Whitepaper

De zakelijke noodzaak van veilige eindpunten

Gesponsord door: Apple

Tom Mainelli Michael Suby
September 2023

DE MENING VAN IDC

Waarvan liggen IT Decision Makers (ITDM's) 's nachts wakker? Beveiliging. Slimme ITDM's weten namelijk dat hoe goed een bedrijf ook georganiseerd is of hoe populair de producten of diensten van dat bedrijf ook zijn, het hele bedrijf in één klap gevaar kan lopen als de beveiliging het laat afweten.

En helaas wordt de wereld er niet veiliger op. Bedrijfsspionage, schurkenstaten, georganiseerde misdaad en zelfs gewone dieven beschikken tegenwoordig allemaal over steeds betere technologie. Om kwaadwillenden voor te blijven, moet IT op zijn hoede blijven en constant bereid zijn om voor nieuwe leveranciers en technologieën te kiezen als ze medewerkers, klanten en gegevens veilig willen houden.

De lijst met beveiligingsuitdagingen waarmee IT wordt geconfronteerd is lang en bevat alles van endpoints (computers) tot datacentra, de netwerken die alles met elkaar verbinden en de software die zorgt dat alles werkt. In dit document richten we ons op het belang van de beveiliging van die endpoints. De reden daarvoor is dat het beveiligen van al die andere gebieden uiteindelijk weinig betekent als de endpoints niet veilig zijn.

Een van de belangrijkste uitdagingen van het beveiligen van endpoints is dat, traditioneel gezien, een veilige endpoint vaak een negatieve impact heeft op de ervaring van de eindgebruiker doordat afgeschermde apparaten lastig te gebruiken zijn. En wanneer dat het geval is, vindt de andere belangrijke zwakke plek in elk beveiligingsprogramma, de gebruiker, vaak manieren om die beveiliging te omzeilen vanuit de motivatie om het werk gedaan te krijgen. Wanneer beveiliging een knelpunt wordt voor gebruikers, dient het niet langer zijn doel.

Dankzij technologische vooruitgang is het steeds beter mogelijk om een goede gebruikerservaring te combineren met een goede beveiliging. Vooruitgang op het gebied van malwaredetectie, gegevensbescherming, authenticatie en het combineren van chips en software betekenen dat de endpoints van nu niet hoeven in te leveren op productiviteit voor een verbeterde beveiliging.

METHODOLOGIE

In juli 2023 organiseerde IDC een online onderzoek onder IT Decision Makers (ITDM's) in de Verenigde Staten en Canada (n=513). Daarin werden ITDM's gevraagd naar hun mening over beveiliging in het algemeen en het belang van het beveiligen van computer-endpoints in het bijzonder.

September 2023, IDC #US51204723

De respondenten vertegenwoordigen een mix van bedrijven met 500 medewerkers of meer uit verschillende sectoren. Deze ITDM's ondersteunen verschillende besturingssystemen, waaronder Microsoft Windows, Apple macOS en Google ChromeOS. Ze zijn zelf verantwoordelijk voor het selecteren, aankopen of uitrollen van beveiligingssoftware voor hun bedrijf of ze managen mensen die dat doen.

DE SITUATIE

Beveiliging blijft een noodzaak voor het management. Vooruitziende bedrijven realiseren zich dat een goede beveiliging geen 'nice to have' is maar een vereiste voor een gezond bedrijf dat actief is in een wereld waar dreigingen constant veranderen, aangedreven door gecoördineerde en goed gefinancierde kwaadwillenden.

Volgens de Future Enterprise Resiliency and Spending Survey (FERS) van IDC uit maart 2023 onder ITDM's die werken bij bedrijven met 500 medewerkers of meer, heeft 50% van de wereldwijd ondervraagde bedrijven in de afgelopen 12 maanden te maken gehad met een ontwrichtende ransomware-aanval. Meer dan een derde van die groep gaf aan dat de aanval de activiteiten met meer dan een week of langer ontwrichtte. Hoewel ze vermoedelijk beschikken over robuuste beveiligingsprotocollen, zijn grotere bedrijven verre van immuun voor dergelijke aanvallen. Het is zelfs zo dat het hoogste percentage ontwrichtingen door ransomware bedrijven trof met 1000-2499 medewerkers (71%), 2500-4999 medewerkers (72%) en 5000-9999 medewerkers (70%). Met andere woorden, hoe groot ze ook zijn, geen enkel bedrijf is immuun voor dergelijke aanvallen.

