White Paper

Erhvervslivets afhængighed af sikre slutpunkter

Sponsoreret af: Apple

Tom Mainelli Michael Suby
September 2023

IDC-ANALYSE

Hvad får IT-beslutningstagere (ITDM'er) til at ligge vågne om natten? Sikkerhed. Det skyldes, at dygtige ITDM'er er klar over, at, uanset hvor veldrevet en virksomhed er, eller hvor eftertragtet et produkt eller en service de tilbyder, kan hele virksomheden komme i fare fra den ene dag til den anden, hvis sikkerheden svigter.

Og desværre ser verden ikke ud til at blive et mere sikkert sted. Virksomhedsspionage, slyngelstater, organiseret kriminalitet og endda almindelige tyve er alle blevet mere avancerede, når det gælder teknologi. For at bevare forspringet foran hackerne skal IT-afdelinger være på vagt og villige til at favne nye leverandører og implementere nye teknologier for at beskytte medarbejdere, kunder og data.

Listen over sikkerhedsudfordringer for IT-afdelinger er lang og omfatter alt fra slutpunkter (computere) til datacentre, de netværk, der forbinder alting, og den software, der kører det hele. I denne hvidbog fokuserer vi på vigtigheden af sikre slutpunkter. Det skyldes, at når det kommer til stykket, betyder sikkerheden på tværs af alle de andre domæner meget lidt, hvis slutpunktet ikke er sikkert.

En af de største udfordringer i forbindelse med sikring af slutpunktet består i, at et sikkert slutpunkt traditionelt ofte medfører en ringere slutbrugeroplevelse med låste enheder, der er besværlige at bruge. Og når det er tilfældet, finder det andet primære svage punkt i enhver sikkerhedsplan – nemlig brugeren – ofte metoder til at omgå denne sikkerhed med henblik på at få arbejdet fra hånden. Når sikkerheden skaber friktion i forhold til brugerne, tjener den ikke længere sit formål.

Teknologiske fremskridt giver stadigt bedre muligheder for at bevare en brugeroplevelse i høj kvalitet, samtidig med at sikkerheden opretholdes. Fremskridt inden for malwareregistrering, databeskyttelse, godkendelse og fletningen af processorer og software betyder, at man med moderne slutpunkter ikke behøver at på kompromis med produktiviteten for at øge sikkerheden.

METODIK

IDC gennemførte en onlineundersøgelse blandt IT-beslutningstagere (ITDM'er) i USA og Canada (n=513) i juli 2023 om deres holdning til sikkerhed overordnet og vigtigheden af at sikre computerslutpunkter specifikt. Respondentpuljen repræsenterer en blanding af virksomheder med 500 medarbejdere eller derover fra en række forskellige brancher. Disse ITDM'er understøtter en blanding af computeroperativsystemer, herunder Microsoft Windows, Apple macOS og Google ChromeOS. De enten vælger, køber eller udruller sikkerhedssoftware til deres virksomhed, eller de er ledere for medarbejdere, der gør det.

September 2023, IDC-nr.US51204723

SITUATIONSOVERSIGT

Sikkerheden er fortsat en absolut nødvendighed for ledere. Fremsynede virksomheder anerkender, at god sikkerhed ikke bare er "rar at have", men snarere en forudsætning for en sund virksomhed i fremgang, der driver forretning i et trusselsmiljø i konstant udvikling drevet af koordinerede og kapitalstærke hackere.

Ifølge IDC's undersøgelse fra marts 2023 "Future Enterprise Resiliency and Spending Survey (FERS)" af erhvervs-ITDM'er i virksomheder med 500 medarbejdere eller derover havde over 50 % af de adspurgte virksomheder verden over været udsat for et driftsforstyrrende ransomwareangreb inden for de sidste 12 måneder. Over en tredjedel i denne gruppe fortalte, at angrebet afbrød driften i en uge eller mere. Større virksomheder har utvivlsomt mere robuste sikkerhedsprotokoller, men de er langt fra immune over for sådanne angreb. Faktisk gik den højeste procentdel af driftsforstyrrelser pga. ransomware ud over virksomheder i kategorien med 1.000 til 2.499 medarbejdere (71 %), 2.500 til 4.999 medarbejdere (72 %) og 5.000 til 9.999 medarbejdere (70 %). Med andre ord er ingen virksomheder, uanset størrelse, immune over for denne type angreb.

