

# Penetrationstest – din vished for sikkerhed\*



*Mangel på it-sikkerhed kan have katastrofale konsekvenser for en virksomhed. Mistede data, afsløring af fortrolige oplysninger, midlertidig nedlukning af funktioner og et efterfølgende imagetab er blot nogle af de negative følger, som ubudne gæster i dit it-system kan medføre.*

## Hvad er udfordringen?

I dag er virksomheder dybt afhængige af deres it-infrastruktur. Den er central i forbindelse med afvikling af forretningskritiske processer og er i sagens natur kompleks for at imødekomme kravet til at lade kunderne selvbetjene egne oplysninger. Det er derfor meget vigtigt for virksomhederne at sikre deres it-infrastruktur ved løbende sikkerhedscheck.

## Hvad kan PricewaterhouseCoopers gøre for dig?

PricewaterhouseCoopers har udviklet metoder og værktøjer til systematisk opsporing af sikkerhedssvagheder. Metoderne har været anvendt globalt i PricewaterhouseCoopers samt på nogle af de største danske organisationer med succes på alle typer af systemer, fra de mindste standalone-maskiner til mainframe-systemer.

## Om PricewaterhouseCoopers' metode for penetrationstest

Vores tilgang til penetrationstests er niveauopdelt og baseret på omfanget af dit sikkerhedsprojekt.

Ved større udviklingsprojekter eller implementering af nye systemer kan sikkerhedsprocessen typisk være kompleks eller uoverskuelig. Hertil skræddersyr PricewaterhouseCoopers en projektorienteret sikkerhedstest, der tager højde for trusselsanalyse, systemsvagheder m.m. i hele projektet. Dette test-scenarie inkluderer en traditionel penetrationstest.

Den traditionelle penetrationstest udføres typisk på enkelte systemer, der allerede er i drift. Den udføres regelmæssigt, for at sikre en kontinuerlig opdatering af sikkerhedsniveauet.

På de næste sider præsenteres PricewaterhouseCoopers' metode for disse to niveauer af sikkerhedstest. På bagsiden fortæller vi om vores programmer for sårbarhedsscanninger, som indgår som standard i alle vore tests, men som også kan benyttes alene.



## Projektorienteret sikkerhedstest – Model 1

Når en virksomhed lancerer et nyt it-system – eksempelvis en webbaseret selvbetjeningservice, en virksomhedsportal eller anden Internet gateway – kan det være en stor udfordring at vurdere alle potentielle trusler.

PricewaterhouseCoopers har gennem en årrække udviklet en metode til systematisk at opspore netop denne type ukendte sikkerhedssvagheder.

Den Projektorienterede sikkerhedstest udarbejdes i et nært samarbejde og dialog med virksomhedens sikkerhedsansvarlige, hvormed vi analyserer, hvilke trusler der findes i forhold til det aktuelle system. På den baggrund identificerer vi alle potentielle angrebepunkter, som ligeledes efterprøves med samme metoder, som kan benyttes af en målrettet angriber eller en industrispion med insider-viden.

### Hvad er udbyttet med en Projektorienteret Sikkerhedstest?

- At sikre en effektiv risikostyring
- At give selve penetrationstesten et risiko- og forretningsbaseret fokus samt at levere et resultat, som kan kombineres med processer for risikostyring og -vurdering

- At sikre, at virksomheden opnår maksimalt udbytte ved at optimere den udførte afprøvning, således at afprøvningens dybde tilpasses risikoen
- At opnå bred dækning af alle relevante systemer, samtidig med at der foretages målrettet detailafprøvning af målesystemer
- At give en årsagsanalyse af de identificerede svagheder, således at der efterfølgende kan udvikles løsninger/procedurer til afhjælpning af de eventuelle svagheder.

### Projektforløb

- Projektstart med afstemning af forventninger til kommunikation og logistik
- Informationsindsamling, herunder god brancheskik for it-sikkerhed, f.eks. lovgivning og kodeks fra Finansrådet m.v.
- Trusselsanalyse samt opstilling af de scenarier, der skal danne grundlag for testen
- Detailplanlægning af testfremgangsmåde
- Opbygning af undersøgelsesarbejdsprogram
- Gennemgang af brugerflade, html-kode og kildekode med henblik på at afdække svagheder om systemets funktionalitet
  - Potentielle svagheder drøftes med kunden for at identificere, hvorvidt svagheden evt. er elimineret af kompenserende kontroller
- Penetrationstest
- Løbende informationsoverførsel og sparring – således at der er fuld klarhed om identificerede svagheder.

### Model 1





## Løbende Penetrationstest – Model 2

Når systemerne er i drift, fordrer kompleksiteten i virksomhedens it-infrastruktur, at der udføres en regelmæssig afdækning af de trusler, der kan påvirke sikkerheden.

Løbende penetrationstest fra PricewaterhouseCoopers giver viden om det aktuelle sikkerhedsniveau på de testede enheder, hvad enten det er internet-tilgængelige systemer, DMZ-systemer, interne servere eller trådløse systemer.

## Intelligente angreb finder de relevante sårbarheder

Testen dækker hele spektret af trusler fra de såkaldte "script-kiddie"-angreb, der typisk udnytter sårbarheder i operativsystemer, til dedikerede angreb, hvor målet er at tilgå, tilføje, ændre eller slette data.

Vores erfaring fra mange af Danmarks store og mellemstore organisationer viser, at minimum 40 % af alle højrisikosårbarheder findes via manuelle testscenarier og vil udelukkende kunne findes i en kombination af de anvendte værktøjer og spidskompetence inden for penetrationstest.

