

Sikkerhed om din IT-sikkerhed...

Periodiske sikkerhedsscanninger er en række teknologisk og økonomisk fordelagtige kontrolforanstaltninger, afviklet som en cyklus af serviceydelser der løbende verificerer sikkerheden i systemerne. Med periodiske sikkerhedsscanninger kan I sige at I kontinuerligt lever op til de krav der er stillet inden for de rammer der er aftalt! Årsabonnement fra kr. 7.500,- !

Med periodiske sikkerhedsscanninger opnår du en løbende kontrol af installationen, således at udbedring af eventuelle sårbarheder kan ske hurtigst muligt. De automatiserede scanninger skal tjene som en kontrol af eventuelle fejlkonfigurationer, fejlprogrammeringer eller manglende sikkerheds-opdateringer. Desuden vil de periodiske scanninger give mulighed for kontinuerlig forbedring af sikkerhedsniveauet. Periodiske sikkerhedsscanninger er det bedste middel til dem der ønsker en proaktiv og forebyggende sikring af IT-aktiverne.

Den menneskelige faktor

De periodiske sikkerhedsscanninger er baseret på automatiske scanningsværktøjer, der løbende opdateres med information om de nyeste sårbarheder. Selvom disse værktøjer er utrolig effektive og prismæssigt fordelagtige at anvende, kan de aldrig erstatte den menneskelige faktor. Derfor bør disse periodiske scanninger efter behov suppleres med en mere gennemgribende test, der også inkluderer angreb udført af sikkerhedsspecialister.

Frekvens

Afhængig af scanningstype kan der som standard vælges en scanningsfrekvens på 1, 4 eller et ubegrænset antal scanninger årligt. Eventuelle andre ønsker aftales individuelt.

Produktbeskrivelse

Ezen

- de skal være prismæssigt konkurrencedygtige uden at gå på kompromis med kvaliteten
- alle skal have råd til at få fortaget mere end én sårbarhedsscanning
- de skal være billige i drift
- de skal være nemme og hurtige at anvende
- fjerne besværet med komplicerede og tidskrævende opdateringer af egne værktøjer
- de kan automatisere de fleste almindelige sikkerhedsstopgaver
- de skal være overskuelige og simple at arbejde med
- de skal være altdækkende
- nSense er en (all-in-one) universal netværks- og webapplikationsscanner, der kan identificere alle kendte typer sårbarheder
- scanninger kan foretages på alle niveauer
- scannerne altid er fuldt opdaterede og klar til brug

Sårbarhedsscanninger

Regelmæssige sikkerhedsscanninger er en kontrolforanstaltning der verificerer at sikkerheden i virksomhedens webapplikationer og andre IT-systemer kontinuerligt lever op til de krav virksomheden stiller.

Med nSense sårbarhedsscanninger får virksomheden fuld afdækning af både webapplikationssårbarheder (nSense WebScan) og platformssårbarheder (nSense SystemScan). nSense sårbarhedsscanninger tjener som kontrol af eventuelle fejlkonfigurationer, fejlprogrammeringer eller manglende sikkerhedsopdateringer. Desuden giver nSense sårbarhedsscanninger mulighed for kontinuerlig forbedring af sikkerhedsniveauet.

nSense sårbarhedsscanninger kan afvikles efter behov eller med faste intervaller. System- og platformsscanninger

kan køres i "Continuous Scan mode", hvilket betyder at scanningerne kører "nonstop". I kombination med e-mail-alertagenter der sender en mail såfremt en sårbarhed detekteres, er man altid opdateret omkring tilstanden på ens sikkerhedsniveau.

nSense WebScan - webapplikationsscanning

nSense WebScan er en sikkerhedsscanner som udfører automatiseret gennemgang for sårbarheder i webapplikationer. nSense WebScan implementerer PeraSec Intelligens teknologi, som ikke er set i andre automatiske webapplikationsscanningsværktøjer. PeraSec Intelligens indeholder en fuldt ud dynamisk metode til informationsindsamling fra webapplikationen inden scanningen bliver gennemført. Ved at gøre dette bliver nSense i stand at undersøge områder af webapplikationen som normalt ikke undersøges ved anvendelse af standardscannere.

