HVAD ER SÅRBARHEDSSCANNING, OG HVORFOR ER DET VIGTIGT?

Hvad var det sidste firma, du hørte om, som blev hacket? Ved du, hvordan hackerne kom ind?
I langt de fleste tilfælde er det første skridt i et angreb at scanne ofrets systemer for sårbarheder, der kan udnyttes. Moderne organisationer skal regelmæssigt evaluere deres egne systemer, så de proaktivt kan lukke hullerne for at øge sikkerheden.

Kravene til netværkssikkerhed udvikler sig med voldsom hast, og cybersikkerhedsproblemer er en konstant udfordring for organisationer. Regelmæssige sårbarhedsscanninger kan hjælpe med at skabe overblik over svagheder i it-infrastrukturen og beskytte organisationens aktiver.

En omfattende og løbende sårbarhedsvurdering giver værdifuld viden om de digitale aktiver, generelle risici og sikkerhedsfejl, hvilket på den mest kosteffektive måde reducerer sandsynligheden for cyberangreb.

SÅRBARHEDSVURDERING OG HÅNDTERING

Sårbarhedsvurdering – også kaldet sårbarhedsanalyse – er en proces, der identificerer, kvantificerer og analyserer sikkerhedsudfordringer i it-infrastruktur. Sårbarhedsvurderingens primære mål er at afdække eventuelle sårbarheder, der kan kompromittere organisationens samlede sikkerhed og drift., hvilket betyder, at en sårbarhedsanalyse kan hjælpe med at reducere sandsynligheden for succesfulde angreb.

Sårbarhedsvurdering er ikke længere bare en nice-to-have, men en need-to-have for enhver organisation. Endvidere vil mange organisationer være forpligtet til at foretage regelmæssige sårbarhedsvurderinger for at kunne leve op til de stigende compliancekrav, der findes i dag, bl.a. GDPR.

En sårbarhedsscanner vurderer computere, netværk eller applikationer for kendte svagheder. Disse svagheder er sårbarheder, som angribere kan udnytte til at få uautoriseret adgang eller på anden måde forårsage skade. Systemadministratorer patcher konstant systemer for at løse sårbarheder, men indimellem fejler enkelte opdateringer. Sårbarhedsscanninger fanger de glemte opdateringer, ligesom de også fanger fejlkonfigurationer, som udgør et meget stort problem. En fejlkonfiguration er bl.a., når systemindstillingerne er angivet forkert eller uhensigtsmæssigt, hvilket kan føre til sårbarheder. Eksempler på fejlkonfigurationer er bl.a. administrative rettigheder, der ikke er ændret fra standardindstillingerne, porte, der er unødvendigt åbne, og forkerte tilladelser, der giver brugerne adgang, som de ikke burde have.

VIGTIGHEDEN AF SÅRBARHEDSSCANNINGER

Hvis et system mangler opdateringer og er forkert konfigureret, er det meget mere sårbart over for angreb. Det er vigtigt at forstå, at opdateringer ikke nødvendigvis løser fejlkonfigurationer, så et system, der blev implementeret i en forkert konfigureret tilstand, kan forblive fejlkonfigureret på ubestemt tid, hvis ingen nogensinde finder fejlkonfigurationen, selvom systemet bliver opdateret regelmæssigt. En sårbarhedsscanning vil afsløre problemet, så en administrator kan justere systemets konfiguration for at forbedre sikkerheden.

Sårbarhedsscanninger er vigtige, fordi systemer på internettet konstant scannes og angribes. Selvom organisationer ikke kører sårbarhedsscanninger på deres internetorienterede systemer, vil andre gøre det – og ikke nødvendigvis med de bedste intentioner i tankerne. Internettets globale karakter gør det muligt for kriminelle fra fjerne steder at angribe enhver organisations systemer relativt ustraffet, og de scanner altid efter upatchede systemer, som de kan udnytte. Selv hvis der allerede findes en opdatering for en given sårbarhed, kan kriminelle udnytte det vindue, der er, fra sårbarheden bliver kendt, og til en opdatering frigives til at udbedre problemet. Derfor er sikkerhedsopdateringer kritiske og skal foretages hyppigt, og en sårbarhedsscanning vil hjælpe med at afsløre manglende opdateringer, der skal udrulles.

Værdien af sårbarhedsscanning er ikke kun begrænset til systemer med adgang via internettet. Det er også nyttigt at køre sårbarhedsscanninger på interne systemer, så eventuelle problemer, der findes, kan løses. Dette forbedrer sikkerheden på dit interne netværk og kan forhindre en hacker, der har etableret et fodfæste i dit interne netværk, i at flytte sig fra system til system og eskalere sine rettigheder.

ER DU STADIG I TVIVL?

Mens alle kan køre en sårbarhedsscanning, er det fortolkningen af resultaterne, der er nøglen til succesen. Kvaliteten af de genererede resultater varierer fra værktøj til værktøj. Når du har kørt en sikkerhedsscanning, skal du fortolke resultaterne og prioritere, hvad der skal rettes.

Hvis du fortsat er i tvivl om behovet for og værdien af at have det rette sårbarhedsvurderings- og håndteringsværktøj, så kontakt en af BlackstoneOnes Security Sales Advisors, der sidder klar til at give en fyldestgørende demo.

BlackstoneOne leverer markedets mest intuitive og "easy to use" platform til kontinuerlig og automatiseret sårbarhedsvurdering og håndtering. Identificer, prioriter og mitiger sårbarhederne i dit netværk og i dine applikationer med BlackstoneOnes alt-i-en platform.

BLACKSTONEONE SECURITY SALES ADVISORS

Marianne Friedmann
mfr@blackstoneone.net
+45 53 53 19 68

Steven Solfjeld
sso@blackstoneone.net
+45 42 71 83 33

Steen Jensen
sje@blackstoneone.net
+45 81 74 56 77

Mikkel Bjerre
mbj@blackstoneone.net
+45 93 99 91 86