Penetrations test

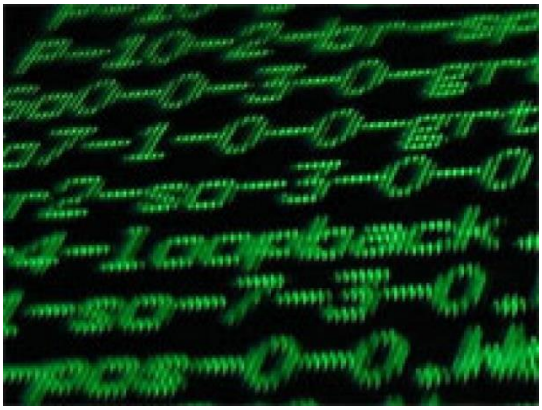
Af netværket

DEFENSIVE IT-SOLUTIONS

Potentielle risici

Jeres virksomhed er som regel beskyttet udadtil med VPN'er og firewalls, med en barriere mellem jeres interne netværk, og et ydre, åbent netværk, som eksempelvis Internettet. Yderligere kan IPS/IDS være i brug, for at kunne arlarmere administratorer, i tilfælde af en potentiel indtrængen – og af og til kan IPS/IDS'en forhindre en sådan indtængen. Disse kontrolforanstaltninger, giver i værste tilfælde, eksterne angribere mulighed for at kompromittere jeres virksomheds interne netværk og fortrolige data, uden at det reelt kan opdages.

Jeres virksomheds netværk er mål for trusler som malware, hackere eller insidere, der har opnået adgang til jeres interne netværk. Undersøgelser understreger vigtigtheden af penetrationstests af netværket, da ca. 95% af alle virksomheder har væsentlige sårbarheder i de underliggende interne netværk. Dette tillader dermed malware, eller en angriber at sætte sig selv ind som switch eller router. Resultatet af dette, bliver at fortroligheden og tilgængeligheden af størstedelen af systerme på pågældende netværk, kan kompromitteres. Dette er inklusiv fortrolige data, som lagres eller kommunikeres af disse systemer.



Ydelser

Med stor erfaring og ekspertise med penetrations tests, og med de bredest internationalt anerkendte certificeringer, udfører Defensive IT-Solutions manuelle tests, som lokaliserer sårbarhederne i jeres netværk. Alle de tests vi kører, er skræddersyet præcis til jeres virksomhed, og er derfor tilpasset til jeres behov.

Defensive IT-Solutions er i stand til at udføre eksterne professionelle penetrationstests af flere forskellige enheder, der eksempelvis kunne være:

- ✓ VPN'er
- ✓ Firewalls
- ✓ IPS/IDS

Interne identificerer og analyserer vi de anvendte protokoller, så vi dermed kan afdække sårbarhederne som lokaliseres i dem. Dette kan f.eks. omfatte følgende:

- ✓ Router-protokoller (F.eks. RIP, IS-IS, OSPF, IGRP)
- ✓ Link layer-protokoller (F.eks. IST, ARP, CDP, LLTD, FDP, NDP, STP)

- ✓ Application layer-netværksprotokoller (F.eks. DHCP, LLMNR, NBT-NS)
- ✓ Redundansprotokoller (F.eks. R-SMLT, VRRP, HRSP, NSRP, ESRP; CARP, GLBP)
- ✓ Åbne porte på interne routere og switches.

Enhver konstateret sårbarhed vil blive uddybende behandlet i en detaljeret sikkerhedsrapport og i en valgfri mundtlig præsentation for at hjælpe udviklere og administratorer til at udbedre de identificerede sårbarheder. Dette inkluderer endvidere en overordnet konklusion til ledelsen

Fordele ved at vælge Defensive IT-Solutions

- ✓ Vi leverer en hurtig og god service, og er proaktive i forhold til ydelsen af hjælp til vores kunder.
- ✓ Vi hjælper dig hurtigt og effektivt, med at finde og fikse sårbarheder, og forhindrer eksterne angribere i at opnå adgang til jeres interne netværk.
- ✓ Vi kan hjælpe med at opnå kontrol over sårbare protokoller på jeres interne netværk, som højst sandsynligt tillader insidere, malware eller hackere at kompromittere hovedparten – eller alle – hosts på jeres interne netværk.
- ✓ Vi fastslår jeres nuværende sikkerhedsniveau, og hjælper jer med at udbedre det.
- ✓ Vi viser rettidig omhu for ledelse, revisorer og/eller kunder.

Kontaktinformationer

Vi står altid til rådighed, i tilfælde af uklarheder eller problemer. Send en mail til info@defit.dk eller ring på mobil-nummeret +45 40 11 30 31, hvis det er din virksomhed, der mangler et sikkerhedsboost fra en virksomhed med stor ekspertise og en effektiv arbejdsindsats.

Her hos Defensive IT-Solutions tager vi med glæde en uforpligtende dialog, hvis din virksomhed har behov for at få udført en sikker og hurtig penetrationstest.

DEFENSIVE IT-SOLUTIONS

Powered by Knowledge

Forhandler: ITZONE