Den samme undersøgelse peger på slutpunkter som det største adgangspunkt ved ransomwareangreb. Primære kompromitteringspunkter omfatter internetsøgning (21 %), flytbare medier (18 %), vedhæftninger i e-mails (17 %), forsyningskæder (17 %), URL-adresser i e-mails (14 %) og insideradgang (8 %).

Det vedvarende skift hen mod flere medarbejdere med arbejde i hybrid- og fjernmiljøer har kun øget udfordringen ved ransomware og andre sikkerhedsrisici for IT-afdelinger. IDC's undersøgelse fra december 2022 "Endpoint Security Survey" viste, at over 97 % af de adspurgte organisationer havde et antal fjernarbejdere. Selvom dette tal forventes at falde en del i løbet af det næste år, vil det forblive meget højt i den nærmeste fremtid.

I virksomhedernes håndtering af de vedvarende udfordringer ved en stor ekstern arbejdsstyrke implementerer flere zero trust-strategier. Fokusområder for bedste praksis omfatter etablering af grundlæggende sikkerhedskontroller, avanceret forsvar til slutpunktssikkerhed, enhedsattester (bekræftelse af, at enheder, der opretter forbindelse til netværket, er legitime) og stærk brugergodkendelse.

Når man tager alt det ovenstående med i betragtning, er det ikke overraskende, at respondenterne i vores undersøgelse overvejende udpegede forbedring af den overordnede datasikkerhed og sikring af computere som deres vigtigste IT-prioriteter, som det fremgår af figur 1.

Det er værd at bemærke i figuren nedenfor, at den tredjevigtigste faktor for IT-afdelingerne var forbedring af medarbejdernes produktivitet gennem bedre enheder. Da vi bad respondenterne om at vælge deres tre vigtigste faktorer overordnet, valgte de hyppigst muligheden "bedre enheder". Dette understreger et vigtigt budskab, som IT-afdelinger bør huske: Sikkerheden er vigtig, men den må ikke indføres på bekostning af medarbejdernes produktivitet, og de bedste enheder tilbyder en kombination af stærk sikkerhed og slutbrugertilfredshed, der ikke hæmmes af denne sikkerhed.

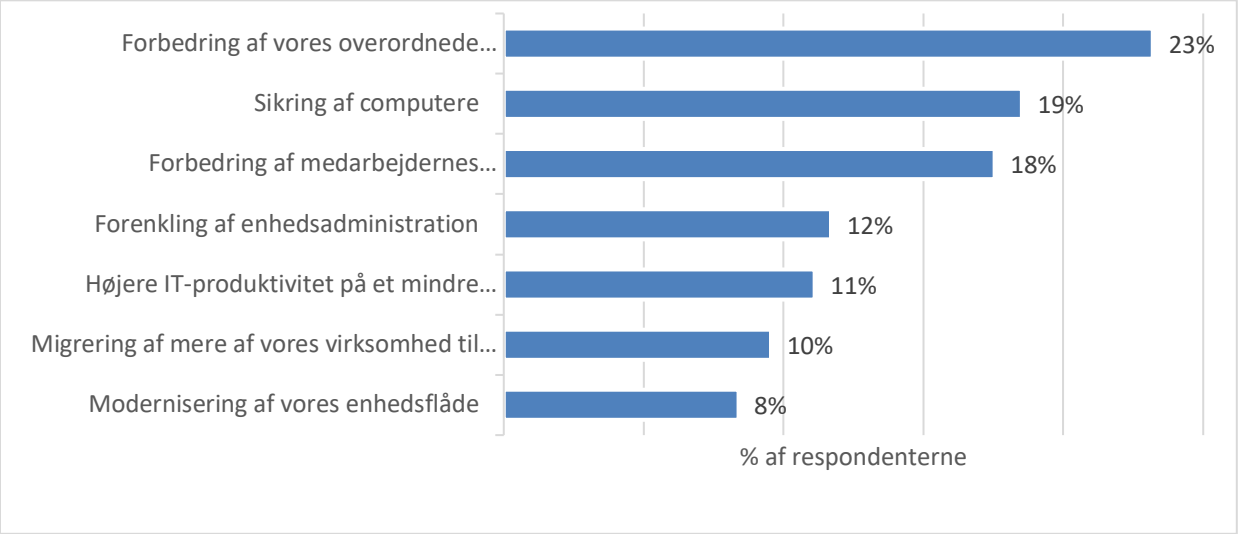
Da vi spurgte ITDM'er, hvad den afgørende faktor var i valget af deres næste computerleverandør, tog sikkerhed førstepladsen foran ydeevne, understøttelse af eksisterende programmer og integration med eksisterende IT-infrastruktur. Men måske mest bemærkelsesværdigt var det, at specifikationer befandt sig nederst på listen.

