



– uvildig sikkerhedstest af virksomhedens IT-system

Anvendelsen af IT er i dag en nødvendighed for at kunne drive en konkurrencedygtig og effektiv virksomhed. Beskyttelse af vores IT-systemer er derfor vigtigere end nogensinde.

Jvf. sikkerhedsorganisationen CERT/CC (CERT Coordination center) er antallet af sikkerhedshændelser mere end fordoblet gennem det seneste årti. Siden 1999 er antallet af nyopdagede sårbarheder fordoblet fra år til år.

Før en virksomhed effektivt kan beskytte sig mod angreb, der tager udgangspunkt i dens sårbarheder, må IT-afdelingen kende til disse sårbarheder.

IPCURE er en uvildig sikkerhedstest, der afdækker hvilke kendte sårbarheder, der findes på netop din virksomheds IT-system.

»» **Hvad tester IPCURE for og hvordan gøres det?**

IPCURE er en uvildig sikkerhedstest der tester netop din virksomheds IT-system. Hele testen gennemføres af Digicures sikkerhedsteknikere som en kombination af manuelle og automatiske test. Testgennemførelsen kræver alene Digicures arbejdsindsats.

Ved hjælp af mere end 2.000 testprocedurer testes der for mere end 20.000 sårbarheder.

Testen inkluderer også informations-lækager, potentielt farlige services, åbne porte etc.

»» **Rapportering**

Når testen er færdig, fremsendes en rapport. Der findes to slags rapporter – henholdsvis en teknisk og en ledelsesorienteret rapport.

Den tekniske rapport indeholder kun oplysninger om sårbarheder, åbne porte etc., mens den ledelsesorienterede yderligere indeholder et ikke-teknisk overblik illustreret med grafer.

Rapporten indeholder endvidere løsningsforslag, aktive links til opdateringer, workarounds,

diskussioner etc., som hjælper dig eller din driftspartner med at løse problemerne hurtigt og dermed omkostningsbesparende.

»» **Hvad er en sårbarhed og hvorfor er det slemt?**

En sårbarhed kan bl.a. være en software- eller konfigurationsfejl, der kan udnyttes til at overtage kontrollen med maskinen; forhindre maskinen i at fungere efter hensigten; få den til at gå ned eller på anden måde kompromittere de systemer, man bruger. I næsten alle softwareprodukter findes der sådanne fejl.

En sårbarhed kan udnyttes ved at køre et simpelt program, der findes frit tilgængeligt på internettet. Derfor er det vigtigt at begrænse antallet af sårbarheder, da det ikke kræver nogle specielle kompetencer at udnytte dem.

95% af de angreb man ser i dag, er en udnyttelse af kendte sårbarheder. Ved at fjerne sårbarhederne, undgår man disse angreb.





>> Dagligt nye sårbarheder

Digicure benytter en lang række af de mest anerkendte og anvendte sikkerhedsanalyse- og testværktøjer. Disse førende værktøjer kombineret med en række manuelle testprocedurer sikrer en grundig og detaljeret analyse.

Da der dagligt kommer nye sårbarheder og for at sikre, at de seneste sårbarheder altid er med i de gennemførte tests, opdateres vores sårbarhedsdatabase mindst to gange i døgnet.

Grundet dette og da man ofte omkonfigurerer sine services, samt installerer nyt software, fås det bedste resultat ved at teste regelmæssigt.

På den måde sikrer man løbende et overblik over IT-sikkerheden.

>> International sårbarhedsklassificering

De sårbarheder der rapporteres, klassificeres i forskellige grupper (Høj-, mellem- eller lavrisiko) efter betydning. Denne klassificering er fastsat efter internationale standarder. Disse grupper afspejler risikoen ved de enkelte sårbarheder og giver derfor et godt overblik, der til dels kan bruges til en prioriteret handlingsplan og dels til revision.

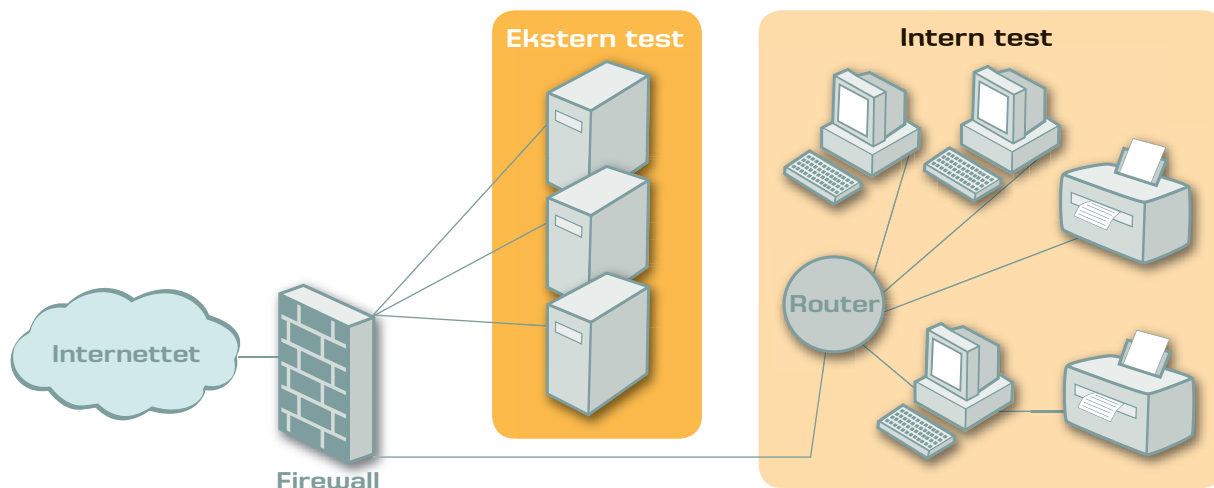
IPCURE kan teste på to forskellige måder



- >> Testen gennemføres over internettet op mod et udsnit eller alle eksterne ip-adresser. Her bliver firewallen, samt de services, der er tilgængelige gennem denne, testet. Disse services kan blandt andet være mailservere, webservere, database servere etc. Alle kendte sårbarheder på disse services bliver afdækket. Der bliver ikke testet på arbejdsstationerne i lokalnettet.



- >> Denne test afvikles "on location". Her bliver der testet op mod et udsnit eller alle interne ip-adresser. Dermed bliver alle arbejdsstationer samt services bagved firewallen testet.



Om DIGICURE »

Digicure er en ekspanderende danskejett virksomhed, som tilbyder virksomheder uvildige analyser indenfor IT-sikkerhed og overvågning af websites. Vores erfaring kommer fra mange års praktisk involvering i implementering af sikkerheds løsninger for såvel store som små virksomheder. Digicure følger en kunde orienteret fremgangsmåde i enhver henseende. Digicures medarbejdere sætter en dyd i at forstå vore kunders behov såvel før, under som efter et samarbejde. Vore kunder spænder vidt på brancher og virksomhedsstørrelser - fælles for dem alle er, at IT-sikkerhed og fokus på webaktiviteter er prioriteret højt i hverdagen.