BlackstoneOne.
peace of mind

Sårbarhedsscanning og AI-powered Vulnerability Management

Produktbladet omfatter
Vigtigheden af sårbarhedsscanning
BlackstoneOnes sårbarhedsløsning gennem Vulnerability Management

Kontakt
Tlf: +45 70 209 209
E-mail: salg-dk@blackstoneone.net

Gyldig fra
December, 2023

BlackstoneOne.
peace of mind

Cybersikkerhed er altafgørende

Har I digitale IT-systemer i jeres virksomhed eller organisation? Så bør I have fokus på, hvordan I hurtigt kan få konstateret, om I er i risiko for at lække data eller blive misbrugt på grund af kendte sårbarheder.

I BlackstoneOne tilbyder vi en løsning til at håndtere sårbarheder i jeres digitale infrastruktur gennem scanninger. Vores sårbarhedsscanning identificerer, beskriver og giver guidens til, hvordan I udbedrer de fundne sårbarheder og de medfølgende sikkerhedsudfordringer, som I stilles overfor.

Er I det næste offer?

Virksomheder har aldrig været mere afhængige af it end nu. I takt med teknologiens udvikling, er de medfølgende risici også steget. Antallet af hackerangreb mod danske virksomheder er i 2022 steget med 64% sammenlignet med 2021. Det er en voldsom rekord, som volder store problemer for både virksomheder og organisationer i Danmark. Det voksende antal af hackerangreb har ligeledes affødt en stribe omfattende reguleringer i relation til cyber-sikkerhed, som stiller større krav til landets virksomheder og organisationer.

Når cybertruslen mod virksomheder og organisationer stiger og reguleringen samtidig skærpes, bliver arbejdet med at beskytte og dokumentere sin digitale infrastruktur kun vigtigere. Derfor er der behov for, at I tager handling for at beskytte værdifuld og følsom data i jeres organisation.

Vores kunder rækker fra mindre og snævert specialiserede virksomheder til store private og offentlige organisationer.
Vi tilbyder en platform, som proaktivt, konstant og kontinuerligt scanner jeres systemer og netværk, og som varsler, når nye sårbarheder viser sig. Platformen giver jer et hurtigt og solidt overblik over jeres sårbarheder, og henviser til de nødvendige tiltag og løsninger, så I kan minimere risici i eller omkring jeres it-systemer.
Vores ekspertise for kompleksiteten mellem implementering af hybride miljøer og anvendelse af nyeste teknologier til at sikkerhedsscanne digitale netværk gør, at I ikke skal opbygge dybe IT-kompetencer indenfor informationssikkerhed på dette område.
Vi sikrer, at jeres digitale infrastruktur bygger på et stærkt, robust og trygt fundament og bringer kompleksiteten ved de fundne sårbarheder ned.

+50%

af Danmarks kommuner bruger BlackstoneOne

Maskinrummet skal virke, før styrehuset kan være funktionsdygtigt

Hos BlackstoneOne undersøger vi maskinrummet gennem automatiseret Vulnerability Management, som sikrer en effektiv proces omkring jeres fundne sårbarheder. Vulnerability Management er ikke kun relevant i relation til det stigende trusselsbillede, men stilles også som krav i flere lovmæssige sammenhænge. Bl.a. i:

NIS2 & DORA

NIS2-direktivet er en opstramning til det eksisterende NIS-direktiv, der skal sørge for, at lovgivningen for cyber- og informationssikkerhed i Europa følger med den digitale udvikling. De omfattede sektorer af kravene i NIS2 fremgår her. Sårbarhedsscanninger kan være en måde for organisationer og virksomheder at opfylde, og opnå dokumentation for, minimumskravene i NIS2. DORA-direktivet er en sektorspecifik forordning, som finder anvendelse på enheder inden for den finansielle sektor. DORA dækker over "værktøjer, som er nødvendige for på behørig og effektiv vis at beskytte alle relevante fysiske komponenter og infrastruktur, herunder computerhardware, servere samt alle relevante lokaler, datacentre og sensitive udpegede områder […]" (se artikel 5(2)). DORA-direktivet har et indirekte krav til sårbarhedsscanninger jf. artikel 21 og 22. Kravene i NIS2 og DORA skal sikre et højt, fælles niveau for cyber- og informationssikkerhed på tværs af alle EU-medlemslande. Vulnerability Management er en vigtig del af begge direktiver, da det hjælper organisationer med at identificere og håndtere trusler mod deres systemer og data.

GDPR

GDPR står for General Data Protection Regulation og er en EU-lov, der beskytter persondata for borgere i alle lande, som er medlem af EU. GDPR gælder derfor alle virksomheder og organisationer i EU og forpligter organisationens dataansvarlige til at sørge for, at dens regler overholdes. Det betyder bl.a., at den dataansvarlige skal indtænke databeskyttelse i alt, hvad der foretages i organisationen eller virksomheden. Vulnerability Management er en vigtig del af at overholde GDPR, da det hjælper organisationer med at identificere og beskytte persondata mod trusler og sårbarheder i systemer, der opbevarer og behandler persondata.

