Windows 11 Pro

Komplett sikkerhetsbok for hybridarbeidsplassen

Cybersikkerhet er viktigst hos 88 % av SMB-er som ble undersøkt som under-forberedt på å håndtere cybertrusler.[1]

Her er noen av måtene en sikker og fremtidssikker IT-infrastruktur hjelper med å beskytte virksomheten mot cybertrusler på:

Bruk en Zero-trust-tilnærming

Zero-Trust-sikkerhetsmodellen reduserer risiko ved eksplisitt å verifisere datapunkter som brukeridentitet, sted og enhetstilstand for hver tilgangsforespørsel, uten unntak. Når verifisert, har brukere og enheter begrenset tilgang til kun nødvendige ressurser.

Zero Trust-prinsippene er tredelt:

1 Først, verifiser eksplisitt. Det betyr alltid å godkjenne og autorisere basert på alle tilgjengelige datapunkter, inkludert brukeridentitet, sted, enhetstilstand, tjeneste eller arbeidsbelastning, dataklassifisering og uregelmessigheter.

2 Nummer to, bruk tilgang med minst mulig rettigheter, noe som begrenser brukertilgang med akkurat-tidsnok- og akkurat-tilstrekkelig-tilgang, risikobaserte adaptive policyer og databeskyttelse for å hjelpe med å sikre både data og produktivitet.

3 Nummer tre, anta sikkerhetsbrudd. Anta sikkerhetsbrudd fungerer på en måte som minimerer eksplosjonsradius og segmenttilgang. Verifiser ende-til-ende-kryptering og bruk analyse for å oppnå synlighet for å forbedre trusseldeteksjon og forsvar.

For å implementere en Zero-trust-tilnærming må organisasjoner forstå sine egne data og hvor de dataene er lagret.

Virksomheter må kjenne til nivået av datasensitivitet og potensielle risikoer for eksponering for å avgjøre hvor zero-trust må gis myndighet. For skybasert lagring og skybaserte apper, som e-posttjenester og skydatalager, er det fornuftig å etablere et zero-trust-miljø, og det er viktig for å redusere risikoer. Uten denne tilnærmingen vil virksomhetens passord, enheter og sensitive data uunngåelig være utsatt for risiko for angrep.

Implementer avanserte godkjenningsmetoder

Sannsynligheten for et sikkerhetsbrudd øker hvis brukergodkjenningsmetoder blir kompromittert. Uautorisert tilgang til en ansatts enhet fører ofte til at en ondsinnet aktør får tilgang til hele nettverket til en organisasjon. Implementering av en metode for å sikre at en bruker er den vedkommende hevder å være, er grunnleggende viktig i dagens hybridarbeidsmiljø. Godkjenning med flere faktorer vil langt på vei skape et sikrere miljø. Passord er ikke lenger tilstrekkelig for å avhjelpe stadig mer sofistikerte trusler siden de ofte kan kompromitteres. Teknikker som godkjenning med flere faktorer, kombinert med den biometriske funksjonaliteten som er tilgjengelig på mange moderne enheter, som Windows Hello for Business, er mye mer effektive for å beskytte organisasjoner og deres nettverk mot cyberangrep, spesielt når de forsterkes med en Zero Trust-sikkerhetsstrategi.