Se figur 1 for at få en oversigt over IT-afdelingernes højeste prioriteter. Se figur 2 for at få en oversigt over de vigtigste overvejelser i valget af computerleverandør.

FIGUR 1

IT-afdelingers højeste prioriteter: Data- og slutpunktssikkerhed

Sp. Hvilke af følgende IT-faktorer prioriteres højt i din virksomhed i dag?



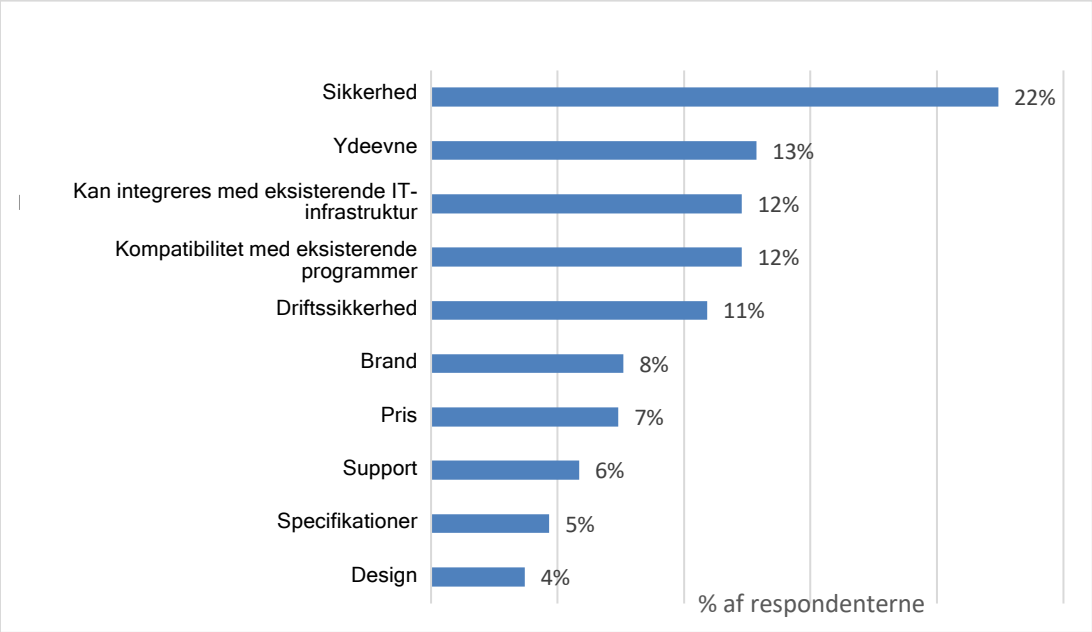
Kilde: IDC's undersøgelse Secure Endpoint Survey, n=513

Bemærk: Data omfatter faktorer, der rangerer som vigtigst (rangeret som nr. 1)

FIGUR 2

Vigtigste faktorer i valget af computerleverandør

Sp. Hvad er de afgørende faktorer, når du skal vælge en computer til din virksomhed?



