

Sårbarhedsscanning af websites



Er der sikkerhedshuller der skal lukkes?

Angreb mod websites sker konstant, og som regel uden dit kendskab. 1000-vis af scanninger, hvor hackere forsøger at finde huller i dit website på daglig basis. Med en sårbarhedsscanning kommer du hackerne i forkøbet, og får mulighed for, at få lukket evt. huller, før de bliver udnyttet.

Hos Unitas bliver sårbarhedsscanninger, evt. kombineret med en udvidet penetrations-test, udført af specialister og med anvendelse af anerkendte og moderne OWASP® base-rede værktøjer.

Unitas anbefaler, at du får udført penetrationstest gennem bruger-login på sitet, hvis dit site rummer fx en kunde-klub eller andre data, der er skjult bag et login og er af fortrolig eller følsom kategori.

Det er også muligt at få scannet andre services som fx FTP eller mail-server.

Unitas varetager planlægning gennem et årshjul, og foretager automatisk scanning efter aftalt hyppighed.

Efter scanning modtager du en rapport over resultatet samt handlingsplan for at lukke evt. huller.

Ved henvendelse sender vi dig en anonymiseret rapport som eksempel.

Resultat

Mulighed for at komme hackerne i forkøbet
Efterlevelse af compliance-referenceramme
En reel handlingsplan for at lukke evt. huller
En ekstern uvildig specialistpartner som udførende
Kendte omkostninger over tid via serviceaftale

Sådan kommer du i gang

2 timers online mini-workshop hvor behov og detaljer klarlægges:

- hvad skal scannes, hvor ofte, hvad vil I opnå

Gennemgang af rapport fra gang til gang på initiativ af Unitas

Forudsætninger

Evt. tilpasning af perimeterudstyr for at kunne gennemføre scanning

Login til bagvedliggende system, hvis der ønskes penetrationstest

COMPLIANCE REFERENCE

Understøtter følgende kontroller:

CIS-20

Elementer i kategori 3, 9, 11, 20

ISO27001

10.6.x, 10.9.x, 12.6.1, 15.2.1 m.fl.

2020 Af: UNITAS ApS	UNITAS
TIL VIRKSOMHEDEN 1	
OM EKSTERN PARTNER UNITAS APS 2	
KONSULENTINFORMATION OG UNDERSKRIFT 2	
OVERORDNET KONKLUSION 4	
FORMÅL, SCOPE, AFGRÆNSNING OG METODE 5	
FORMÅL 5	
MÅLSÆTNING 5	
SCOPE 5	
AFGRÆNSNING 5	
METODE 5	
RESULTAT AF SÅRBARHEDSSCANNING 6	
RESULTATOPSUMMERING – SÅRBARHEDSSCANNING MED BRUG AF OPENVAS 6	
RESULTATOPSUMMERING – SÅRBARHEDSSCANNING MED BRUG AF OWASP 6	
RESULTAT AF PENETRATIONSTEST 7	
BILAG 1 – FULD SCANNINGSRAPPORT FRA OPENVAS 8	
BILAG 2 – FULD SCANNINGSRAPPORT FRA OWASP 46	

Testrapport

- sårbarhedsscanning og penetrationstest af <Virksomhed>
<Virksomhed>

Økonomi

Eksempler:

Indledende scanning 7.500,-

4 årlige scanninger kr. 15.000,-

Indledende penetrationstest (inkl. scanning) 10.000,-

4 årlige penetrationstests kr. 22.500,-

Priserne er pr. service/website.

Kontakt os hvis I har mange sites eller særlige behov.

DKK ekskl. moms og transportomk.