Datzelfde onderzoek toonde ook aan dat endpoints de belangrijkste ingang vormen voor aanvallen met ransomware. Punten waar het in eerste instantie misgaat, zijn surfen op het web (21%), verwisselbare media (18%), e-mailbijlages (17%), toeleveringsketen (17%), URL's in een e-mail (14%) en toegang door mensen binnen het bedrijf zelf (8%).

De voortdurende verschuiving naar meer medewerkers die werken in hybride- of thuiswerkconstructies heeft er alleen maar voor gezorgd dat ransomware en andere beveiligingsrisico's een nog grotere uitdaging vormen voor IT. De Endpoint Security Survey van IDC uit december 2022 gaf aan dat bij meer dan 97% van de organisaties een deel van de medewerkers op afstand werkt. Hoewel het de verwachting is dat dat aantal in de komende 12 maanden wat zal afnemen, zal het voorlopig nog erg hoog blijven.

Terwijl bedrijven worstelen met de uitdagingen van grote aantallen medewerkers die op afstand werken, implementeren steeds meer bedrijven zero-trust-strategieën. Best practice-gebieden zijn onder andere het vaststellen van een baseline van beveiligingscontroles, geavanceerde verdediging van endpoints, attestatie van apparaten (ervoor zorgen dat apparaten die verbinding maken met het netwerk legitiem zijn) en sterke gebruikersverificatie.

Rekening houdend met het bovenstaande, mag het geen verrassing zijn dat deelnemers aan ons onderzoek in groten getale het verbeteren van de algehele gegevensbeveiliging en ervoor zorgen dat computers veilig zijn, selecteerden als hun belangrijkste IT-prioriteiten. Dit wordt weergegeven in figuur 1.

Het is waard om te melden dat in de onderstaande figuur het op twee na belangrijkste onderwerp voor IT het verbeteren van de productiviteit van werknemers door middel van betere apparaten was. Toen we respondenten vroegen hun belangrijkste drie onderwerpen te selecteren, werd betere apparaten

het vaakst geselecteerd. Dit benadrukt een belangrijke boodschap voor IT: Beveiliging is belangrijk, maar mag niet ten koste gaan van de productiviteit van werknemers. De beste apparaten bieden een combinatie van goede beveiliging en tevredenheid van de eindgebruiker die niet wordt belemmerd door die beveiliging.

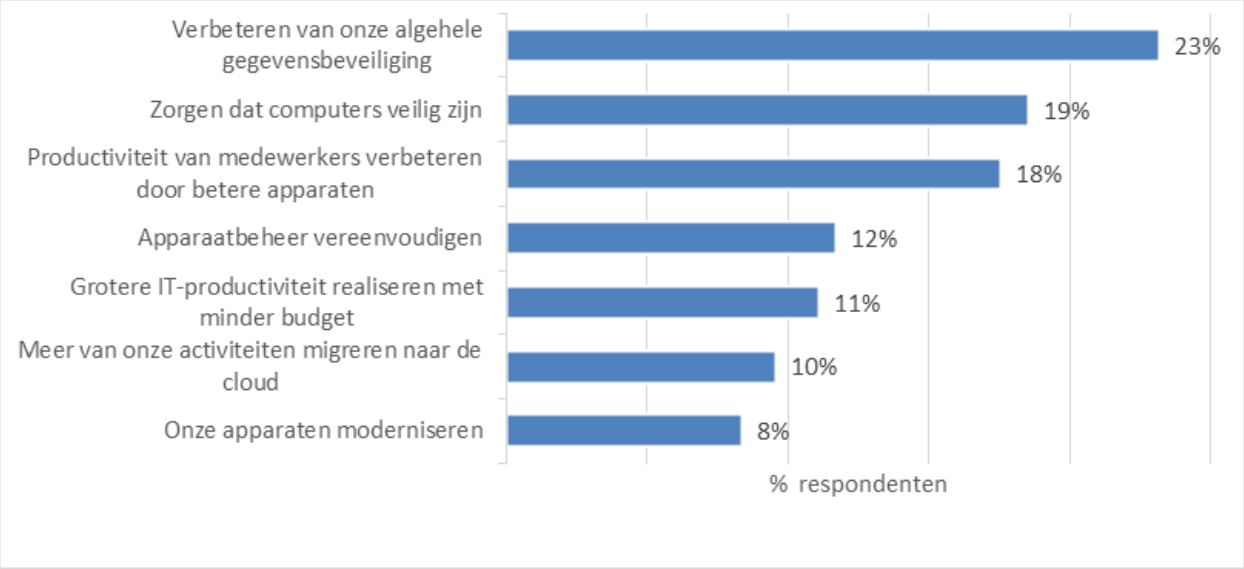
Toen we ITDM's vroegen wat hun belangrijkste doorslaggevende factor was bij het kiezen van hun volgende computerleverancier, kwam beveiliging op de eerste plaats, gevolgd door prestaties, ondersteuning voor bestaande applicaties en integratie met de bestaande IT-infrastructuur. Misschien wel het opvallendst, is dat de optie Specificaties als een van de minst belangrijke punten werd gezien.