Kilde: IDC's undersøgelse Secure Endpoint Survey, n=513

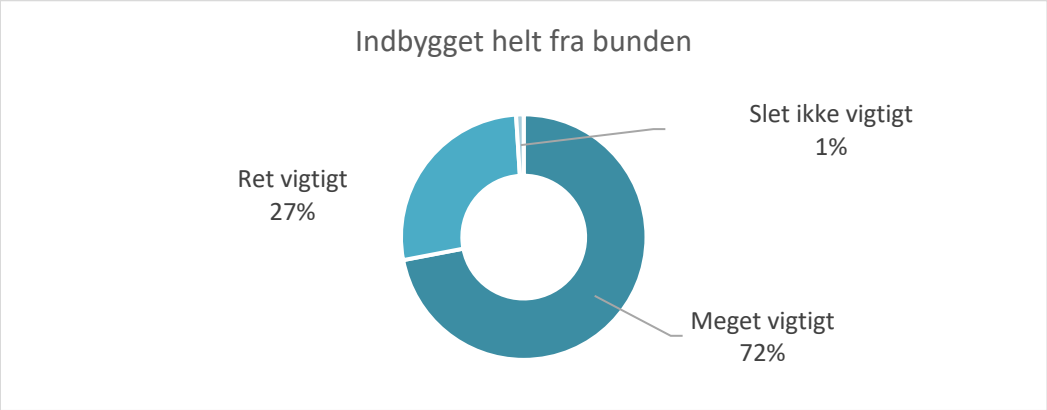
Bemærk: Data omfatter faktorer, der rangerer som vigtigst (rangeret som nr. 1)

To koncepter, der havde stor betydning for respondenterne, var indbygget sikkerhed og integreret databeskyttelse. Respondenterne fik spørgsmålet: "Hvor vigtigt, vil du sige, det er at have sikkerhed indbygget i en computer helt fra bunden – herunder processoren, firmwaren og operativsystemet – for at beskytte den mod eksisterende trusler og for at foregribe fremtidens trusler?" Og svaret var overvældende positivt, idet 72 % sagde, at det var meget vigtigt, og 27 % sagde, at det var ret vigtigt. Kun 1 % sagde, at det slet ikke var vigtigt. Når man dykker ned i dataene, er det værd at bemærke, at blandt ITDM'er inden for sundhedspleje og organisationer i finanssektoren var procentdelen, der sagde, at det var meget vigtigt, endnu højere (hhv. 84 % og 75 %). Konceptet integreret databeskyttelse scorede ligeledes højt. Vi spurgte: "Hvor vigtigt, vil du sige, det er at have datakrypteringsfunktioner integreret i computerhardwaren?" 71 % sagde, at det var meget vigtigt, 29 % sagde, at det var ret vigtigt, og 0 % sagde, at det ikke var vigtigt. Se figur 3 for at få en oversigt over indbygget sikkerhed og integreret datakryptering.

FIGUR 3

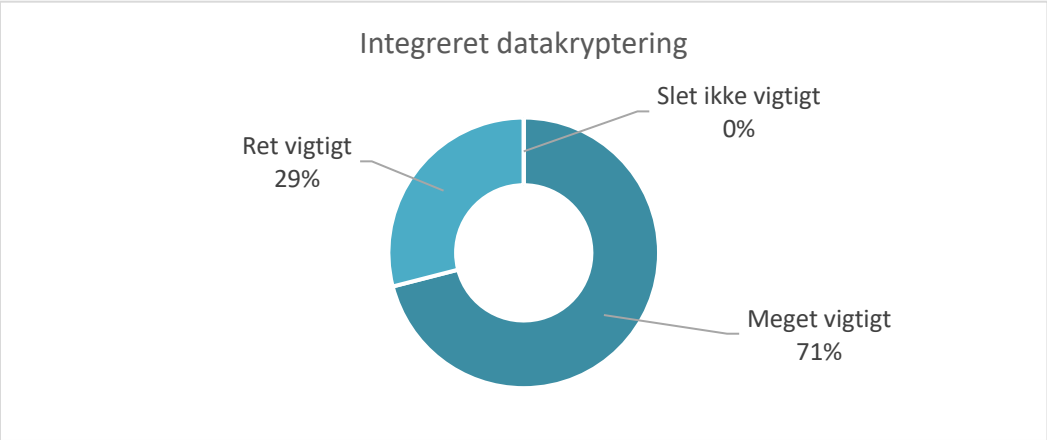
Vigtigheden af indbygget sikkerhed og integreret datakryptering

Sp. Hvor vigtigt, vil du sige, det er at have sikkerhed indbygget i en computer helt fra bunden – herunder processoren, firmwaren og operativsystemet – for at beskytte den mod eksisterende trusler og for at foregribe fremtidens trusler?



