



## Faren ved sårbarheder

Sårbarheder findes i næsten alle softwareprodukter. Det er fejl, der kan udnyttes til at overtage kontrollen med maskinen, forhindre den i at fungere efter hensigten, få den til at gå ned eller på anden måde kompromittere dit system.

En sårbarhed kan udnyttes ved at køre et simpelt program, enhver uden særlige kompetencer kan finde på internettet og anvende. 95% af alle angreb udnytter kendte sårbarheder. Man undgår angrebene ved at fjerne sårbarhederne. Det kan Digicure hjælpe dig med ved regelmæssige sikkerhedsscanninger.

### »» IPCURE EKSTERN: Sikkerhed udefra



En IPCURE ekstern sårbarhedsanalyse giver dig et komplet overblik over din virksomheds eksterne IT-sikkerhed ved hjælp af en række dybtgående tests.

Testen gennemføres over internettet op mod de eksterne ip-adresser. Her testes din firewall og services tilgængelige herigennem, deriblandt mailservere, webservere, databaseservere etc., og sårbarhederne afdækkes. Analysen afsluttes med en let forståelig, detaljeret rapport, som fortæller dig alt om de fundne sårbarheder – og giver gode råd om, hvordan de mest effektivt og økonomisk kan fjernes.

### »» IPCURE PCI: Lad Digicure sikre dig PCI Compliance



PCI-standarden er en international standard for håndtering, opbevaring og transmission af kreditkortdata. Hvis din virksomhed har med betalingskort at gøre, skal den overholde reglerne fra PCI. Manglende overholdelse kan føre til syvcifrede bøder, ansvar for eventuelle tab samt mistet ret til at acceptere kreditkort.

En IPCURE PCI sikkerhedsanalyse fortæller dig, om din virksomhed opfylder PCI DSS-standarden. Digicure kan også hjælpe med at opnå og vedligeholde PCI compliance. Vi tilbyder rådgivning, sikkerhedsanalyser og scanninger til e-handelsvirksomheder med kreditkortbetaling, service providers m.v..

### »» IPCURE INTERN: Sikkerhed blandt medarbejderne



Over 60% af alle gennemførte angreb i virksomheder bliver begået af ansatte eller tidligere ansatte. Derfor er det lige så vigtigt at beskytte det interne som det eksterne netværk mod hackere.

Denne test afvikles hos dig, hvor vi foretager en sikkerhedsscanning af servere, klienter og andre services, som er knyttet til de interne ip-adresser. Den interne analyse vil blandt andet afsløre manglende sikkerhedsopdateringer, wireless access points, services og applikationer aktive på netværket, problemer med key registry, password-politikker, mappedelinger, USB-enheder, åbne drev og porte mm.

Efter en IPCURE intern sårbarhedsanalyse har du et komplet overblik over virksomhedens tekniske IT-sikkerhed, og den sikkerhedsansvarlige kan let vælge, hvor der skal sættes ind.

### »» IPCURE WEB: Sikkerhed på nettet



70% af alle hjemmesider er sårbare overfor datatyveri eller datamanipulation. Hackerne fokuserer på websteder og webbaserede applikationer som indkøbssystemer, formularer, loginsider og dynamisk indhold. De er tilgængelige fra enhver PC i verden og forbinder ofte direkte til værdifulde backend data som kundedatabaser m.v.

[fortsætter på bagsiden >>](#)





>> fortsat fra forsiden.

Digicures sikkerhedsekspert kan identificere sikkerhedsbrister i virksomhedens webapplikationer, før de bliver udnyttet. Vi crawler hele din hjemmeside med avancerede scanningsværktøjer, simulerer realistiske angreb mod dine systemer og udfører en lang række sikkerhedstests. Samtlige sider analyseres med henblik på kritiske SQL injections, cross site scripting og andre risikomomenter. Resultaterne checkes, og alle sårbarheder gennemgås manuelt. Derefter udarbejder vi en detaljeret rapport over det fundne inklusive en sikkerhedsrating og en praktisk anbefaling til løsning af eventuelle problemer.

### >> Sikkerhedsrapporten et værdifuldt værktøj

Efter enhver IPCURE test modtager du en rapport, som overskueligt og let forståeligt beskriver de fundne sårbarheder og foreslår løsninger.

Rapporten er kernen i vores samarbejde og opdelt i henholdsvis en teknisk og en ledelsesorienteret del.

Den tekniske del indeholder alle oplysninger om sårbarheder, mens den ledelsesorienterede yderligere indeholder et ikke-teknisk overblik. Rapporten giver dig desuden konstruktive forslag, aktive links til opdateringer, workarounds, diskussioner etc., som hjælper dig eller din driftspartner med at løse problemerne hurtigt og omkostningsbesparende.

### >> IPCURE TRÅDLØS: Sikkerhed gennem luften



Et trådløst netværk med sikkerhedshuller kan give hackere adgang til dit interne netværk udefra. IPCURE trådløs sikkerhedstest evaluerer sikkerheden i din trådløse netværksløsning ved hjælp af anerkendte metoder. Resultatet er et klart overblik over eventuelle sårbarheder, som beskrives i sikkerhedsrapporten sammen med anbefalinger til løsning.