Forsterk maskinvaresikkerheten

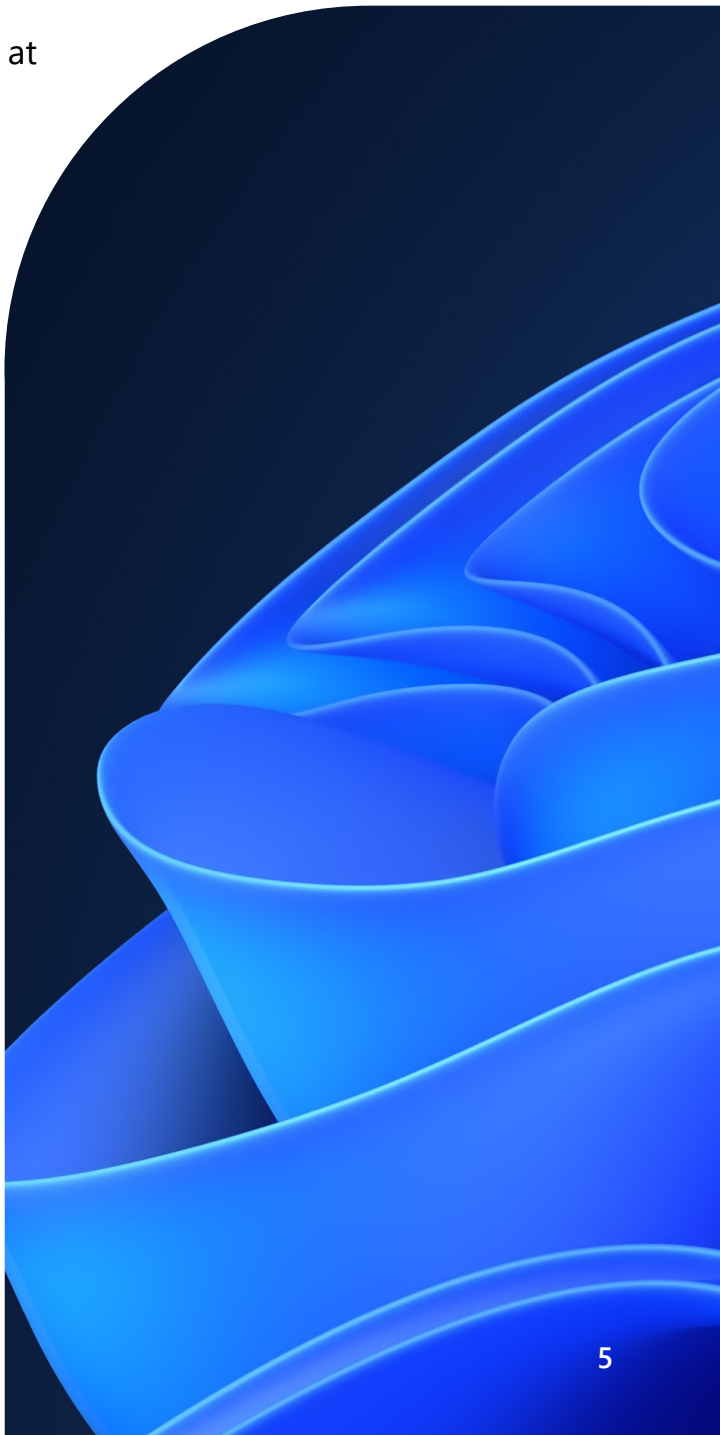
Operativsystemet alene kan ikke beskytte mot det store utvalget av verktøy og teknikker som cyberkriminelle kan bruke for å kompromittere en datamaskin. Inntrengere kan, når de først har kommet seg inn, distribuere skadelig programvare som er vanskelig å fjerne, i enhetens fastvare, eller de kan stjele sensitive data og viktig legitimasjon. Det kan være vanskelig å oppdage disse inntrengerne når de først har fått tilgang. Det må være en sterk forbindelse mellom maskinvaresikkerhet og programvarebaserte sikkerhetsapper. Moderne trusler krever maskinvare som er sikker på brikke- og prosessornivå og som beskytter sensitiv forretningsinformasjon akkurat der den er lagret. Det er hele klasser med sårbarheter som kan fjernes ganske enkelt ved å ha innebygd sikkerhetsfunksjonalitet på maskinvarenivået.

Slik funksjonalitet finnes i alle Windows 11-PC-er med sikret kjerne, for eksempel. I tillegg kan det oppnås betydelige ytelsesforbedringer sammenlignet med å distribuere lignende sikkerhetsfunksjonalitet med programvare alene. Dette øker sikkerheten til et system uten at det går på bekostning av systemytelsen.

Bruk tilgangskontroller for identitetsbasert beskyttelse

I skyen kan administratorer styre og administrere identiteter og tilgang fra ett sted. Med Microsoft Azure Active Directory (Azure AD) kan de for eksempel sentralstyre identitetene til de ansatte samt konfigurere og distribuere policyer for tilgang til apper, nettsteder og grupper. Administratorer kan bygge inn overholdelseskrav, og alle nye regler kan innlemmes etter hvert som det trengs.

