimale lengte wachtwoord is 8 posities"
KPMG
© 2006 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie. Alle rechten voorbehouden.
5

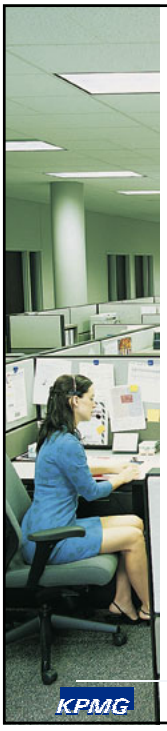

"Gestelde eisen"
Normen voor beveiliging
Authorisation
Confidentiality
Controllability
Isolation
Identification & authentication
Integrity
Nonrepudiation
Principles
Access control
Encryption
Monitoring
Segmentation
Signatures
Auditing
Message digests
Best practices
Author. API
Key mgmt
Conf. scan
Log analysis
Firewalls
User management
Crypto service.
Content scan.
Logging API
Directory
Crypto API
Intruder det.
Standards for technologies
KPMG
© 2006 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie. Alle rechten voorbehouden.
6


Objecten
Application controls
AO/IC
Gebruikersprocessen
Bedrijfsapplicaties
Bedrijfsproces specifiek
IT-beheerprocessen
IT-infrastructuur
Generiek voor alle Bedrijfs-processen
General IT controls
Verwerking door de mens
Verwerking door techniek
KPMG
© 2006 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie. Alle rechten voorbehouden.
7


Objecten
Bedrijfsapplicaties en ICT-infrastructuur
Applicaties
Middleware
DBMS
Besturingssystemen
Computerhardware
Computernetwerken
KPMG
© 2006 KPMG EDP Auditors N.V., lid van KPMG International, een Zwitserse coöperatie. Alle rechten voorbehouden.
8



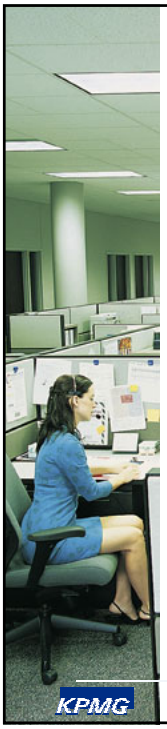
Security testing – een klassiek probleem



Security testing

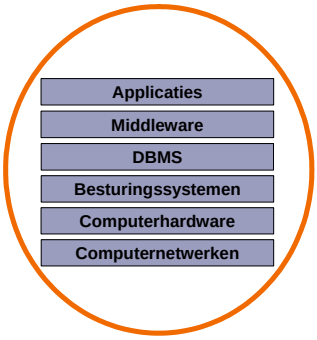
- Controle van gewenst aanwezige maatregelen (**slagboom**)
- Controle van aanwezigheid alternatieve routes (**alleen via slagboom**)

“Alleen toegang voor bevoegd personeel”