Kilde: IDC's undersøgelse Secure Endpoint Survey, n=513

Sp. Hvor vigtigt, vil du sige, det er at have datakrypteringsfunktioner integreret i computerhardwaren?



Kilde: IDC's undersøgelse Secure Endpoint Survey, n=513

Selvom hardware med sikkerhed, der er indbygget fra bunden, er vigtigt, og integreret datakryptering er et centralt krav, ved sikkerhedseksperter, at det svageste led i en sikkerhedskæde typisk er slutbrugerne selv. Derfor er brugergodkendelse så vigtigt, og derfor har teknologileverandører arbejdet målrettet på at udvikle forholdene for godkendelse. Dette er desværre et område, hvor vores undersøgelse viser, at mange organisationer halter bagefter.

På plussiden viser undersøgelsen, at 68 % af respondenterne sagde, at deres virksomhed kræver komplekse adgangskoder, og 63 % sagde, at de benytter tofaktorgodkendelse. Til gengæld benytter kun 23 % enkeltlogon-teknologier (SSO), og kun 20 % benytter biometrisk sikkerhed (f.eks. fingeraftryks- eller ansigtsidentifikation). Det er værd at bemærke, at blandt vores respondenter sagde 56 %, at biometrisk godkendelse var meget mere sikkert end adgangskoder, 35 % sagde, at det var lidt mere sikkert, mens 9 % sagde, at det var lige så sikkert, og ingen (0 %) sagde, at det var mindre sikkert.

For nylig så en vigtig ny godkendelsesteknologi dagens lys, nemlig adgangsnøglen. En adgangsnøgle er digitale legitimationsoplysninger, der benytter et nøglepar til at levere en mere sikker løsning end en adgangskode. Eftersom teknologien er ny, sagde blot 14 % af respondenterne, at deres virksomheder bruger den, men forudseende ITDM'er bør se nærmere på teknologien i dag. Se figur 4 for at få en oversigt over brug af brugergodkendelse.

FIGUR 4

Metoder til brugergodkendelse

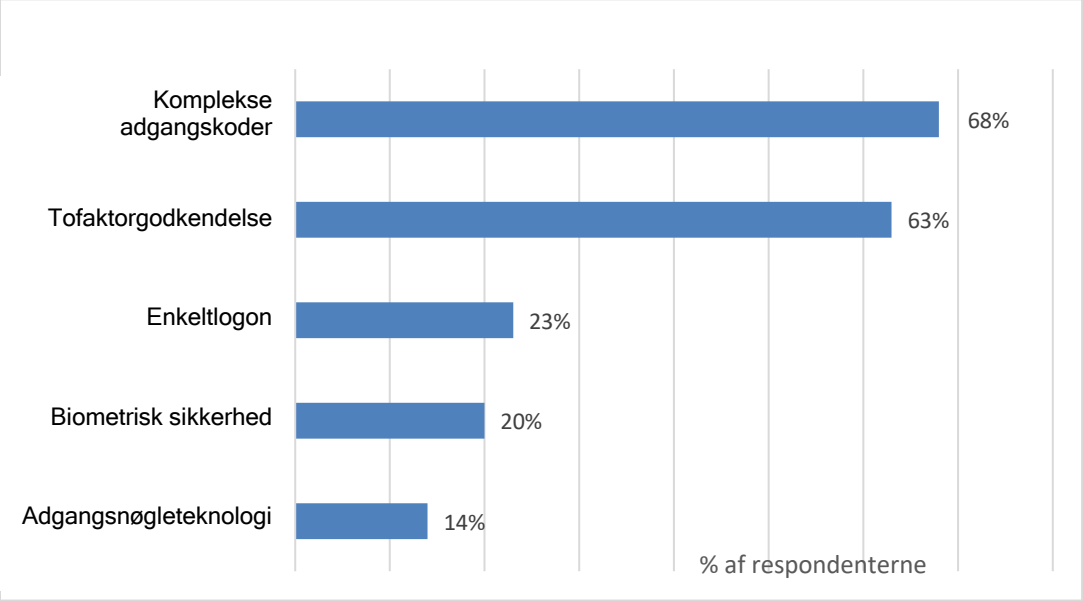
Sp. 1. Kræver din virksomhed, at medarbejdere bruger komplekse adgangskoder til at logge på deres computer?