Zie figuur 1 voor de belangrijkste IT-prioriteiten. Zie figuur 2 voor de belangrijkste overwegingen bij het kiezen van een computerleverancier.

FIGUUR 1

De belangrijkste prioriteiten voor IT: gegevens- en endpointbeveiliging

V. Welke van de volgende IT-onderwerpen hebben de grootste prioriteit bij uw bedrijf op dit moment?



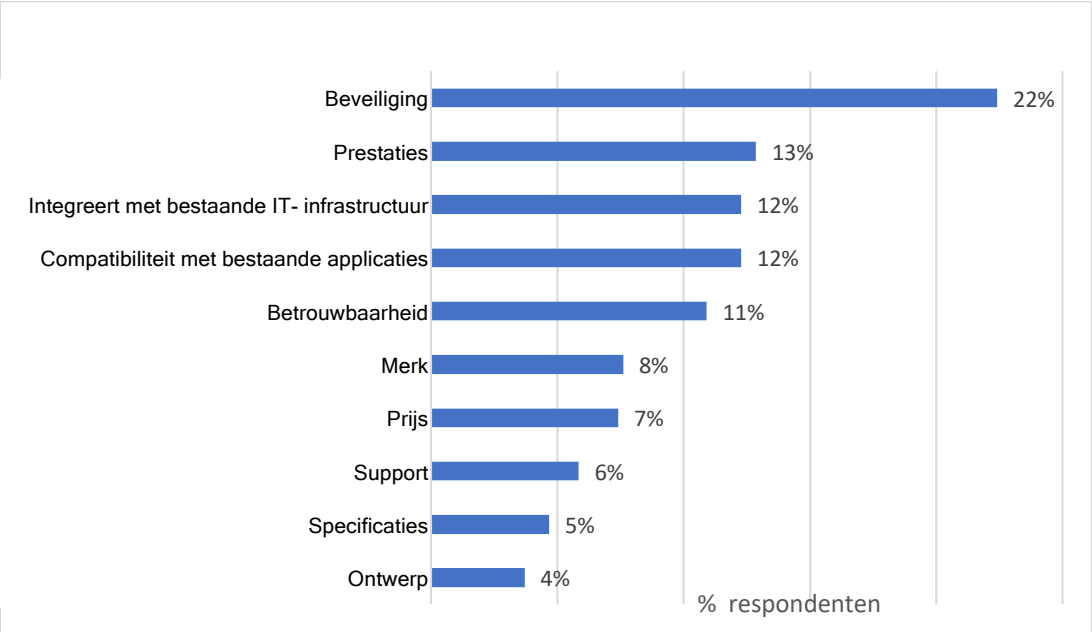
Bron: IDC's Secure Endpoint Survey, n=513

Opmerking: Gegevens omvatten de opties die als het belangrijkst werden geselecteerd (geselecteerd als nr. 1)