Skybaserte kontroller øker sikkerheten og styrker overholdelse. Microsofts undersøkelser har funnet at godkjenning med flere faktorer alene kan blokkere over 99,9 % av angrep mot kontoer.[2] Betinget tilgang lar administratorer opprette regler basert på aktivitet eller sted, noe som ytterligere reduserer mulighetene angripere har for å utnytte sårbarheter. For eksempel kan påloggingsforsøk som kommer fra utlandet eller som kommer på uvanlige tidspunkt, avvises. I tillegg kan administratorer aktivere enkeltpålogging som gir brukere sikker tilgang til apper overalt, samtidig som passordbehandlingen blir enklere for IT.



Microsoft introduserte nylig generell tilgjengelighet av sikkerhetsstøtte for flere skyer. Nå kan virksomheter innføre flerskyressurser i Azure Security Center, som Google Cloud Platform (GCP) og Amazon Web Services (AWS), samt beskytte servere med Azure Defender for Servers basert på Azure Arc.

Beskytt eksterne enheter

Microsoft-skyen gjør det enklere å administrere enheter og apper. Med Microsoft Intune for eksempel, kan enhetsdistribusjon administreres sikkert og eksternt, mens apper enkelt kan skaleres etter behov.

Microsoft Windows Autopilot benytter sikkerhetsinnstillinger og andre kontroller til å hjelpe med å beskytte enheter før en ansatt kobler til noen ressurser.

Sikre apper

Få mer beskyttelse mot ikke-klarerte kilder ved å åpne filer og nettsteder i en isolert container med Windows Defender Application Guard. Skyen først-design muliggjør enkel utvidelse med Microsoft 365, Microsoft Defender for Cloud og Microsoft Defender for Endpoints.[3]

Effektiviser sikkerhetsadministrasjon på tvers av ulike steder, og utvid sikkerheten til skyen. Hjelp med å beskytte enheter, data, apper og identiteter overalt. Distribuer trygt i visshet om at 99,6 % av appene er kompatible med Windows 11.[4]

Automatiser sikkerhetsvedlikehold

Skybaserte teknologier gjør det mulig for IT-administratorer å automatisk ta i bruk oppdateringer, rettelser og sikkerhetskopier på tvers av systemer og enheter. Dette reduserer konfigurasjonsfeil og begrenser nedetiden samtidig som systemene beskyttes mot nye trusler. Rutineoppgaver kan automatiseres slik at administratorer kan fokusere på viktige oppgaver som trenger deres ekspertise.

Hold virksomheten sikret med Windows 11 Pro-enheter

Transformering av virksomhetens sikkerhetstilstand bør være en prioritet, og å utstyre arbeidsstyrken med sikre enheter en hjørnestenen for suksess. Nye Windows 11 Pro-enheter, kombinert med Microsoft 365, er bygd for sikkert hybridarbeid.

- Beskytt de ansatte mot skadelig programvare, virus, phishing-forsøk og skadelige koblinger, og bidra til å sikre forretningskritiske data.
- Få lag med kraftfull sikkerhet på tvers av enheter, data, identiteter, apper og skyen.
- Effektiviser IT med enhetlige, skybaserte verktøy for administrasjon av endepunkter, inkludert Microsoft Endpoint Manager, Azure Active Directory og Windows Autopilot. Angi og håndhev policyer eksternt, administrer apper og identiteter og distribuer enkelt forretningsklare enheter.
- Bli kvitt hindringer for eksternt samarbeid med én enkelt løsning som inkluderer videokonferansefunksjoner, produktivitetsapper, fildeling og mer. Sørg for at de ansatte har sikker tilgang til viktige apper og informasjon med en enhetlig samarbeidsløsning.
- For personer i datasensitive industrier eller forretningsscenarier er PC-er med sikret kjerne de sikreste Windows-enhetene, og de leveres med alle de avanserte sikkerhetsfunksjonene i Windows 11 aktivert.

Reduser risikoen for cyberangrep betydelig ved å erstatte eldre PC-er med nye og moderne enheter som er optimalisert for sikkerhet og hybridarbeid. Windows 11 Pro og Microsoft M365 fører sammen maskinvare og programvare for å gi kraftig "out-of-the-box"-beskyttelse for å skjerme enheter, data, apper, 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] *Selges separat*

[4] *App Assure-programdata fra oktober 2018 til februar 2022. Siden 2018 har App Assure fungert med tusenvis av kunder og har evaluert over 1,1 millioner apper der 99,6 prosent av appene var kompatible. Hvis du vil vite mer, kan du gå til App Assure-nettstedet og se Windows IT Pro-blogginnlegg om App Assure*