Windows 11 Pro

Komplet sikkerhedsmanual til den hybride arbejdsplads

Cybersikkerhed er topprioritet med 88 % af SMV'er, der er uforberedte til at håndtere cybertrusler.[1]

Her er nogle af de måder, som en sikker, fremtidssikret IT-infrastruktur hjælper med at beskytte din forretning mod cybertrusler på:

Indtag en zero-trust-position

En zero-trust-sikkerhedsmodel reducerer risici ved eksplicit at bekræfte datapunkter såsom en brugers identitet, placering og enhedstilstand for hver adgangsanmodninger – uden undtagelser. Når brugere og enheder så er bekræftet, har de begrænset adgang til kun nødvendige ressourcer.

Zero-trust-principper er trefoldige:

1 Bekræft først eksplicit. Det betyder, at du altid skal godkende og autorisere baseret på alle tilgængelige datapunkter, inkl. brugers identitet, placering, enhedstilstand, service eller arbejdsbyrde, dataklassifikation og anomalier.

2 Brug dernæst mindst priviligeret adgang, hvilket begrænser brugeradgang med tids- og omfangsnødvendig adgang, risikobaserede, adaptive politikker og databeskyttelse for at hjælpe med at sikre både data og produktivitet.

3 Antag for det tredje brud. Antag, at brud opererer på en måde, der minimerer skadesradius og segmentadgang. Bekræft komplet kryptering, og brug analyse til at få synlighed og optimere trusselsdetektering og -forsvar.

For at implementere en zero-trust-tilganger organisationer nødt til at forstå deres egne data, og hvor de data opbevares.

Virksomheder bør kende graden af datafølsomhed og de potentielle risici ved eksponering for at afgøre, hvor zero-trust skal bemyndiges. For cloudbaseret lager og cloudbaserede programmer såsom mailtjenester og clouddatalager er det afgørende at etablere et zero-trust-miljø for at mindske risici. Uden denne tilgang er firmaadgangskoder, enheder og følsomme data sårbare over for angreb.

Implementér avancerede godkendelsesmetoder

Et sikkerhedsbrud bliver langt mere sandsynligt, hvis metoder til brugergodkendelse bliver kompromitteret. Uautoriseret adgang til en medarbejders enhed giver ofte en svindler adgang til en organisations fulde netværk. Det er afgørende at implementere en sikker måde til at sikre, at brugere er dem, de siger, de er, i nutidens hybride arbejdsmiljø. Multifaktor-godkendelse kan gøre meget for at skabe et mere sikkert miljø. Adgangskoder er ikke længere nok til at mindske sofistikerede trusler, da de ofte nemt kompromitteres. Teknikker som to-faktorgodkendelse kombineret med biometriske funktioner, der allerede findes på mange moderne enheder, f.eks. Windows Hello for Business, er langt mere effektive til at beskytte organisationer og deres netværk mod cyberangreb, især når det forstærkes med en zero-trust-sikkerhedsstrategi.

