Vi undersøger hele virksomhedens angrebsflade og finder de svagheder, som kan føre til omkostningsfulde sikkerhedsbrud.

Få overblik over sårbarheder - før hackeren

Danske virksomheder oplever i stigende grad at blive udsat for cybertrusler og hackerangreb. Et angreb er ofte forbundet med store omkostninger for de virksomheder der rammes. Følgerne af et succesfuldt angreb kan være ganske alvorlige og har typisk langsigtede konsekvenser.

Derfor er det vigtigt at scanne sit it-miljø for sårbarheder jævnligt for at få lukket huller og opdage sårbarheder, inden de bliver udnyttet. NetDesign kan hjælpe med at give et overblik over hvilke sårbarheder, der findes i virksomhendens cyberforsvar og infrastruktur.

Anvendelse

Vi anbefaler at scanningerne udføres regelmæssigt. På den måde opnåes overblik over sårbarheder i netværket, udviklingen kan følges nøje, og der kan reageres før det er for sent. NetDesign tilbyder enkeltstående, variable eller faste skanningsaftaler afhængig af virksomhedens behov.

Når en scanning er gennemført, samles alle resultater og konklusioner i en gennemarbejdet rapport. Her fremlægges vores anbefalinger til, hvilke sikkerhedsmæssige tiltag, der bør iværksættes. Herudover tilbyder vi en hotlineaftale samt sparring med en af vores sikkerhedsspecialister, hvor skanningsresultaterne gennemgåes.

NetDesign tilbyder en række forskellige skanningsværktøjer til afdækning af, hvorvidt forskellige angrebs- og hackingmetoder vil kunne give adgang til kritiske informationer:

- Ekstern Sårbarhedsscanning
- Intern Sårbarhedsscanning
- Penetrationstest
- Webapplikations assessment

Ekstern Sårbarhedsscanning

NetDesigns eksterne sårbarhedsscanning er rettet mod en virksomheds offentlige IP-adresser eller domænenavne, som er tilgængelige fra internettet. Formålet er, at skabe overblik over den eksterne angrebsflade og vise, hvad en potentiel hacker vil kunne få adgang til via internettet. Vi anbefaler, at man udfører en ekstern sårbarhedsscanning minimum en gang i kvartalet.

Intern Sårbarhedsscanning

Denne type sårbarhedsscanning er basal set fuldstændig lig den eksterne. Dog foretages den interne sårbarhedsscanning fra positioner inde på virksomhedens interne netværk rettet mod interne IP-adresser. På den måde skabes et fuldkomment billede af det interne netværk og sårbarheder identificeres på enheder, der ikke kan tilgås eksternt. Vi anbefaler, at der foretages en intern sårbarhedsscanning minimum en gang i kvartalet.

Penetrationstest

En penetrations test (pen-test) er en målbaseret opgave, hvor NetDesigns whitehat hacker udfører et simuleret angreb inden for, et på forhånd aftalt scope. Denne test identificerer ikke nødvendigvis alle sårbarheder der er i virksomheden, men vil i højere grad gå efter de sårbarheder, der kan udnyttes ved et målrettet angreb.

Webapplikations assessment

NetDesigns webapplikations assessments er en gennemgang af virksomhedens webapplikationer og har til formål at finde sårbarheder og uregelmæssigheder. Testen udføres ved hjælp af automatiserede skanninger samt manuelle scripts udviklet specielt til opgaven. Denne fremgangsmåde sikrer et optimalt indblik i, hvordan en hacker ville kunne kompromittere de testede webapplikationer. Vi anbefaler, at der udføres en webapplikations assessment minimum en gang i kvartalet.

NetDesign er en "full service" integrator med fokus på it-sikkerhed som en cirkulær proces ud fra begreberne Assess, Protect, Detect, Respond og React. Vi har det højest certificerede ekspertteam inden for IT-sikkerhed, og giver dig "Peace of Mind", så du kan fokusere på din kerneforretning. Vi rådgiver om end-to-end løsninger, der giver dig størst mulig sikkerhed hele vejen fra risikoanalyse til avancerede sikkerheds løsninger med 24/7 overvågning.

Kontakt os på sikkerhed@netdesign.dk eller ring på +45 2424 9425 for yderligere information.

NetDesign