



INTERN SIKKERHEDSTEST

>> Hvorfor er den interne netværkssikkerhed vigtig?

Virksomhedens anvendelse af IT er i dag væsentlig for selskabets indtjening og image. Det er derfor vigtigt, at IT anvendelsen er sikker, og uden risiko for uautoriseret adgang til at modificere, slette eller læse fortrolige data både bevidst eller ubevidst. Statistikker viser, at mere end 60 % af alle gennemførte angreb i virksomheden bliver begået af ansatte eller tidligere ansatte. Det er derfor ligeså vigtigt at beskytte det interne som det eksterne netværk for hackere.

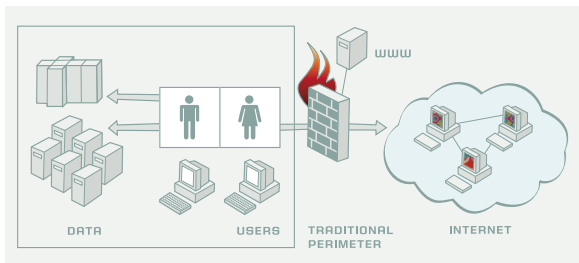
>> Dit lokale netværk kan være svært at overskue

IPCURE scanneren checker dit netværk for potentielle sikkerhedshuller som kan udnyttes til at kompromittere infrastrukturen. Ved at analysere operativsystemet og de applikationer der kører på netværket, identificerer IPCURE scanneren mulige sikkerhedshuller. Med andre ord fungerer den som djævelens advokat og orienterer dig før en hacker opdager og udnytter det.

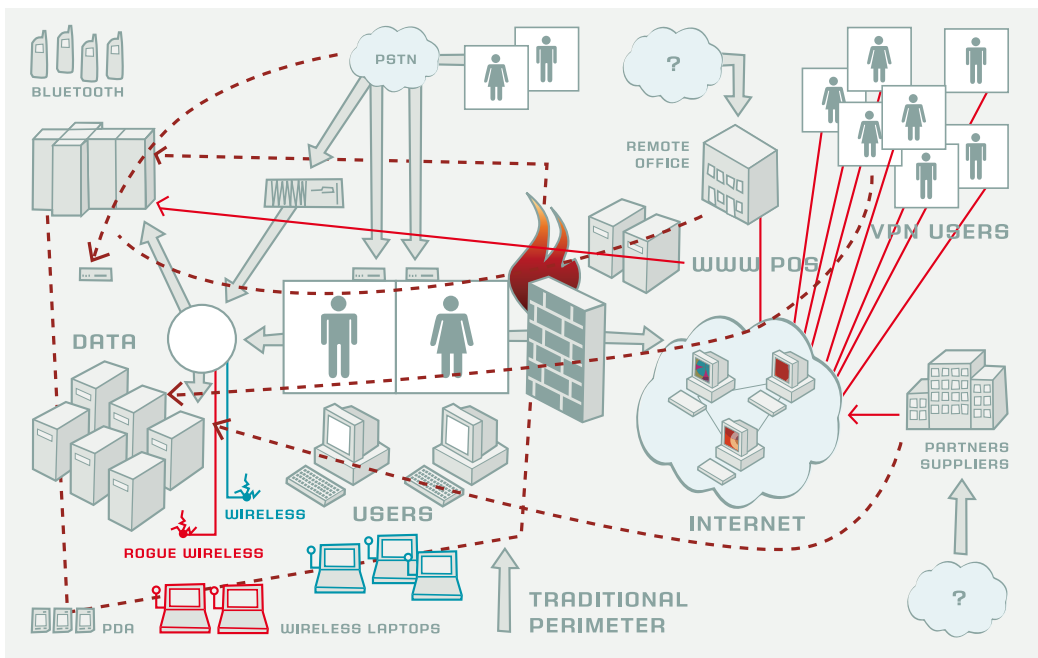
>> Få detaljeret information om samtlige enheder

Med IPCURE har du mulighed for at scanne hele dit netværk, IP- for IP-adresse og få overblik over manglende sikkerhedsopdateringer, wireless access points, USB enheder, åbne drev, åbne porte, services og applikationer der er aktive på netværket, key registry, password politikker, brugere, grupper og meget andet. Resultatet kommer i overskuelige rapporter, hvilket gør det muligt proaktivt at sikre netværket – f.eks. lukke unødige porte, lukke drev, installere service packs og hotfix m.v.

Et netværk kan være enkelt og overskueligt



- eller komplet og svært overskueligt





»» Få overblik over sikkerhedshuller og anbefalede løsninger

Når IPCURE har gennemført scanningen, bliver sårbarhederne kategoriseret efter risiko og en anbefaling bliver anvist. Hvor det er muligt, er der links til yderligere information om problemerne, f.eks. et BugTrag ID eller et Microsoft KnowledgeBase artikel ID m.v.

»» Find alle drev på netværket

IPCURE lister samtlige drev på netværket, incl. administrative drev og printer drev (C\$, D\$, ADMIN\$) og viser, hvem der har adgang til de enkelte drev, som bl.a. kan hjælpe med at:

- Checke om rettigheder til de enkelte drev er korrekte
- Checke om en bruger deler drev med andre brugere
- Forebygge anonym adgang til drev
- Sikre at start-op foldere eller lignende systemfiler ikke er delte, da det kan give uautoriserede brugere adgang til at afvikle kode

»» Wireless node/link detection

IPCURE kan identificere maskiner/enheder der er forbundet til dit netværk via et wireless link. Wireless links er en stor sikkerhedsrisiko, hvis de ikke er sikrede korrekt. At finde uautoriserede og usikrede wireless links er derfor vigtigt.

»» Check for passwordpolitikker

IPCURE checker automatisk for passwordpolitikker for brugere på alle enheder. IPCURE vil vise både drev og NTFS adgangsforhold for alle drev på netværket – hvilket giver et hurtigt overblik til brug for at lukke unødige drev.

»» Automatisk planlægning og igangsætning af test samt sammenligning med tidligere test

IPCURE scanneren kan udføre planlagte sikkerhedsscanninger (dagligt, ugentligt eller månedligt) og automatisk sammenligne med tidligere testresultater. Enhver ny port eller services der er aktive samt nye sikkerhedshuller er markerede, hvilket giver et hurtigt overblik.

»» Løbende proces

Netværkssikkerhed er en løbende proces, hvorfor man ikke med et snapshot kan forvente at forblive sikker. Digicure anbefaler, at man månedligt eller som minimum kvartalsvis gennemfører en sikkerhedsscanning både på inder- og ydersiden af firewallen.

»» Krav

IPCURE scanneren kræver ganske få ressourcer og vil ikke belaste dit netværk mærkbart. En ganske almindelig PC med CD rom drev vil være tilstrækkelig. Og efter mindre end 15 min. er systemet klar til at gennemføre de første test.