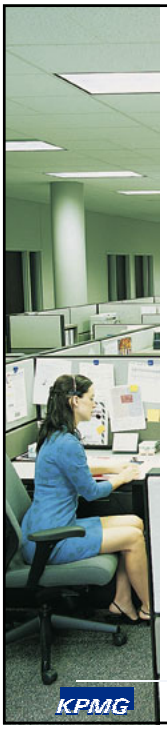


Security testing
Het vergiet in ontwikkeling …

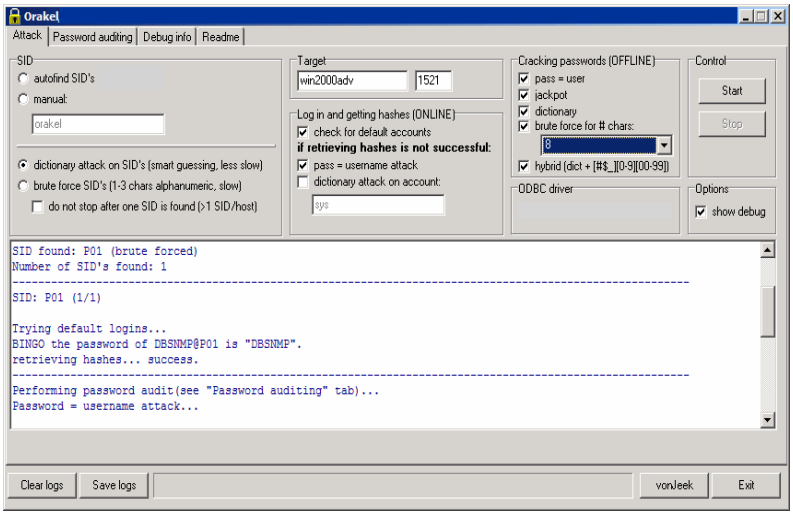
- Webapplicaties
- Databases
  - Authenticatie
- Besturingssystemen
  - Patching
- Bedrijfsnetwerken
  - Externe netwerkkoppelingen
  - Draadloze netwerken