Sårbarhedsscanneren er rettet direkte imod den nyeste form for sårbarheder som findes i webapplikationer. Ingen traditionel firewall, intet antivirussystem e.l. er i stand til at forhindre hackere i at udnytte disse sårbarheder. Sårbarhedsscanneren bliver løbende konfigureret og optimeret af sikkerhedsspecialister.

nSenses automatiske webapplikations-sårbarhedsscanner dækker følgende områder:

- Cross Site Scripting
- SQL Injection
- Cookie Poisoning
- Parameter Tampering
- Forceful browsing
- WebDav Vulnerabilities
- Forceful Browsing based on textual analysis
- Textual Analysis - Suspicious Content
- Authentication Bypassing
- Simple Object Access Protocol Vulnerabilities
- Stealth Commanding
- 2 phase Cross Site Scripting Discovery

Resultaterne af scanningerne dokumenteres i en rapport, der er tilgængelig via en sikker forbindelse til kundens konto hos nSense. Rapporten fortæller præcist hvilke sårbarheder der er identificeret, hvor de er fundet, hvor alvorlige de er samt hvorledes de kan udbedres. Scanningerne kan afvikles efter behov eller gentages periodisk for at sikre løbende kontrol - typisk fra 4 til 12 gange pr. år.

nSense SystemScan - systemscanning

nSense SystemScan er en traditionel sårbarhedsscanner rettet mod platforme og systemer. nSense SystemScan anvender Nessus i en professionel udgave med "direct feed" af sårbarhedsopdateringer samt en lang række andre Open Source-sårbarhedsscannere. Herudover anvendes egenudviklede scannere. Open Source Scanner kan - korrekt sat op - finde rigtig mange sårbarheder, men nøgleordet er her "korrekt-sat-op". Open Source-scannere er ikke de nemmeste programmer at sætte op og forudsætter en hel del kendskab inden for sikkerhedsområdet.

nSense har et langt mere intuitivt brugerinterface og bliver løbende opdateret og optimeret af sikkerhedsspecialister. nSense SystemScan forudsætter derfor ikke specialistviden omkring opsætning og opdatering af en sårbarhedsscanner og sparer samtidig den tid der ellers ville blive anvendt til dette. Scanneren skal heller ikke installeres af kunden og den benytter heller ikke plugins eller andre programmer som skal installeres på de hosts der ønskes scannet.

nSense SystemScan er samtidig optimeret til at minimere falske positive og rapporterer derfor mere realistisk de potentielle sårbarheder der findes og som kan udnyttes. Ligeledes kommer SystemScan også med links til Proof of Concept-kode hvorved man selv har mulighed for at afprøve de fundne sårbarheder.

Sårbarhedsscanneren dækker følgende sårbarheder og områder:

- Operativsystem baserede sårbarheder (Microsoft, UNIX, Linux, mm.)
- Sårbarheder i standardapplikationer (mail & web servere, router, firewalls m.m.)
- Konfigurationsmæssige sårbarheder i firewalls og intrusion detection-systemer
- Konfigurationsmæssige sårbarheder i web-/applikations-servere

nSense Report Center

nSense Report Center er kundens videnscenter, som indeholder data for de scanninger og overvågningstjenester der er afviklet. Her kan de individuelle rapporter vises online på hjemmesiden eller printes ud som færdige rapporter i forskellige formater og udgaver. Samtidigt er det muligt at få fremvist et historisk billede af de tidligere gennemførte scanninger eller overvågningstjenester, således at man kan følge hvorledes udviklingen har været i en given periode.

Som basisrapport for såvel WebScans som SystemScans leveres en Scan Report. Scan Report kan så afhængigt af behov overbygges med et Expert Review eller/og Executive Summary. Det er også muligt at samle det hele i én rapport. Således kan vi skræddersy den løsning der passer bedst til den enkelte kundes behov.

Scan Rapport

nSense Scan Rapport er en automatisk genereret rapport med resultaterne fra den udførte test. Rapporten indeholder alle resultaterne fra scanningen og et kort resumé. Rapporten henvender sig til personer med indsigt i systemet og/eller webapplikationen samt forståelse for de mulige trusler systemet eller webapplikationen kan udsættes for på baggrund af fundne sårbarheder.

Expert Review

Expert Review er en overbygning til ScanReport. nSense leverer en skabelon til udarbejdelse af denne rapport som kræver manuel gennemgang af en sikkerhedsekspert. Expert Review henvender sig således til de virksomheder som ønsker at benytte sig af eksterne sikkerhedseksperter for en manuel og uvildig gennemgang af ScanReport. De fundne sårbarheder vil blive verificeret og vurderet af sikkerhedseksperter, der på denne baggrund skriver en konklusion med eventuelle forslag til forbedringer. nSense Expert Review kan tilbydes af autoriserede nSense-partnere, som har kompetente sikkerhedseksperter med den påkrævede certificering.

Executive Summary

Executive Summary henvender sig til firmaets ledelse. Rapporten indeholder et kort resumé af hele scanningen. Ved hjælp af grafer og tabeller illustreres sikkerhedsniveauet på en nem og overskuelig måde. Disse understøttes af eksempler der adresserer hvilke forretningsmæssige konsekvenser de identificerede sårbarheder eventuelt ville kunne medføre. nSense Executive Summary kan tilbydes af autoriserede nSense-partnere, som har kompetente sikkerhedseksperter med den påkrævede certificering.

Præsentation og yderlig uddybning

Ønskes der en præsentation af rapporten og/eller yderligere dialog omkring rapportens indhold, kan det tilbydes til normale vilkår for køb af konsulentassistance.