



Sårbarhedsscan

Sårbarhedsscanning er et vigtigt element i proaktiv sporing og udbedring af sikkerhedsproblemer i netværket.

Håndtering af sikkerhedsrisici er en udfordring for virksomheder i alle størrelser.

Virtuelle platforme, legacy operativsystemer, nye applikationer - det skal være nemt at udveksle oplysninger med alle kunder, leverandører og samarbejdspartnere over hele verden.

I takt med den stigende vækst i digitaliseringen følger stadig flere sårbarheder og hyppigere cyberangreb som udgør en enorm sikkerhedsrisiko.

Vær på forkant med it-truslerne

Regelmæssige sårbarhedsscanninger gør det muligt at rette op på svagheder, før de bliver udnyttet. Dermed er du langt bedre forberedt, når en kendt sårbarhed forsøges udnyttet i et angreb.

Med et KonsensIT sårbarhedsscan får du overblik over alle kendte sårbarheder i netværket - det kan være på patch niveau på operativsystemer, applikationer samt firmware på hardware udstyr.

Vores scanner bliver synkroniseret dagligt, således at alle sårbarhedsscan til enhver tid afspejler de seneste sårbarheder på alle platforme.

Alle de fundne sårbarheder og systemsvagheder bliver klassificeret efter, hvor stor en sikkerhedsrisiko de udgør.

Der genereres en rapport som bliver gennemgået af vores sikkerhedsspecialister, som også vil komme med anbefalinger til at få lukket sårbarhederne.

Vi anbefaler, at der foretages en efterfølgende scanning efter at have patchet alle sårbarheder, samt at der herefter foretages sårbarhedsscan med faste intervaller, minimum hvert halve år.