NorSIS

SIKKER FJERNTILGANG

Ansatte og leverandører kan ha behov for å koble til nettverket eksternt.

Tenk sikkerhet først. Få ansatte og leverandører til å følge gode sikkerhetsstandarder før de kobler til nettverket. Gi dem verktøy for å gjøre sikkerhet en del av deres faste arbeidsrutine.

HVORDAN
BESKYTTE ENHETER

Enten de ansatte eller leverandørene bruker enheter tilhørende bedriften eller deres egne når de kobler seg til nettverket, bør disse enhetene være sikre. Følg disse tipsene – og sørg for at ansatte og leverandører også gjør det:

Alltid endre alle forhåndsdefinerte ruter-passord, samt standardnavnet på ruteren. Og hold ruterens programvare oppdatert. Du må kanskje besøke leverandørens nett-sted for å gjøre det.

Vurder å aktivere full diskkryptering for bærbare datamaskiner og andre mobile enheter som kobles eksternt til nettverket ditt. Bruk operativsystemets innstillinger for dette alternativet, som vil beskytte data som er lagret på enheten hvis den blir tapt eller stjålet.

Endre smarttelefoninnstillingene til å stoppe automatiske tilkoblinger til offentlig Wi-Fi.

Hold antivirusprogramvare oppdatert på en-heter som kobler til nettverket ditt, inkludert mobile enheter.

NorSIS

EKSTERN TILKOBLING TIL NETTVERK

Krev at ansatte og leverandører bruker sikre tilkoblinger når de kobler seg eksternt til nettverket ditt. De burde:

Bruk en ruter med WPA2- eller WPA3-kryptering ved tilkobling hjemmefra. Kryptering beskytter informasjon som sendes over et nettverk, slik at utenforstående ikke kan lese den. WPA2 og WPA3 er krypteringsstandarder som beskytter informasjon som sendes over et trådløst nettverk.

Bruk alltid virtuelt privat nettverk (VPN) for å kryptere trafikken mellom datamaskinene og internett når du benytter åpent tilgjengelig Wi-Fi-nettverk. Åpent Wi-Fi-nettverk gir ikke en sikker internettforbindelse på egenhånd. Dine ansatte kan få en personlig VPN-konto fra en VPN-tjenesteleverandør, eller kanskje du vil etablere en egen bedrifts-VPN som de ansatte kan bruke.

HVA DU BØR GJØRE FOR Å OPPRETTHOLDE SIKKERHETEN

Lær opp dine ansatte:

Inkluder informasjon om sikker ekstern tilgang i virksomhetens faste sikkerhetsopplæring.

Ha retningslinjer som dekker grunnleggende cybersikkerhet lett tilgjengelig for dine ansatte og forklar viktigheten av å følge dem. Fortell personalet om risikoen ved offentlig Wi-Fi.

Før du lar en hvilken som helst enhet – enten hjemme hos en ansatt eller i leverandørens nettverk – koble til virksomhetens nettverk, må du sørge for at det oppfyller nettverks sikkerhetskrav.

Gi de ansatte verktøy som bidrar til å opprettholde sikkerheten

Krev at ansatte bruker unike, sterke passord og unngår åpne arbeidsstasjoner uten tilsyn.

Krev totrinnsbekreftelse for å få tilgang til områder i nettverket ditt som har sensitiv informasjon. Dette krever ytterligere trinn utover å logge inn med et passord – som f.eks. en midlertidig kode på en smarttelefon.

Vurder å anskaffe VPN for ansatte som trenger å koble seg eksternt til bedriftsnettverket.

Hvis du tilbyr Wi-Fi for gjester og kunder, må du sørge for at den er adskilt fra bedriftsnettverket.

Inkluder bestemmelser for sikkerhet i leverandørkontrakter, spesielt hvis leverandøren vil koble eksternt til nettverket ditt.