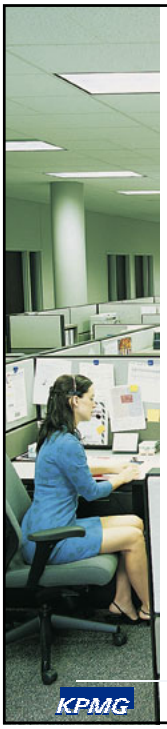
KPMG



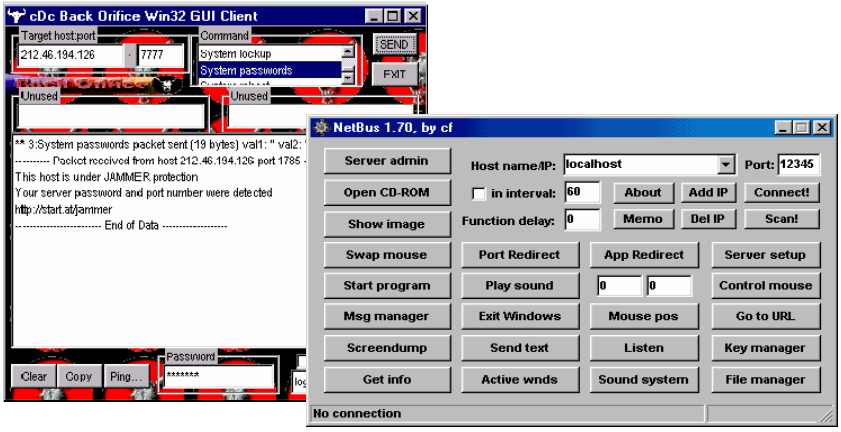
Security testing
Databases

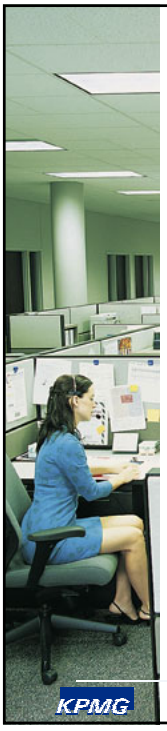


KPMG



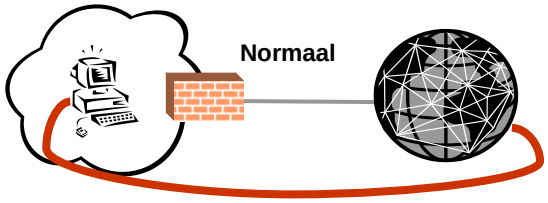
Security testing
Besturingssystemen

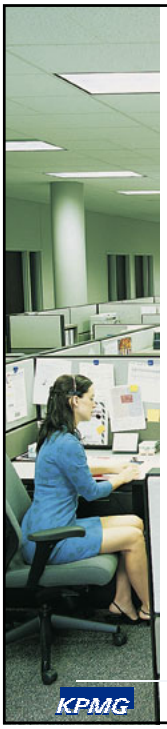




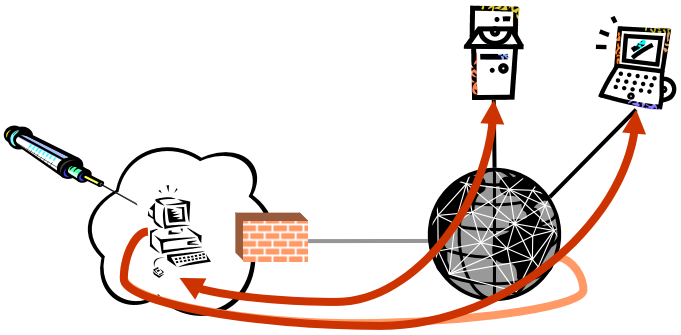
Security testing
Externe netwerkkoppelingen

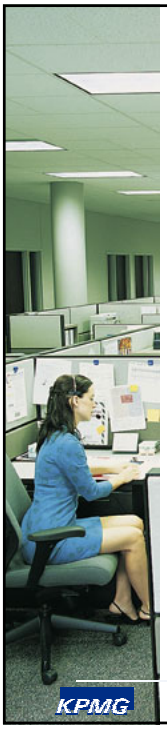
Extrusion Detection met CHILLI



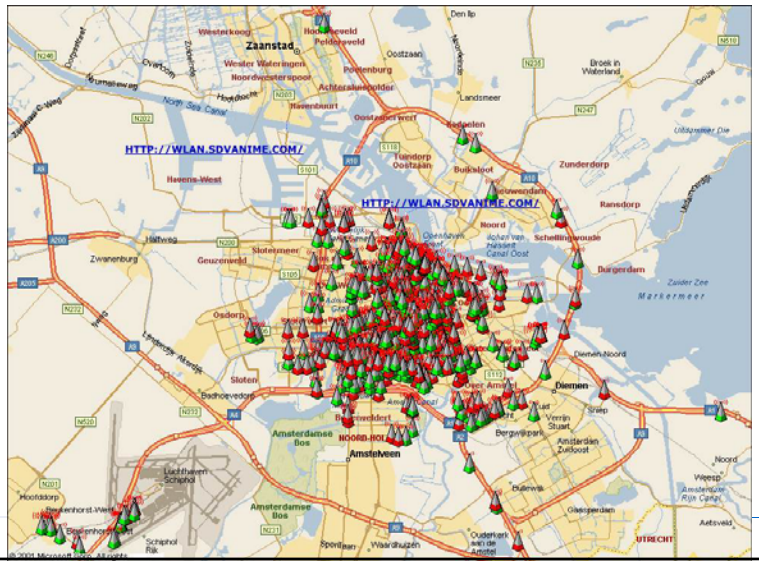


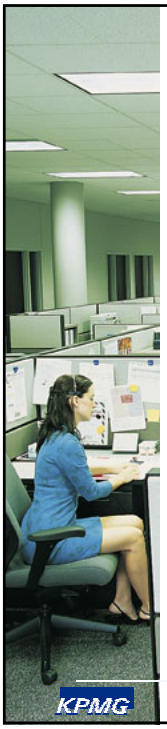
Security testing
Externe netwerkkoppelingen



