Sårbarhetsanalyse

Finn svakhetene før noen utnytter dem

Etisk Hacker AS undersøker avtalte IT-systemer for tekniske svakheter og tester om utvalgte funn kan utnyttes. Dere får oversikt over risikoen og anbefalte tiltak, slik at IT-ansvarlig eller driftsleverandør kan prioritere det viktigste først.

HVORFOR VIRKSOMHETEN TRENGER DETTE

01

Avdekk skjulte svakheter

En tjeneste som er åpen, en utdatert server eller en feil innstilling kan gi en angriper en vei inn.

Verdi: Finn forhold som bør rettes.

02

Se hva som kan utnyttes

Kontrollert testing av utvalgte funn viser om en oppdaget svakhet faktisk kan brukes i et angrep.

Verdi: Et tydeligere bilde av reell risiko.

03

Prioriter riktige tiltak

Når funn vurderes etter alvorlighet, blir det enklere å bruke tid og budsjett der behovet er størst.

Verdi: Et konkret grunnlag for IT-arbeidet.

04

Beskytt drift og informasjon

Utnyttede svakheter kan føre til uvedkommende tilgang, tap av informasjon eller driftsstans.

Verdi: Grunnlag for å redusere risikoen.

Hva er en sårbarhetsanalyse

Tenk på det som en kontroll av virksomhetens digitale dører og låser. Vi kartlegger hvilke innganger som finnes, undersøker kjente svakheter og prøver utvalgte funn innenfor avtalte rammer. Resultatet viser hva dere bør følge opp.

Dere trenger ikke forstå verktøyene for å få verdi av testen. Det viktigste er å vite hvor dere er utsatt, og hva dere bør gjøre med det.

Dette inneholder analysen

Fra tekniske funn til en forståelig prioritering

Testen kombinerer kartlegging, analyse, kontrollert utnyttelse og rapportering. Systemer, testtidspunkt og rammer for aktiv testing avklares før oppstart.

01 **Kartlegging av nettverk og tjenester**

Vi ser etter åpne tilkoblingspunkter, tjenester og systemversjoner, og sjekker kjente sårbarheter. Nmap brukes til kartleggingen.

02 **Undersøkelse av webtjenester**

Med Nikto undersøker vi webservere og webtjenester for kjente svakheter og usikre innstillinger som kan gi angrepsmuligheter.

03 **Kontrollert testing av utvalgte svakheter**

Med Metasploit tester vi om identifiserte svakheter kan utnyttes, og vurderer mulige konsekvenser. Aktiv testing skjer innenfor avtalt omfang.

04 **Rapport med risiko og anbefalte tiltak**

Dere får funn, alvorlighetsgrad, relevante CVE-referanser og råd om utbedring. Kritiske funn markeres i rødt. Bevis, som logger og skjermbilder, tas med der det er mulig.

Regelmessige skanninger kan avtales

Skanninger kan planlegges daglig, ukentlig eller månedlig, med automatisk utsendelse av PDF-rapporter til avtalt e-postadresse. Hyppighet og omfang tilpasses virksomheten.

Få oversikt over hvor virksomheten er utsatt

Kontakt oss for å avklare hvilke systemer som bør testes, og et passende omfang for deres virksomhet.

eddie@etiskhacker.no | +47 400 13 483 | etiskhacker.no

Test og rapport behandles konfidensielt. Analysen gir et øyeblikksbilde av avtalte systemer og kan ikke avdekke alle svakheter. CVE er referansenumre for offentlig kjente sårbarheter.