FIGUUR 2

Belangrijkste factoren bij het selecteren van een computerleverancier

V. Wat zijn de belangrijkste doorslaggevende factoren bij het kiezen van een computer voor uw bedrijf?



Bron: IDC's Secure Endpoint Survey, n=513

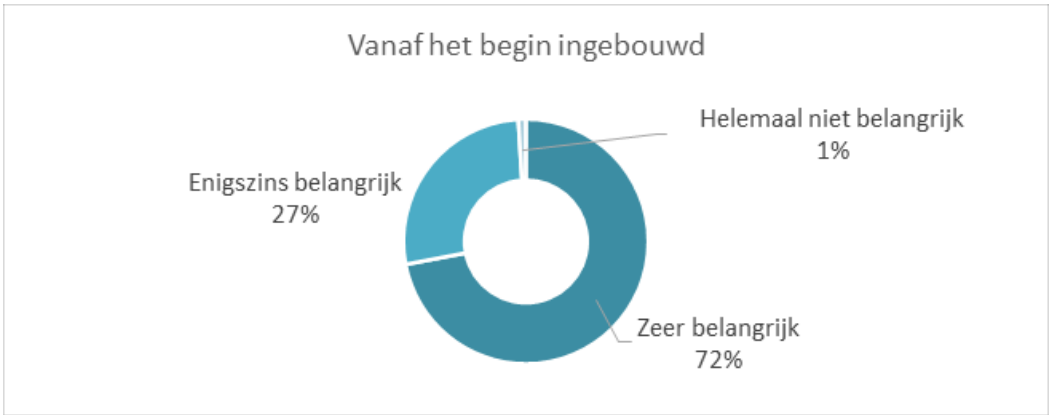
Opmerking: Gegevens omvatten de opties die als het belangrijkst werden geselecteerd (geselecteerd als nr. 1)

De twee concepten die respondenten vooral aanspraken, waren ingebouwde beveiliging en geïntegreerde gegevensbescherming. Ook werd de vraag gesteld: "Hoe belangrijk is het volgens u dat beveiliging vanaf het begin in een computer is ingebouwd - inclusief de chips, de firmware en het besturingssysteem - om deze te beschermen tegen de dreigingen van nu en vooruitlopend op die van morgen?" Het antwoord was overweldigend positief: 72% gaf aan dat het zeer belangrijk was en 27% gaf aan dat het enigszins belangrijk was. Slechts 1% zei dat het helemaal niet belangrijk was. Als we de gegevens nader bekijken, valt op dat onder ITDM's die werken bij gezondheidszorg- en financiële organisaties, het percentage dat aangaf dat het zeer belangrijk was nog hoger lag (respectievelijk 84% en 75%). Het concept van geïntegreerde gegevensbescherming scoorde eveneens hoog. We vroegen ook: “Hoe belangrijk is het volgens u dat encryptiemogelijkheden zijn geïntegreerd in de computerhardware?” 71% gaf aan dat het zeer belangrijk was, 29% gaf aan dat het enigszins belangrijk was en 0% gaf aan dat het onbelangrijk was. Zie figuur 3 voor de details over ingebouwde beveiliging en geïntegreerde gegevensversleuteling.

FIGUUR 3

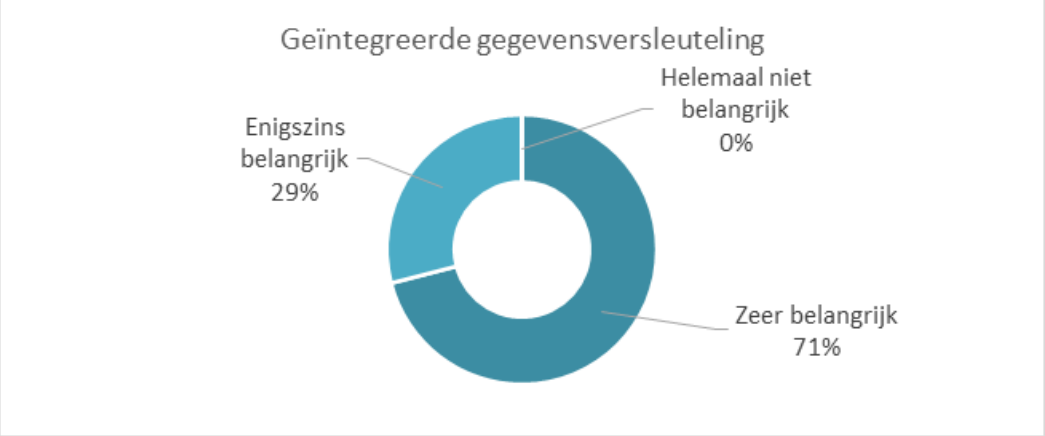
Het belang van ingebouwde beveiliging en geïntegreerde gegevensversleuteling

V. Hoe belangrijk is het volgens u dat beveiliging vanaf het begin in een computer is ingebouwd - inclusief de chips, de firmware en het besturingssysteem - om deze te beschermen tegen de dreigingen van nu en vooruitlopend op die van morgen?