NSIS

NSIS er en dansk standard for cyber- og informationsikkerhed og står for National Standard for Identiteters Sikringsniveauer. Formålet med standarden er at skabe en fælles ramme for tillid til digitale identiteter og digitale identitetstjenester gennem en række tekniske og organisatoriske krav. Vulnerability Management er en vigtig del af NSIS, da det hjælper organisationer, som indgår i en tillidskæde, med at beskytte deres it-systemer og data mod cybertrusler. NSIS har derfor en central betydning for identitetsløsninger som MitID og NemLog-in samt en række decentrale løsninger som f.eks. organisationer med en Lokal IdP.

Fremtidens løsning for nutidens trusler

Datatilsynet anbefaler, at sårbarhedsscanninger udføres regelmæssigt for at hindre cyberangreb. Derfor er det ikke tilstrækkeligt kun at udføre sårbarhedsscanninger 2-4 gange om året. Med BlackstoneOne får I automatisk scannet jeres digitale infrastruktur månedligt, hertil tilbyder platformen også 'Automatisk Frekvens Prioritering', så frekvensen af scanninger automatisk øges på sårbare IP-adresser og landingpages (URL) i jeres infrastruktur.
Det betyder, at:

HØJ-RISIKO

Enheder med høj-risiko sårbarheder, vil minimum blive scannet dagligt.

MELLEM-RISIKO

Enheder med mellem-risiko sårbarheder, vil minimum blive scannet hver 4. dag.

LAV-RISIKO

Enheder med lav-risiko sårbarheder, vil minimum blive scannet ugentligt.

Få overblik på alle enheder og reducer risikoen for cyberangreb

For at opretholde et stærkt sikkerhedsniveau er det altafgørende, at I regelmæssigt scanner alle jeres aktive enheder. Derfor udfører vi automatisk månedligt en host discovery i jeres digitale infrastruktur, så vi sikrer, at alle aktive enheder er inkluderede i de igangværende scannings-analyser, nye såvel som tidligere registrerede enheder. På den måde leverer vi et kontinuerligt opdateret og nøjagtigt overblik over de fundne aktuelle sårbarheder, der identificeres på de scannede enheder i jeres IT-infrastruktur. Vores resultater skabes på baggrund af flere scanningsprocesser- og teknologier, som giver et samlet og koncentreret overblik.

> Med BlackstoneOne har vi fanget ting, hvor jeg ikke vidste, hvor galt det kunne være gået.
>
> /Projektleder i Nyborg Forsyning og Service, Kaj Andersen

Hvorfor vælge BlackstoneOne?

Reducerer cybertruslen
Overblik styrker jeres it-sikkerhed og reducerer derved risici i relation til sårbarheder i jeres it-infrastruktur.

Tidsbesparende
I sparer både tid og ressourcer, som kan bruges på andre værdiskabende opgaver.

Understøtter compliance
Understøtter efterlevelsen af compliancekrav, herunder GDPR og NIS2, i forhold til regelmæssige sårbarhedsscanninger i organisationen.

Dansk produceret
Vi ejer, udvikler og vedligeholder selv vores platform, og kan derfor tilbyde nem og hurtig adgang til vores support for at sikre tryghed.

Regelmæssige scanninger
BlackstoneOne sårbarhedsscanninger gennemføres regelmæssigt, da nye sårbarheder kommer til løbende.

Økonomisk fordelagtig
Udover at være ressource- og tidsbesparende, er vores platform fordringsløs. Platformens simplicitet gør, at I ikke skal rekruttere, uddanne og fastholde medarbejdere med dybe IT-tekniske sikkerhedskompetencer.

Fokus på det essentielle
Vores scanninger frasorterer automatisk IP-adresser, hvis de bliver registreret på en URL-scanning, og hermed fremgår samme sårbare enhed ikke flere gange.