Udruller din virksomhed computere, der understøtter biometriske sikkerhedsforanstaltninger som f.eks. scanning af fingeraftryk?

Sp. 3. Er din virksomhed begyndt at undersøge fordelene ved at bruge adgangsnøgleteknologi?

Sp. 4. Kræver din virksomhed tofaktorgodkendelse?

Sp. 5. Benytter din virksomhed enkeltlogon-funktionalitet (SSO)? (J/N)



Kilde: IDC's undersøgelse Secure Endpoint Survey, n=513

Data angiver procent, der svarer "ja"

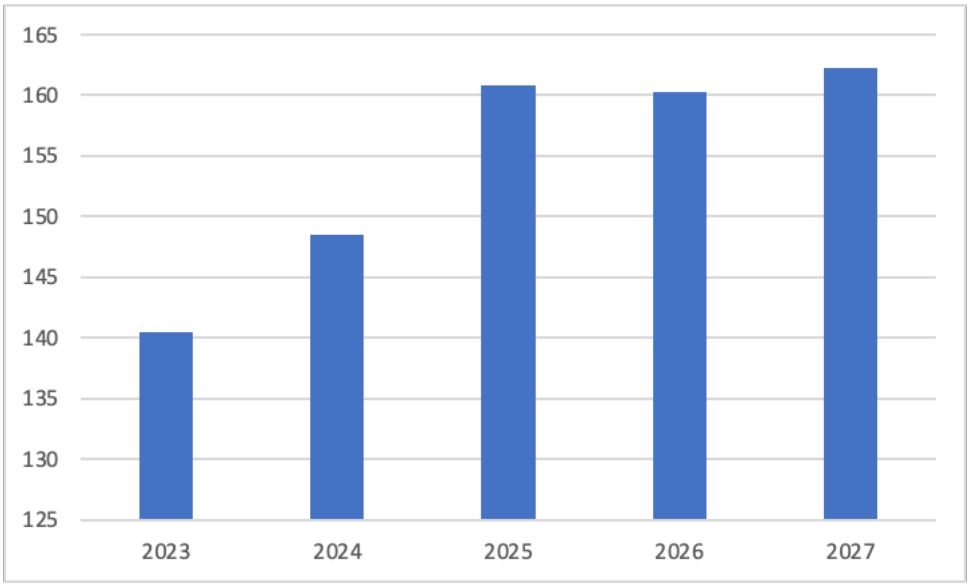
Blandt respondenterne havde en chokerende høj procentdel ikke engang implementeret helt elementære godkendelsesprotokoller med komplekse adgangskoder (32 %) eller tofaktorgodkendelse (37 %). **Det er værd at forfølge en bedste praksis**, som sikrer, at din virksomhed har implementeret en ensartet form for godkendelse i hele organisationen. Når disse elementære protokoller er etableret, kan du begynde at overveje SSO-funktioner kombineret med en stærk mastergodkendelsesprotokol. Til slut bør du, når du gennemfører din næste hardwareopdatering, se nærmere på computere, der understøtter de højeste godkendelsesniveauer: biometrisk sikkerhed og adgangsnøgleteknologi. Aktivering af biometriske data og adgangsnøgler er ensbetydende med en fremtid, hvor medarbejdere hurtigt og sikkert kan logge på deres computere og derfra direkte på deres apps og websteder.

Med dette sidste punkt – din næste hardwareopdatering – runder vi dette afsnit af. Mange virksomheder har en flåde af aldrende computere installeret, og disse bør udskiftes. Selvom din organisation har købt en stor procentdel nye slutpunkter så sent som i 2020, nærmer disse computere sig hastigt fireårsgrænsen. Hen over denne periode har hardwaresikkerheden fortsat udviklet sig til at kunne

håndtere truslerne på stedet. Det er måske lige så væsentligt, at de fleste af disse produkter blev leveret inden det udbredte skift i retning af fjern- og hybridarbejde, hvilket betyder, at mange af dem mangler de kvalitetskameraer, -mikrofoner og -højttalere, som er nødvendige for, at medarbejderne kan gøre brug af de webkonferencer og samarbejdsapps, der er blevet så vigtige. Efter flere års fald i forsendelserne forudser IDC's Personal Computing Device Tracker vækst i kategorien hen over den næste årrække. Bemærk: Kommercielle computere repræsenterer computere, der købes af andre enheder end forbrugere. Se figur 5 for at få en oversigt over IDC's prognose for forbrugercomputere/kommercielle computere.