Bron: IDC's Secure Endpoint Survey, n=513

V. Hoe belangrijk is het volgens u dat encryptiemogelijkheden zijn geïntegreerd in de computerhardware?



Bron: IDC's Secure Endpoint Survey, n=513

Hoewel hardware met vanaf het begin ingebouwde beveiliging belangrijk is en geïntegreerde gegevensversleuteling een belangrijke vereiste is, weten beveiligingsexperts goed dat eindgebruikers zelf doorgaans de zwakste schakel in elke beveiligingsketen zijn. Daarom is het dat gebruikersauthenticatie zo belangrijk is en hebben technologieleveranciers hard gewerkt

aan de ontwikkeling van nieuwe authenticatiemogelijkheden. Helaas is dit een gebied waar veel organisaties volgens ons onderzoek nog achterlopen.

Aan de positieve kant laat ons onderzoek zien dat 68% van de respondenten aangaf dat hun organisatie het gebruik van complexe wachtwoorden vereist en 63% zei dat ze gebruikmaken van tweefactorauthenticatie. Minder positief is dat slechts 23% gebruikmaakt van single sign-on-technologieën (SSO) en dat maar 20% biometrische beveiliging (zoals vinger- of gezichtsidentificatie) gebruikt. Het is het vermelden waard dat van onze respondenten 56% aangaf dat biometrische authenticatie veel veiliger was dan wachtwoorden, dat 35% aangaf dat het iets veiliger was, dat 9% aangaf dat het even veilig was en dat niemand (0%) zei dat het minder veilig was.

Een belangrijke nieuwe authenticatietechnologie die recent werd geïntroduceerd is de passkey. Een passkey is een digitaal wachtwoord dat gebruikmaakt van een sleutelpaar. Het biedt een veel veiligere oplossing dan een wachtwoord. Omdat dit een nieuwe technologie is, gaf slechts 14% van de respondenten aan dat hun bedrijf dit gebruikt, maar slimme ITDM's zouden deze technologie nu al eens nader moeten bestuderen. Zie figuur 4 voor details over gebruikersauthenticatie.

FIGUUR 4

Methoden voor gebruikersauthenticatie

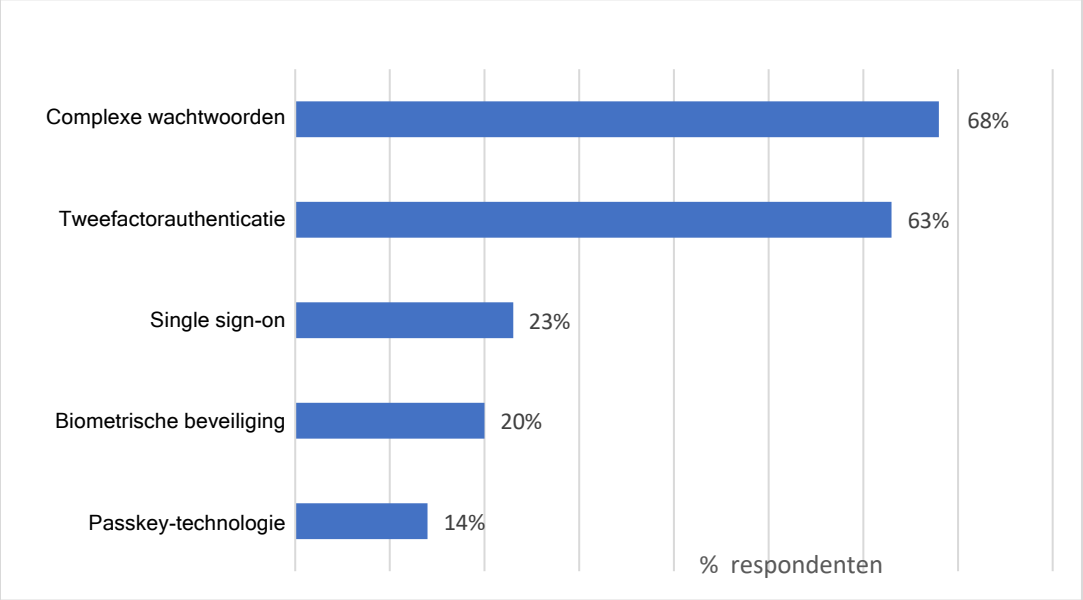
V1. Vereist uw bedrijf dat werknemers complexe wachtwoorden gebruiken om in te loggen op hun computer?