Styrk hardwaresikkerhed

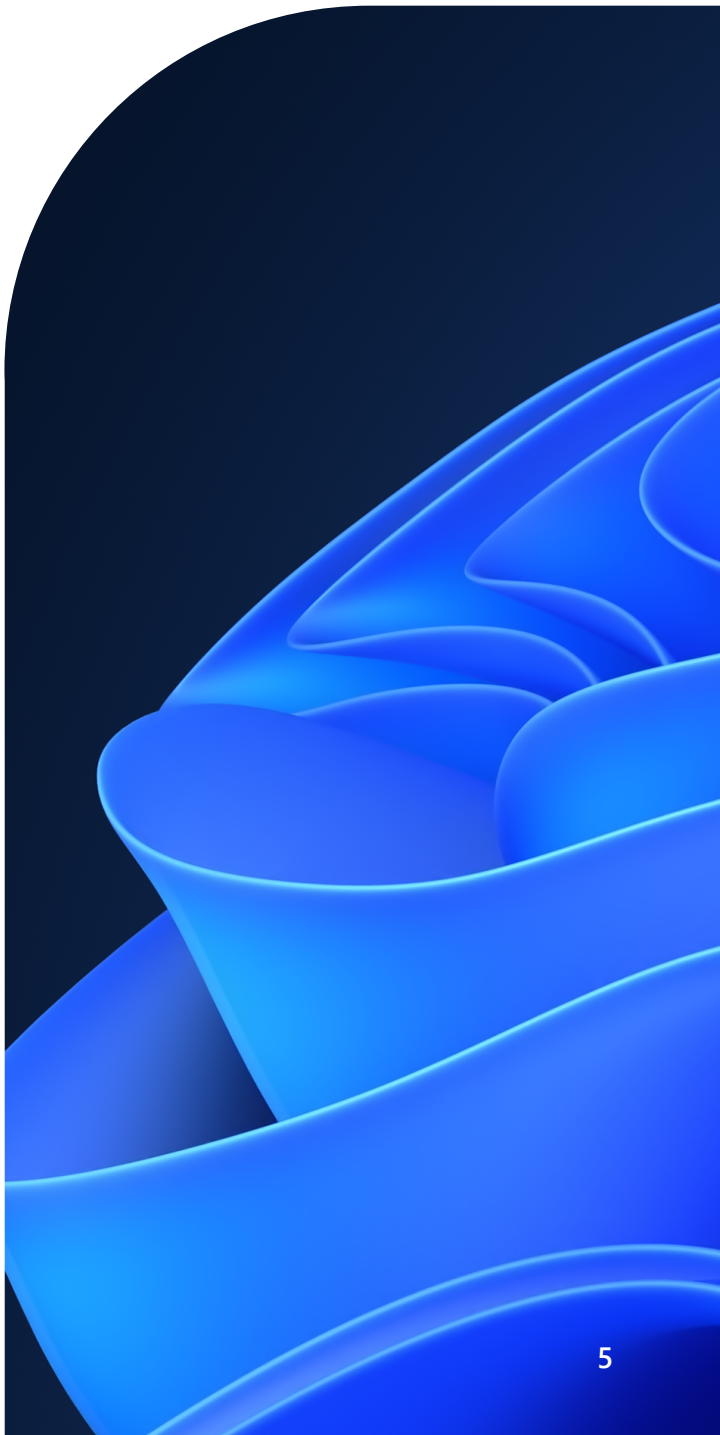
Operativsystemet alene kan ikke beskytte mod de mange forskellige værktøjer og teknikker, som cyberkriminelle bruger til at kompromittere en computer. Når en fremmed først har anskaffet sig adgang, kan personen installere malware i enhedens firmware, som er meget svær at fjerne, eller stjæle følsomme data og vigtige loginoplysninger. Det kan være svært at detektere disse fremmede, når først de har fået adgang. Der skal være en stærk kombination af hardwaresikkerhed og softwarebaserede sikkerhedsprogrammer. Moderne trusler kræver computeringshardware, som er sikker ved chip- og processorniveauet og beskytter følsomme oplysninger, lige der hvor de er gemt. Der er hele klasser af sårbarheder, som kan elimineres ved blot at have indbyggede sikkerhedsfunktioner på hardwareniveauet.

Disse funktioner kan f.eks. findes i alle Windows 11 Secured-core-pc'er. Desuden kan der opnås betydelige ydeevneforbedringer sammenlignet med at installere lignende sikkerhedsfunktioner kun med software. Dette øger systemets generelle sikkerhedssituation, uden at det går ud over systemets ydeevne.

Brug adgangskontroller for identitetsbaseret beskyttelse

I clouden kan administratorer styre og administrere identiteter og tilgå dem fra én placering. Med eksempelvis Microsoft Azure Active Directory (Azure AD) kan de centralt styre medarbejdernes identiteter samt konfigurere og implementere politikker om adgang til programmer, websteder og grupper. Administratorer kan integrere overholdelseskrav, og alle nye regler kan inkorporeres, når de opstår.

Cloudbaserede kontroller øger sikkerheden og styrker overholdelse. Microsofts forskning viser, at multifaktor-godkendelse alene kan blokere over 99,9 % af kontokompromitterende angreb.[2] Betinget adgang gør, at administratorer kan oprette regler baseret på aktivitet eller placering, hvilket yderligere reducerer angriberes mulighed for at udnytte sårbarheder. Loginforsøg, der kommer uden for landet eller sker på underlige tidspunkter, kan f.eks. afvises. Desuden kan administratorer aktivere enkeltlogin, så brugere kan sikre adgang til programmer overalt, hvilket samtidig gør adgangskodestyringen nemmere for IT.