FIGUR 5

Prognose for kommercielle computere på verdensplan



Kilde: IDC PCD Tracker, august 2023

Virksomheder bør løbende reevaluere medarbejdernes computerbehov for at forblive konkurrencedygtige på markedet og tiltrække og fastholde dygtig arbejdskraft. Mens IT-afdelinger tidligere var tvunget til at afveje balancen mellem sikkerhed og medarbejdertilfredshed, kan den rette leverandør i dag hjælpe med at finde en løsning uden behov for kompromis. Endelig bør man **overveje endnu en bedste praksis**, der består i at indføre principper for zero trust-adgang i forbindelse med den næste hardwareudrulning. Denne strategi antager, at når en enhed forsøger at tilgå en virksomhedsressource, får den ikke adgangstilladelse, før den er bekræftet. Zero trust anvender teknologier og processer, der attesterer til enhedens sikkerhedstilstand (optimalt fra processorniveau op til og gennem kritiske IT- og sikkerhedsprogrammer), forbindelse til netværk (f.eks. offentligt wi-fi vs. privat netværk) og brugeridentitet.

Overvejelse af Mac i virksomheden

Flere IT-afdelinger understøtter Mac-computere i dag, og vores undersøgelse peger på en vigtig forklaring på dette. Blandt

vores respondenter, der repræsenterede en blanding af operativsystemer i deres installerede flåde, sagde 76 %, at de mener, at Mac-computere er mere sikre end andre computere. Og i løbet af de næste 12 måneder var den primære årsag til at indføre flere Mac-computere, at de mente, at Mac-computere er mere sikre (47 %), tæt efterfulgt af nem udrulning og administration (36 %).

Apple-kundefokus

"En af de virkelig vigtige egenskaber i Apple-produkter er, at anonymitet og sikkerhed faktisk er integreret i selve produktet. Det er ikke en eftertanke, og det er noget, vi sætter stor pris på." – Linda Jojo, Executive Vice President og Chief Customer Officer, United Airlines

Apple fokuserer på at levere en enestående brugeroplevelse, samtidig med at sikkerheden øges gennem integration af den i Apple Silicon hele vejen op gennem softwaren. Et eksempel på dette er Apples Touch ID, en indbygget biometrisk sikkerhedsfunktion. Apple Silicon har Secure Enclave, som krypterer og beskytter den adgangskode, der bruges til at beskytte Touch ID-data.

Mac-computere håndterer risikoen for kompromitterede OS- og bootsekvenser og er udstyret med Sikker start og Signeret systemenhed. Sikker start sørger for, at kun den kryptografisk certificerede version af macOS køres ved opstart, og Signeret systemenhed beskytter operativsystemets integritet under afviklingen. Forældet software udgør også en cyberrisiko, som Apple minimerer ved at automatisere og sikre end-to-end-distribution og -installation af softwareopdateringer.

Robust tredjepartssoftware er afgørende for medarbejdernes produktivitet, men softwaren skal også være fri for malware. Apple har en tilgang med flere lag til forebyggelse af malware. Apples Mac App Store scanner alle apps for malware. Software til Mac-computere kan også downloades fra internettet, og derfor kræver Apple, at udviklere indsender deres apps til Apples notartjeneste, som også scanner for malware. Apples Gatekeeper, der er inkluderet i macOS, kontrollerer for notarisering og forhindrer usignerede apps i at køre. Desuden blokerer og fjerner XProtect – Apples antimalwareværktøj – al kendt skadelig software.