## Procedure for penetrationstest

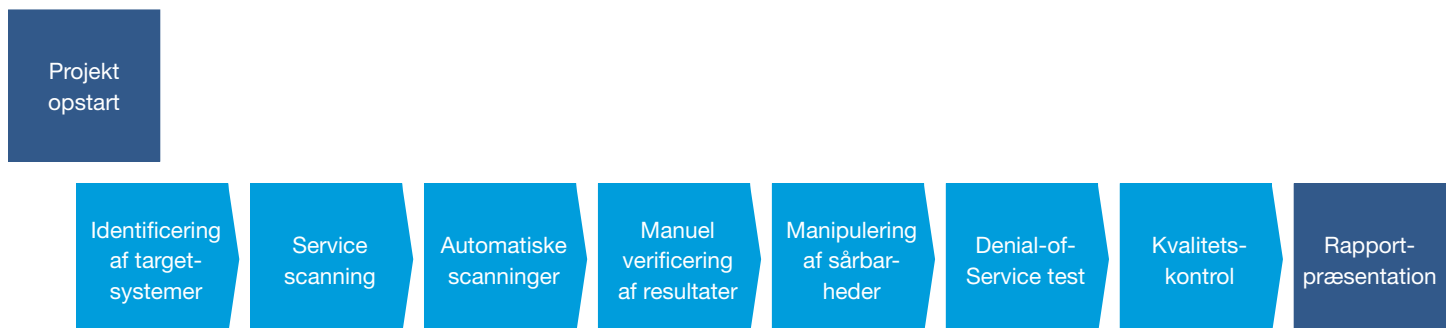
PricewaterhouseCoopers' Penetrationstest følger en velbeskrevet og -afprøvet testprocedure:

- Indledende identificering og afstemning af target-systemer
- Udførelse af selve testen
  - automatiske værktøjer med efterfølgende verificering af resultater
  - manuelle og avancerede testcases
  - ude-af-drift angreb (DOS) (hvis aftalt)
  - avanceret udnyttelse af testresultater til dybdegående penetration af systemerne
- Analyse af resultater samt risikovurdering
- Rapportering og præsentation.

## Rapportering og præsentation

Resultaterne af alle vores tests samles i en rapport, der indeholder et overordnet ledelses-summary med en vurdering af sikkerhedsniveauet og prioriterede anbefalinger til, hvordan dette kan øges. Desuden indeholder rapporten detaljerede beskrivelser af samtlige fundne sårbarheder med angivelse af risikoniveau, hvor de er fundet, og hvordan de kan udbedres. Rapporten præsenteres af den ansvarlige sikkerhedskonsulent på et møde, hvor alle kundens interessenter har mulighed for at få besvaret spørgsmål.

## Model 2



## Sårbarhedsscanninger

Det globale it-trusselbillede påvirkes hele tiden af udviklingen inden for internet- og systemsårbarheder. Kontrol med sårbarheder i egne netværk og systemer kræver konsekvent opdaterede tests.

For at afdække sikkerheden på mindre kritiske systemer, eller som et regelmæssigt supplement til de mere dybdegående testscenarier beskrevet på de foregående sider, tilbyder PricewaterhouseCoopers også forskellige niveauer af sårbarhedsscanninger i abonnementsform.

Disse scanningsydelser er baseret på såvel proprietær udvikling som kommercielle værktøjer, der vedligeholdes løbende af vores sikkerhedskonsulenter og -udviklere. Vi tilbyder sårbarhedsscanninger på to niveauer i form af den traditionelle sårbarhedsscanner **Pro-Scan** samt webapplikationsscanneren **WebCHK**.

Et **Pro-Scan** abonnement giver mulighed for at scanne internet-tilgængelige systemer for kendte sårbarheder, primært i operativsystemet. Scanninger oprettes via en PricewaterhouseCoopers hjemmeside og udføres mod de systemer og i den frekvens, som kunden ønsker. Rapporter er ligeledes tilgængelige for download fra hjemmesiden.

### Pro-Scan giver dig:

- Sårbarhedskontrol med alle internet-tilgængelige netværk samt enheder med IP-adresser
- Sikkerhed for at jeres internet-tilgængelige enheder ikke er sårbare over for de mest almindelige trusler, såsom vira og orme
- Flexibel planlægning af regelmæssige scanninger
- Vished for dit sikkerhedsniveau.

**WebCHK** scanninger går et spadestik dybere og giver mulighed for at teste sikkerheden i web-applikationer, hvor der typisk er størst mulighed for at udnytte sikkerhedsbrister.

### WebCHK giver dig:

- Kontrol af sårbarheder på egenudviklede webapplikationer
- Sikkerhed for at jeres websider, der typisk udgør den største sikkerhedsmæssig risiko, ikke kan bruges som adgang til mere kritiske data
- Flexibel planlægning af regelmæssige scanninger.

Begge abonnementer kontrolleres af virksomheden, der selv bestemmer hvilke systemer og i hvilken frekvens, der skal scannes. PricewaterhouseCoopers' konsulenter kontrollerer resultaterne af alle scanninger, fjerner falske-positiver og kontakter dig i tilfælde af graverende trusler.

Med PricewaterhouseCoopers Security & Technology som sikkerhedspartner har du mulighed for at sammensætte det optimale niveau for sikkerhedstest af dine systemer.



### Kontakt:

Security & Technology  
Tlf. 3945 3945  
E-mail: [itsecurity@pwc.dk](mailto:itsecurity@pwc.dk)

PricewaterhouseCoopers  
Strandvejen 44  
2900 Hellerup  
[www.pwc.dk/it-sikkerhed](http://www.pwc.dk/it-sikkerhed)