AI-forstærket formidling:
Fra kompetence-mangel til kompetence transformation

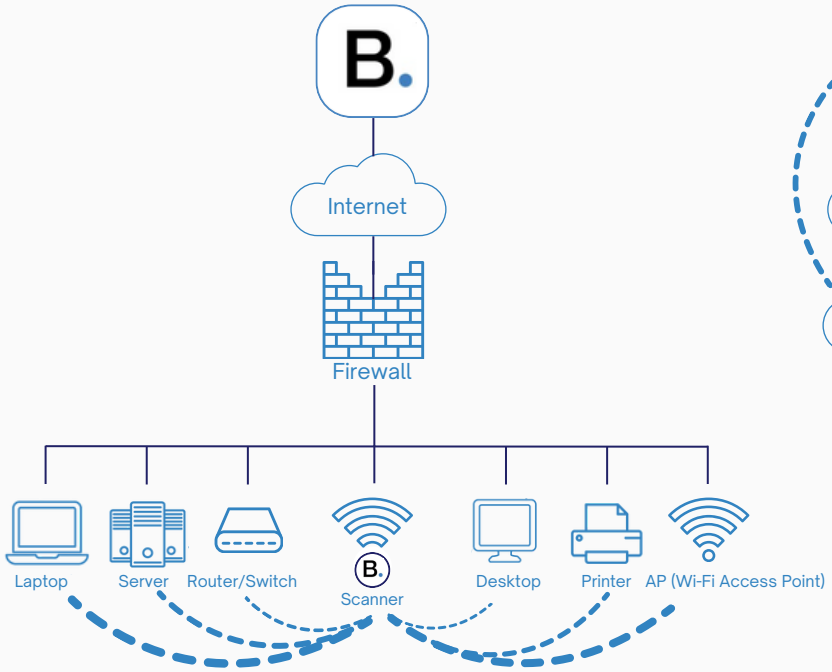
Vi har udviklet en AI-assistent, som I kan benytte, når I anvender vores platform. AI-teknologien er designet således, at den er håndgribelig og nem at gå til. Den hjælper jer med at forstå og håndtere jeres komplekse sårbarheder på en lettilgængelig måde. AI-assistenten fungerer som en co-pilot, der gennemsøger mange kilder for information og giver den optimale beskrivelse og guidens til at udbedre sårbarheder tilpasset det specifikke it-miljø, hvor sårbarheden er fundet. Det åbner således op for en mere præcis og effektiv løsningsproces. AI-assistenten gør det hertil muligt at oversætte, så I nemt kan formidle beskrivelser og løsninger af sårbarheder til relevante systemejere i organisationen.

En særlig relevant feature ved AI-assistenten er også, at I netop kan søge information om specifikke sårbarheder, som vi har fundet i jeres netværk, uden at det er til skue for andre, hvilken virksomhed, I søger fra. Når I bruger vores AI-assistent, gør I altså ikke opmærksom på, hvilke sårbarheder I har. Således fungerer vores AI-assistent, som en proxy I kan benytte jer af, til at få en given information om jeres sårbarheder.

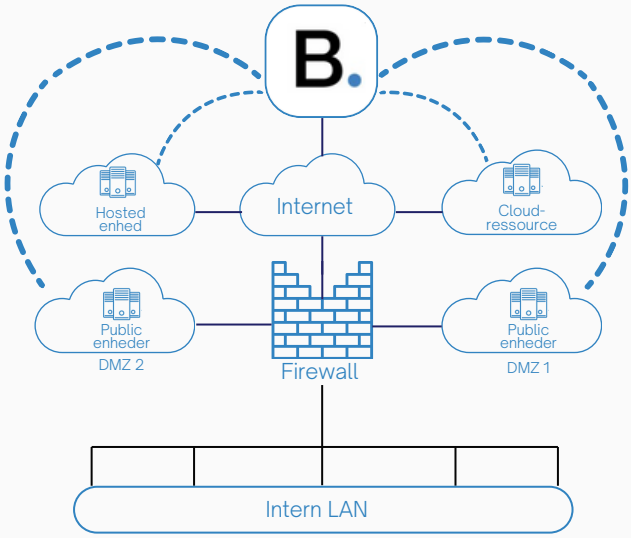
Vi hjælper jer med, at forstå jeres sårbarheder

Sårbarhedsscanninger af BlackstoneOne afdækker kendte sårbarheder og fejlkonfigurationer på jeres interne og eksterne netværk, såsom servere, netværksenheder, printere, webservere og -applikationer.

Intern sårbarhedsscanning



Ekstern sårbarhedsscanning



En intern sårbarhedsscanning udføres via en eller flere scannere opsat i jeres infrastruktur. Scanningerne afdækker sårbarheder, der er eksponeret på jeres interne netværk, såsom interne servere, klienter, printere, IP-telefoner, netværksudstyr og webapplikationer

En ekstern sårbarhedsscanning er koncentreret om organisationens eksterne infrastruktur, såsom webserver og kundeportaler, såvel internetvendte IP-adresser, som websites og landingspages. Ekstern sårbarhedsscanning udføres typisk med kendskab til organisationens IP- og URL-adresser og en eventuel whitelisting, der forhindrer blokering.

NB.
Nogle servere kan tilgås både internt og eksternt, hvorfor det er vigtigt at scanne både internt og eksternt.

De identificerede sårbarheder tilgås via BlackstoneOne-portalen. Her findes der detaljerede beskrivelser af sårbarhederne, som eksempelvis kan omhandle manglende patch-niveau på operativsystemet, installeret tredjeparts-software eller anbefalede konfigurationstilpasninger.

Vores mission og kerneværdier

Et aktuelt overblik

Med BlackstoneOne har I et opdateret overblik over jeres sårbarheder.

Brugervenligt

BlackstoneOne er en tidsbesparende og intuitiv løsning med fokus på brugervenlighed, og som ikke kræver teknisk snilde.

Brugeradministreret

Med BlackstoneOne sikrer I, at den enkelte bruger får de rette informationer.

Brugerindflydelse

Vi vægter brugerindflydelse højt, og videreudvikler konstant ud fra kunders behov og ønsker.

Book en demo og læs meget mere på: www.blackstoneone.net

BlackstoneOne.
peace of mind