Data er blandt en organisations mest dyrebare aktiver, og de skal beskyttes derefter. Kombinationen af hardwarehåndhævet FileVault-kryptering, Apple-understøttede VPN-protokoller og end-to-end-kryptering i Apple-tjenester (f.eks. iMessage og iCloud) sikrer, at data beskyttes, når de er inaktive, under transport og under brug.

Social engineering er en finpudset færdighed blandt hackere, og det betyder, at slutbrugere altid skal være på vagt. Det er et stort ansvar, men Apple hjælper med at løfte opgaven takket være Advarsel om bedragerisk websted i Safari. Desuden er legitimationsoplysninger til godkendelse ofte et mål for hackere, så Apples understøttelse af adgangsnøgler gør det lettere for organisationer at modernisere deres godkendelsesmetoder – igen uden at skulle gå på kompromis med den positive slutbrugeroplevelse.

God sikkerhed hænger sammen med robust enhedsadministration. Til det formål tilbyder Apple en række funktioner til enhedsadministration, herunder indbygget MDM-framework (Mobile Device Management). Apple Business Manager muliggør berøringsfri udrulning og linker til MDM-løsninger, mens API'er til slutpunktssikkerhed til Mac sætter udviklere i stand til at udvikle løsninger, der overvåger, analyserer og reagerer på sikkerhedstrusler. Apple tilbyder også identitetsintegrationer med et indbygget SSO-framework, der fungerer sammen med moderne identitetsudbydere (IdP'er).

Endelig tilbyder Apple disse sikkerhedsfunktioner, herunder både større og mindre softwareopdateringer, med macOS uden yderligere omkostninger for erhvervs- eller forbrugerkunder.

UDFORDRINGER/MULIGHEDER

På trods af et trusselsmiljø i konstant udvikling udfordres IT-afdelinger til at udrette mere med færre midler: færre penge, færre IT-medarbejdere og færre ressourcer. Ud over at håndtere de løbende sikkerhedsrisici, som det kræves af enhver virksomhed, har mange IT-organisationer også fået til opgave at forbedre medarbejdernes produktivitet og tilfredshed målbart gennem den hardware, den software og de tjenester, de implementerer. Det kan virke uoverkommeligt at løse begge opgaver – forbedring af sikkerheden såvel som medarbejdernes produktivitet og tilfredshed. Men samtidig repræsenterer det en vigtig mulighed for IT-afdelingerne. En mulighed for at revurdere den hardware, den software og de tjenester, der indkøbes, de leverandører, der vælges, og hvordan de implementerer dem i en stadigt mere hybrid arbejdsstyrke. Desuden er det klart på tide at omberegne modellerne for samlede ejeromkostninger (TCO), så de bedre afspejler, hvordan virksomheder indkøber og bruger teknologi i dag.

KONKLUSION

Sikkerhed er og vil fortsætte med at være et vigtigt anliggende for IT-afdelinger. På et tidspunkt, hvor IT-budgetter er små, og der er en markant hardwareopdatering om hjørnet, er det en god idé at revurdere, hvilke leverandører man vil lægge pengene hos fremadrettet. Overvej at implementere bedste praksis for godkendelse og berøringsfri udrulninger, og køb hardware, der gør disse omlægninger mulige. Der er ingen grund til at prioritere sikkerheden højere end produktiviteten og medarbejdertilfredsheden, når der findes leverandører, som tilbyder computere med indbygget sikkerhed og datakryptering, og som garanteret leverer både sikkerhed og en positiv slutbrugeroplevelse.

Om IDC

International Data Corporation (IDC) er den førende globale udbyder af markedsundersøgelser, rådgivningstjenester og arrangementer på markedet for informationsteknologi, telekommunikation og forbrugerteknologi. IDC hjælper IT-fagfolk, forretningsledere og investeringssamfundet med at tage faktabaserede beslutninger om teknologikøb og forretningsstrategi. Mere end 1.100 IDC-analytikere tilbyder regional og lokal ekspertise inden for teknologi- og branchemuligheder og -tendenser i over 110 lande verden over. I 50 år har IDC leveret strategisk indsigt, der hjælper vores kunder med at nå deres centrale forretningsmæssige mål. IDC er et datterselskab af IDG, der er verdens førende selskab inden for teknologimedier, -forskning og -arrangementer.

Globalt hovedkvarter

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com