V2. Gebruikt uw bedrijf computers die biometrische beveiligingsmaatregelen ondersteunen, zoals vingerscans?

V3. Is uw bedrijf begonnen met het onderzoeken van de voordelen van het gebruik van passkey-technologie?

V4. Vereist uw bedrijf het gebruik van tweefactorauthenticatie?

V5. Maakt uw bedrijf gebruik van single sign-on (SSO) mogelijkheden? (J/N)



Bron: IDC's Secure Endpoint Survey, n=513

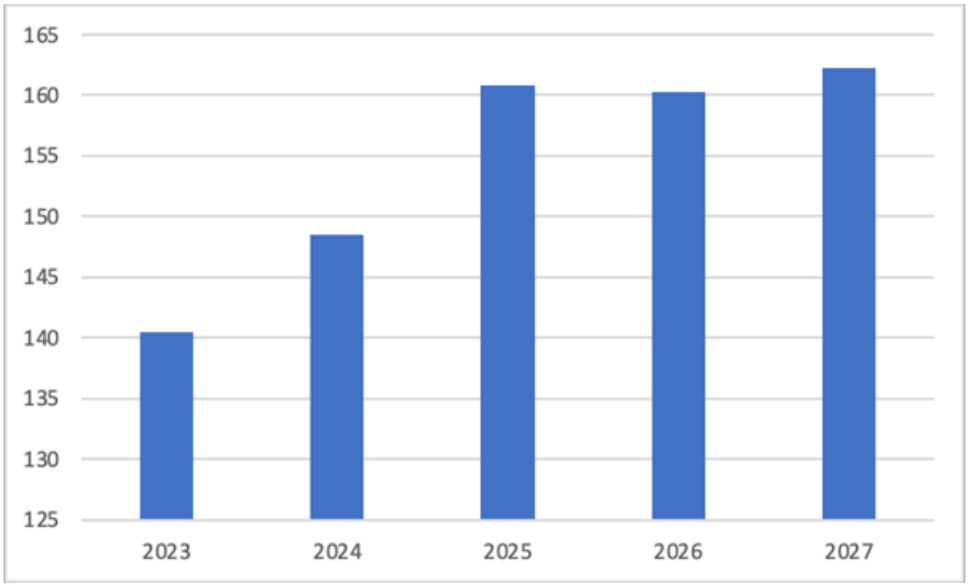
Gegevens geven percentage aan dat met 'ja' antwoordde

Onder de respondenten heeft een schokkend hoog percentage zelfs de basale authenticatieprotocollen met complexe wachtwoorden (32%) en twee-factor-authenticatie (37%) niet geïmplementeerd. **Een best practice die de moeite waard is om toe te passen,** is ervoor zorgen dat uw bedrijf een consistente vorm van authenticatie in de hele organisatie heeft geïmplementeerd. Begin nadat u deze baseline hebt geïmplementeerd met het overwegen van SSO-mogelijkheden in combinatie met een sterk master-authenticatieprotocol. Kijk tot slot bij de volgende hardware-update ook eens naar computers die in staat zijn om de hoogste verificatieniveaus te ondersteunen zoals biometrische beveiliging en passkey-technologie. Het inschakelen van biometrie en passkeys betekent dat medewerkers in de toekomst snel en veilig kunnen inloggen op hun computers en vanaf daar ook direct op hun apps en websites.

Met dat laatste punt - het vervangen van de huidige hardware - sluiten we dit hoofdstuk af. Veel bedrijven zijn in het bezit van verouderde computers die vervangen moeten worden. Zelfs als uw organisatie pas in 2020 een aanzienlijk percentage nieuwe endpoints heeft gekocht, naderen die computers al snel de grens van vier jaar. In die periode is hardwarebeveiliging zich blijven ontwikkelen om bestaande dreigingen het hoofd te bieden. Misschien wel net zo belangrijk is dat de meeste van deze producten werden uitgebracht voordat er een wijdverspreide verschuiving plaatsvond naar thuis- en hybride werken. Dit betekent dat veel van deze producten de camera's, microfoons en luidsprekers van hoge kwaliteit missen die werknemers nodig hebben om gebruik te kunnen maken van de webconference- en samenwerkingsapps van nu. Na een aantal jaar waarin het aantal bestellingen afnam, voorspelt de Personal Computing Device Tracker van IDC nu dat deze categorie in de komende paar jaar een groei zal doormaken. Opmerking: Zakelijke eenheden vertegenwoordigen eenheden gekocht door niet-consumenten. Zie figuur 5 voor IDC's prognose voor particuliere/zakelijke computers.