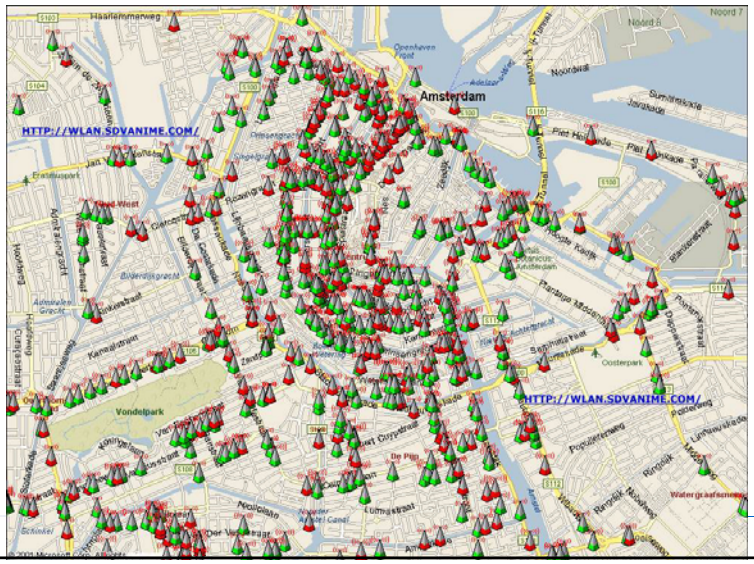


Security testing
Draadloze netwerken



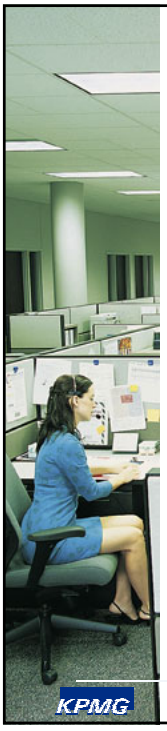


Security testing
Draadloze netwerken



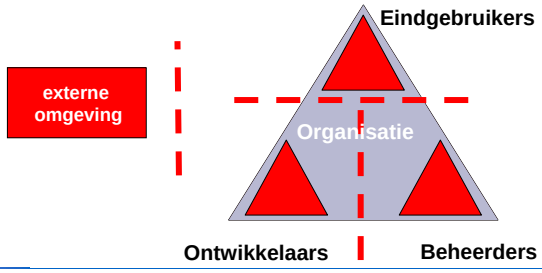
KPMG

17



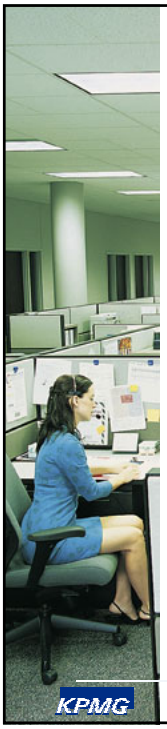
Security testing
Doel

- Een van de meest overtuigende manieren voor bedrijven om de kwetsbaarheid voor aanvallen in te schatten en zich ertegen te verdedigen, is het inzetten van ervaren hackers die proberen in te breken in de bedrijfssystemen.
- Met penetratietesten vindt controle van feitelijk gerealiseerde functiescheidingen plaats



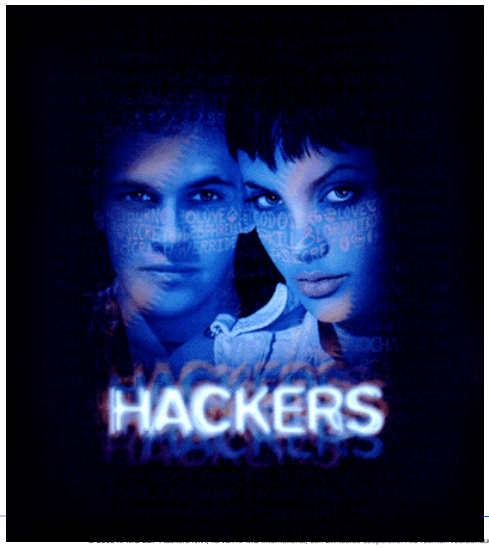
KPMG

18

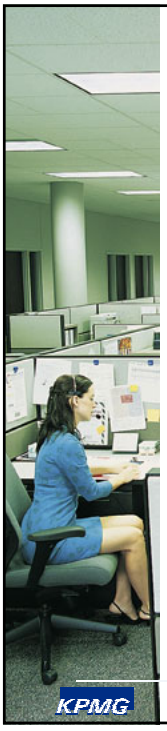


Security testing

Tegen welke bedreigingen ?



