



Pentest

Fra svaghed til styrke med en pentest

En pentest er en praktisk og målrettet test af jeres IT-sikkerhed, hvor formålet er at **simulere realistiske angreb mod jeres systemer - præcis som en rigtig angriber ville gøre**. I modsætning til en klassisk sikkerhedsanalyse, hvor man vurderer konfigurationer og opsætninger, er en pentest en aktiv, teknisk test, der forsøger at finde frem til sårbarheder gennem konkrete angrebsveje.

Testen udføres med udgangspunkt i et fastlagt scope og inden for klare rammer, hvor vi arbejder struktureret og ansvarligt, men med samme tankegang og metoder som en ondsindet aktør ville anvende.

En pentest er relevant, når man bl.a. ønsker at:

- Dokumentere reelle risici frem for hypotetiske
- Validere, at eksisterende sikkerhedstiltag fungerer i praksis
- Imødekomme krav fra fx NIS2, DORA eller kunders compliance-behov

Vi angriber både udefra - ligesom en hacker på internettet ville gøre - og indefra, som hvis nogen allerede har fået adgang til jeres netværk. Det kaldes et "assumed breach" og hjælper med at finde ud af, hvad en angriber ville kunne gøre, hvis de først er kommet indenfor.

Vi tilpasser altid testen til jeres konkrete setup og hverdag, så det giver mening i forhold til jeres drift. Hele forløbet foregår i tæt dialog med jer, og I får løbende indblik i hvad der sker, så der aldrig opstår tvivl om, hvad vi gør eller hvorfor vi gør det.



Proces og tidsplan

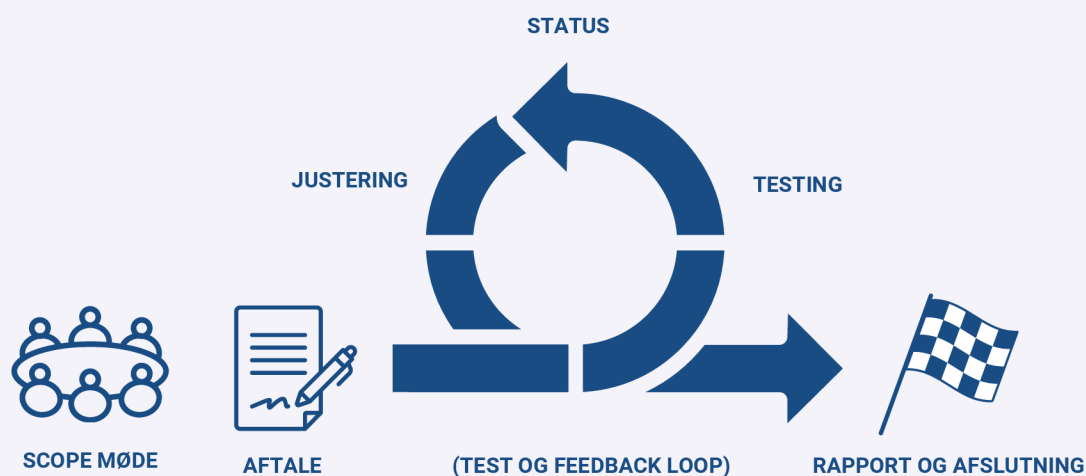
Pentesten tager udgangspunkt i jeres setup og mål. Vi arbejder fleksibelt og prioriterer at levere indsigt, der er let at handle på.

Formål: Dokumentér reelle risici gennem praktisk hacking-simulation.

Proces:

- **Scope-møde:** Et indledende møde, hvor vi sammen aftaler, hvad der skal testes, hvordan testen skal foregå, hvilke områder vi skal fokusere på, og hvem hos jer vi skal tale med undervejs. Vi sikrer, at I ved præcis, hvad der bliver gjort - og at testen passer til jeres virksomhed og behov.
- **Testfase:** Gennemførelse af realistiske angrebsveje fra eksternt (internet) og internt (assumed breach)
- **Gen-test (valgfrit):** Efter udbedringer validerer vi, om sårbarheder er korrekt lukket
- **Afsluttende møde:** Rapportgennemgang med mulighed for at dykke ned i fund og næste skridt

Testen tilpasses løbende undervejs, så vi kan dykke dybere ned i områder med særlig risiko. Hvis relevante forhold ændrer sig under testen, justerer vi indsatsen i dialog med jer.



Tidsplan

Den typiske tidsplan for en pentest ser sådan ud:

- **Scope-møde:** Uge 1
- **Testfase:** Uge 2 til 3
- **Rapportlevering:** Senest 14 dage efter afsluttet test
- **Afsluttende møde:** Aftales umiddelbart efter levering

Tidsplanen kan justeres afhængigt af jeres behov, tilgængelighed og kompleksitet i infrastrukturen.

Resultat, leverancer og pris

Resultat

Pentesten giver jer et realistisk billede af, hvor jeres løsning er mest sårbar, hvordan en angriber kan udnytte disse svagheder og hvad I skal gøre for at lukke hullerne.

Det hele dokumenteres i en struktureret rapport og præsenteres på en måde, der både giver overblik og teknisk dybde. Formålet er, at I kan handle direkte på fundene og omsætte dem til konkrete forbedringer i jeres drift.

Leverancer

Rapporten fra pentesten består af to dele:

- **Ledelsesresume:** En let læselig one-pager med en samlet vurdering og anbefalinger målrettet ledelsen. Leveres som udgangspunkt på dansk.
- **Teknisk rapport:** En detaljeret teknisk gennemgang af fundne sårbarheder, trin-for-trin angrebsveje, dokumentation, og konkrete forslag til afhjælpning. Leveres på engelsk.

Derudover afholdes et afsluttende online møde, hvor rapporten gennemgås og næste skridt kan drøftes.

Pris

Prisen for en pentest starter ved 39.000 DKK ekskl. moms.

Den endelige pris afhænger af omfanget og fastlægges i fællesskab under et scopemøde, hvor vi afstemmer forventninger, mål og teknisk rækkevidde.

Vi tilbyder fem pentestpakker med forskelligt omfang, fra grundlæggende vurderinger til dybdegående angrebssimulationer.

Pentest pakker	Dage til testen	Pris (eksl. moms)
ESSENTIAL	3 dage	39.000,00 DKK
STANDARD	6 dage	78.000,00 DKK
ADVANCED	9 dage	112.000,00 DKK
ELITE	12 dage	145.000,00 DKK
RED TEAM FULL	18 dage	210.000,00 DKK

Hvorfor vælge Cyber Partners?

Vi arbejder som hackere, ikke som traditionelle konsulenter. I stedet for at gennemgå tjeklister, udfører vi realistiske simulationer, der afspejler de trusler, I faktisk står overfor. Resultatet er konkret viden frem for generiske rapporter, og I modtager praktiske handlingsplaner, som I kan tage i brug med det samme. Hele indsatsen er nøje tilpasset jeres branche, systemer og specifikke behov.



CYBER PARTNERS

Enkelt, forståeligt og tilgængeligt

Se mere på cyberpartners.dk