FIGUUR 5

WW prognose zakelijke computers



Bron: IDC PCD Tracker, augustus 2023

Bedrijven zouden de computerbehoeften van hun medewerkers continu moeten evalueren om concurrerend te blijven en toptalenten moeten aantrekken en behouden. Waar IT vroeger moest kiezen tussen beveiliging en medewerkerstevredenheid, kan de juiste leverancier tegenwoordig helpen met een oplossing waarbij die keuze overbodig is. **Een laatste best practice om te overwegen,** is het toepassen van zero-trust toegangsprincipes voor uw volgende uitrol van nieuwe hardware. Deze strategie gaat ervan uit dat telkens wanneer een apparaat toegang probeert te krijgen tot een bedrijfsresource, dit apparaat pas vertrouwd kan worden als het geverifieerd is. Zero-trust maakt gebruik van technologieën en processen die de beveiligingsstatus van het apparaat (optimaal vanaf de chips tot en met kritieke IT- en beveiligingstoepassingen), het verbindende netwerk (bijv. openbaar wifi versus privénetwerk) en de identiteit van de gebruiker bevestigen.

Mac overwegen voor bedrijven

Vandaag de dag zijn er meer IT-afdelingen die Macs ondersteunen en ons onderzoek wijst daarvoor een belangrijke reden aan. Van onze respondenten, die verschillende besturingssystemen vertegenwoordigen in hun installed base, gaf 76% aan dat ze van mening zijn dat Macs veiliger zijn dan andere computers. En in de komende 12 maanden is de belangrijkste reden voor het gebruiken van meer Macs, dat ze van mening zijn dat Macs veiliger zijn (47%), op de voet gevolgd door het gemak waarmee ze kunnen worden geïnstalleerd en beheerd (36%).

Apple richt zich op het bieden van een geweldige gebruikerservaring terwijl ze de beveiliging verbeteren door die beveiliging in te bouwen in alles, van hun chips tot en met de software. Een voorbeeld hiervan is Apple's Touch ID, een ingebouwde biometrische beveiligingsfunctie. De Apple-chips zijn voorzien van Secure Enclave, dat de passcode versleutelt en beschermt die wordt gebruikt om Touch ID-gegevens te beveiligen.

Spotlight op Apple-klant

"Eén van de allerbelangrijkste kenmerken van Apple-producten is dat privacy en beveiliging zijn ingebouwd in het product zelf. Het is geen latere toevoeging en dat is iets wat we erg waarderen." — Linda Jojo, Executive Vice President and Chief Customer Officer, United Airlines

Om het risico van besmette besturingssystemen en opstartsequenties aan te pakken, zijn Macs uitgerust met Secure Boot en Signed System Volume. Secure Boot zorgt ervoor dat alleen de cryptografisch gecertificeerde versie van macOS wordt ingeschakeld tijdens het opstarten. Signed System Volume beschermt de integriteit van het besturingssysteem als het actief is. Verouderde software vertegenwoordigt ook een cyberrisico dat Apple minimaliseert door de end-to-end verspreiding en installatie van software-updates te automatiseren en beveiligen.

Goede software van derden is essentieel voor de productiviteit van medewerkers, maar die software mag geen malware bevatten. Apple maakt gebruik van een meerlaagse benadering voor het voorkomen van malware. De Mac App Store van Apple scant elke app op malware. Omdat software op Macs ook van het web kan worden gedownload, eist Apple van ontwikkelaars dat ze hun programma's indienen bij de notarisdienst van Apple, die ook scant op malware. Apple's Gatekeeper, inbegrepen in macOS, controleert op notarisatie en voorkomt dat niet-ondertekende apps kunnen worden uitgevoerd. Daarnaast blokkeert en verwijdert Xprotect - de anti-malwaretool van Apple - alle bekende kwaadaardige software.

Gegevens behoren tot de meest waardevolle activa van een organisatie en moeten dienovereenkomstig worden beschermd. De combinatie van door chips versterkte FileVault-encryptie, door Apple ondersteunde VPN-protocollen en end-to-end-encryptie in Apple-services (zoals iMessage en iCloud) zorgt ervoor dat gegevens worden beschermd terwijl ze niet worden gebruikt, terwijl ze worden overgezet en terwijl ze wél worden gebruikt.