KPMG

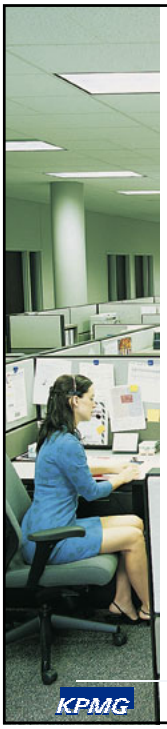


Security testing

Fasering van testen

- **Map**
  - Welke koppelingen heeft een netwerk?
  - Welke systemen en componenten bevinden zich in het netwerk?
  - Welke netwerkservices zijn actief op de aanwezige systemen?
- **Scan**
  - Welke systemen en netwerkservices presenteren mogelijke zwakheden?
    - 'Black box' – verkenning van systemen en benaderbare applicaties met mogelijk aanwezige zwakheden als gevolg van bekende bugs.
    - Zonder menselijke intelligentie, gebruik van uitsluitend standaardhulpmiddelen, resulterend in technische bevindingen.
- **Test**
  - Welke systemen en netwerkservices kunnen naar succesvol worden aangevallen?
    - 'Black', 'grey' of 'white box' – gedetailleerde (handmatige) uitnutting van aangetroffen (mogelijke) zwakheden.
    - Gebruik van menselijke intelligentie gecombineerd met hulpmiddelen, misbruik van aangetroffen zwakheden, resulterend in bevindingen op strategisch, tactisch en operationeel niveau.

KPMG



Security Compliance Monitoring

Security Mapping, Scanning & Testing Model

Mapping

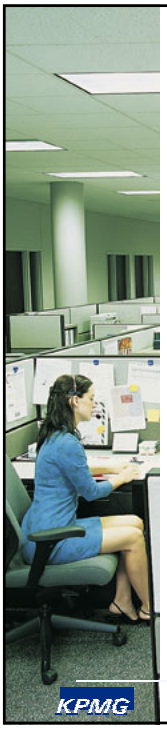
Quarterly Intrusive Testing
- *Verify vulnerabilities*
- *Imitate Advanced "Hacker" Activity*
- *Manual Techniques*

Ongoing Monitoring & Assessment
- *Respond to alerts*
- *Correct identified vulnerabilities*
- *Design mitigating controls*

Frequent Non-intrusive Scanning
- *Port & Service Scanning*
- *Identify known vulnerabilities*
- *Identify missed security patches*
- *Automated Testing*

Reporting

KPMG

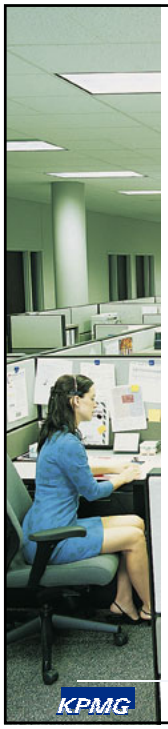


Security testing

Selectie van objecten

- **Infrastructuurtest**
  - Interne netwerk (test van binnenuit)
  - Externe netwerk (test van buitenaf)
    - Internet
    - Inbellen & modem
    - Draadloze netwerken
- **Applicatietest**
  - Met behulp van applicatietesten kunnen zwakheden in (aangepaste) software, met name met betrekking tot de beveiliging, worden geïdentificeerd
  - Zowel traditionele als op webservices gebaseerde software kan worden getest
  - Op basis van applicatietesten kunnen verbetermogelijkheden worden vastgesteld, zoals documentatie en programmeerkwaliteit (sourcecode)