Microsoft introducerede for nylig den generelle tilgængelighed af understøttelse af multi-cloudsikkerhed. Nu kan virksomheder onboarde multi-cloudressourcer til Azure Security Center såsom Google Cloud Platform (GCP) og Amazon Web Services (AWS) samt beskytte servere med Azure Defender til servere baseret på Azure Arc.

Beskyt fjernenheder

Microsofts cloud gør det nemmere at administrere enheder og programmer. Med Microsoft Intune kan enhedsinstallationen eksempelvis administreres sikkert og eksternt, mens programmer nemt kan skaleres til at reagere on demand.

Microsoft Windows Autopilot anvender sikkerhedsindstillinger og andre kontroller til at hjælpe med at beskytte enheder, før en medarbejder forbinder til nogen ressourcer.

Sikre programmer

Få mere beskyttelse mod upålidelige kilder ved at åbne filer og websteder i en isoleret beholder med Windows Defender Application Guard. Cloudprioriteret design muliggør nem udvidelsesmulighed med Microsoft 365, Microsoft Defender for Cloud og Microsoft Defender for Endpoints.[3]

Strømlin sikkerhedsstyring på tværs af forskellige steder, og udvid sikkerheden til clouden. Hjælp med at beskytte enheder, data, apps og identiteter overalt. Installér med tryghed, velvidende at 99,6 % af programmer er kompatible med Windows 11.[4]

Automatisér sikkerhedsvedligeholdelse

Cloudbaserede teknologier gør, at IT-administratorer automatisk kan installere opdateringer, rettelser og sikkerhedskopier på tværs af systemer og enheder. Dette reducerer konfigurationsfejl, begrænser nedetid og beskytter samtidig systemer mod nye trusler. Rutineopgaver kan automatiseres, så administratorer har tid til at fokusere på vigtige opgaver, der virkelig kræver deres ekspertise.

Hold din virksomhed sikker med Windows 11 Pro-enheder

Det bør være en høj prioritet at opgradere din organisations sikkerhedstilstand, og at udstyre dine medarbejdere med sikre enheder er hjørnestenen for at opnå succes. Nye Windows 11 Pro-enheder kombineret med Microsoft 365 er bygget til sikkert hybridarbejde.

- Beskyt dine medarbejdere mod malware, vira, phishing-forsøg, skadelige links, og hjælp med at sikre forretningskritiske data.

- Få lag af kraftfuld sikkerhed på tværs af enheder, data, identiteter, programmer og clouden.

- Strømlin IT med forenede, cloudbaserede slutpunktsadministrationsværktøjer, inkl. Microsoft Endpoint Manager, Azure Active Directory og Windows Autopilot. Fjernindstil og -håndhæv politikker, administrer programmer og identiteter, og installér nemt erhvervsparate enheder.

- Overkom problemer ved fjernsamarbejde med en enkelt løsning, der inkluderer videomøder, produktivitetsapps, fildeling og mere. Sørg for, at dine medarbejdere har sikker adgang til kritiske arbejdsapps og -oplysninger med en forenet samarbejdsløsning.

- For personer i datafølsomme brancher eller forretningsscenarier er Secured-core-pc'er de mest sikre Windows-enheder og leveres med alle de avancerede sikkerhedsfunktioner i Windows 11 aktiveret.

Reducer betragteligt risikoen for cyberangreb ved at udskifte gamle pc'er med nye, moderne enheder, der er optimeret til sikkerhed og hybrid arbejde. Windows 11 Pro og Microsoft M365 forener hardware og software for at skabe brugsklar og kraftfuld beskyttelse til at sikre dine enheder, data, programmer, identiteter og tjenester.

Windows 11 Pro

[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Sælges separat*

[4] *App Assure-programdata fra oktober 2018 til februar 2022. Siden 2018 har App Assure arbejdet sammen med tusindvis af kunder og evalueret over 1,1 millioner apps med en 99,6 % appkompatibilitet. Få mere at vide på App Assure-webstedet, og se Windows IT Pro Blog-indlægget om App Assure*