Nu social engineering tot het arsenaal van kwaadwillenden behoort, moeten eindgebruikers op hun hoede zijn. Een ingewikkelde verantwoordelijkheid, maar Apple helpt daarbij met Safari Fraudulent Website Warning. Omdat inloggegevens vaak worden gestolen door kwaadwillenden, maakt de passkey-ondersteuning van Apple het voor organisaties bovendien eenvoudiger om hun authenticatiemethoden te moderniseren, wederom zonder dat dit ten koste gaat van een positieve eindgebruikerservaring.

Een goede beveiliging gaat hand in hand met robuust apparaatbeheer. Om die reden biedt Apple hiervoor een aantal opties, zoals een ingebouwd managementframework met Mobile Device Management (MDM). Apple Business Manager maakt een zero-touch-uitrol mogelijk en is gekoppeld aan MDM-oplossingen. Met Endpoint Security API's voor Mac kunnen developers oplossingen bouwen voor het monitoren en analyseren van en het reageren op beveiligingsdreigingen. Apple biedt ook identiteitsintegraties middels een ingebouwd SSO-framework dat met moderne identiteitproviders (IdP's) werkt.

Tot slot biedt Apple met macOS deze beveiligingsfuncties, inclusief zowel grote als kleine software-updates, zonder zakelijke of particuliere klanten daar extra kosten voor in rekening te brengen.

UITDAGINGEN/KANSEN

Ondanks constant veranderende dreigingen, staat IT voor de uitdaging om meer te doen met minder: minder budget, minder IT-medewerkers en minder middelen. Behalve dat ze oplossingen moeten vinden voor de permanente beveiligingsrisico's waar elk bedrijf mee te maken heeft, hebben veel IT-organisaties ook de taak om de productiviteit en tevredenheid van werknemers meetbaar te verbeteren via de hardware, software en diensten die ze uitrollen. Het succesvol en tegelijk volbrengen van beide taken - de veiligheid en de productiviteit van medewerkers verbeteren en hun tevredenheid verhogen - kan onmogelijk lijken. Maar het vertegenwoordigt ook een belangrijke kans voor IT. Een kans om de hardware, software en diensten die het bedrijf aanschaft, de leveranciers waar het deze van koopt en de manieren waarop het ze inzet voor een steeds meer hybride personeelsbestand opnieuw te evalueren. Bovendien is het duidelijk tijd om de modellen voor totale eigendomskosten te herberekenen om beter aan te sluiten bij de manier waarop bedrijven tegenwoordig technologie kopen en gebruiken.

CONCLUSIE

Beveiliging is en blijft een topprioriteit voor IT. In een tijd waarin IT-budgetten krap zijn en er een belangrijke vernieuwing van hardware voor de deur staat, is het zinvol om opnieuw te evalueren bij welke leveranciers u uw geld gaat uitgeven. Overweeg het implementeren van best practices rond authenticatie en zero-touch implementaties en koop hardware die deze verschuivingen mogelijk maakt. Plaats beveiliging niet hoger op de prioriteitenlijst dan productiviteit en werknemerstevredenheid als er leveranciers zijn die computers op de markt brengen met ingebouwde beveiliging en gegevensversleuteling die zowel beveiliging als een positieve eindgebruikerservaring mogelijk maken.

Over IDC

International Data Corporation (IDC) is de voornaamste wereldwijde leverancier van marktinformatie, adviesdiensten en evenementen voor de informatietechnologie-, telecommunicatie- en consumententechnologiemarkten. IDC helpt IT-professionals, leidinggevenden en de investeringsgemeenschap om gefundeerde beslissingen te nemen over technologieaankopen en bedrijfsstrategie. De ruim 1100 IDC-analisten beschikken over mondiale, regionale en lokale expertise op het gebied van technologie en de sectorkansen en -trends in meer dan 110 landen wereldwijd. IDC biedt al 50 jaar strategische inzichten om onze klanten te helpen hun belangrijkste zakelijke doelstellingen te verwezenlijken. IDC is een dochteronderneming van IDG, 's werelds meest toonaangevende bedrijf op het gebied van technologie, media, onderzoek en evenementen.

IDC CEMA

Male namesti 11
110 00 Praag 1, Tsjechië
+420 2 2142 3140
Twitter: @IDC
blogs.idc.com
www.idc.com