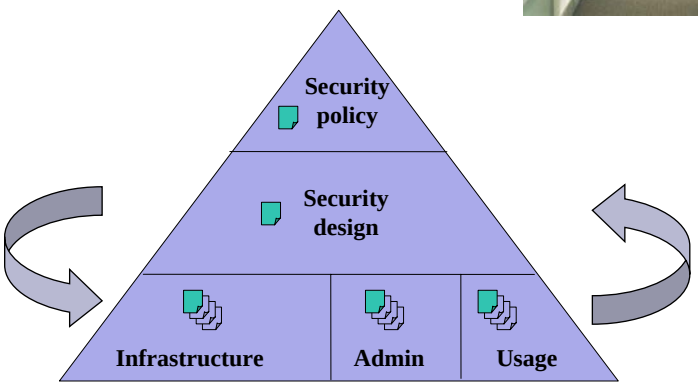
KPMG

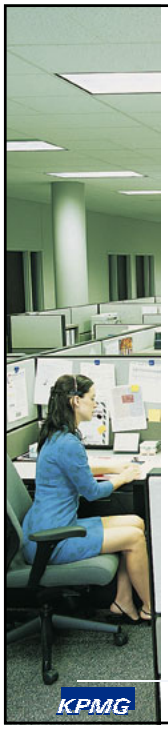


Security testing

Deduceer oorzaken …

Security testing ondersteunt de controle van security management capabilities





Structureren van testen

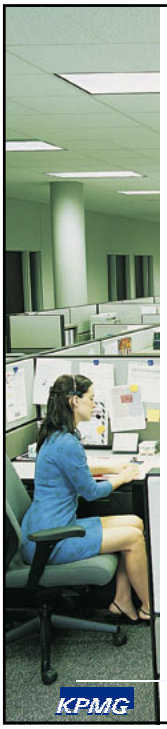
Determine Security testing principles

Vaststellen gewenste kwaliteit van testen
- Comfort – Negative en Positive assurance

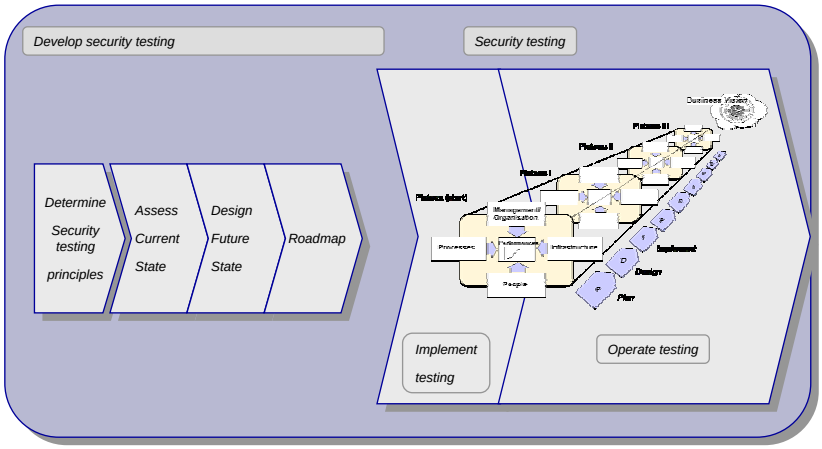
Selecteren objecten
- Samenhang AO/IC – Applicatie – ICT – Beheer

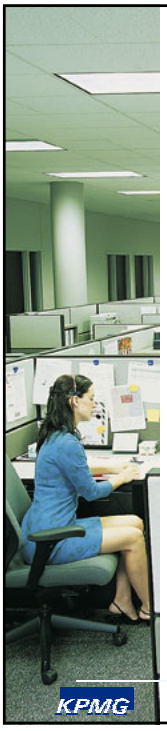
Bepalen te stellen eisen
- Gevraagd (e.g. project)
- Ongevraagd (beleid)

Vaststellen wijze van testen
- Handmatige en automatische controle
- Regelmaat van testen



Structureren van testen





Wilt u meer informatie?

KPMG Information Risk Management
Postbus 74105
1070 BC Amsterdam
www.kpmg.nl/irm

Ir. P. (Peter) Kornelisse RE CISA
tel. +31 (0)20 656 8035
fax +31 (0)20 656 8083
e-mail kornelisse.peter@kpmg.nl