Sårbarhedsscanning
as a Service

Hvorfor sårbarhedsscanninger?
Cyber-truslerne mod alle typer af virksomheders it-infrastruktur stiger – ligegyldigt hvor man er i verden. Håndtering af sårbarheder er et ansvar der bør tages seriøst, for at infrastruktur og applikationer ikke er sårbare overfor angreb. Det modner it-sikkerheden og gør organisationen mere opmærksomme på sårbarheder. Og så gør det jo ikke noget at revisoren også er glad for at se at der arbejdes struktureret med sårbarheder.

Hvad er en sårbarhedsscanning?
En ekstern sårbarhedsscanning opdager og indsamler information om alle systemer som er direkte forbundet til internettet. For hver enhed (asset) som scanningsapplikationen identificerer, vil den forsøge at finde ud af hvilket operativsystem, der benyttes og hvilken software der er installeret sammen med information om-kring åbne porte og brugerkonti. Inu:it leverer også interne sårbarhedsscanninger – rekvirer mere info herom.

Scanneren vil også forsøge at benytte de kendte standard admin-konti til at logge ind og indsamle endnu flere oplysninger.

Efter alt dette er samlet, vil scanneren sammenligne informationerne op imod en database med kendte sår-barheder, og generere en rapport over de fundne enheder og deres sårbarheder.

Hvor kan inu:it hjælpe?
"Godt så – så står vi med en tyk rapport i hånden. Og hvad så?", spørger I sikkert…
Inu:it hjælper jer med at forstå rapporten og foretage konkrete handlinger baseret på rapportens anbefalinger.

Inu:it benytter en af markedets førende produkter fra it-sikkerhedsfirmaet Tenable til scanning af sårbarheder. Når vi har scannet og fået genereret en rapport, analyserer inu:its sikkerhedsspecialister rapporten og præsenterer de væsentligste anbefalinger for jer til en fast pris.
Lige nu er best practice – og dermed også vores anbefaling – at vi udfører en scanning en gang i kvartalet. Denne frekvens kan naturligvis justeres op og ned efter ønske.

Baseret på konklusionerne kan I eller inu:it foretage de konkrete handlinger, som vi bliver enige om.

Økonomi

	Første scanning Opsætning og første sårbarhedsscanning, udarbejdelse af rapport og anbefalinger	Øvrige Scanninger Sårbarhedsscanning, rapport, anbefalinger	Konkrete actions - baseret på anbefalingerne og efter aftale
Basic - eksempelvis kun én mailserver eller lign	5.995,-	3.995,-	Efter medgået tid
Standard – op til 15 forskellige IP'adresser	9.995,-	4.995,-	
Enterprise – mere end 15 IP'adresser	Lad os tage en snak		

Alle priser ex moms. (Ikke relevant i Grønland)

Vil du vide mere om mulighederne?
.. kontakt Erik

Erik Kristoffersen
Intern IT ansvarlig

M: +45 96 34 55 49
ek@inuit.gl