Digital sikkerhet på reise – er du forberedt?

Planlegger du å arbeide fra utlandet i ferien? Arbeid utenfor virksomhetens kontorer kan potensielt medføre en høyere risiko for digitale angrep.

Advokat
Cathrine Østenstad Blich
Intility

Legal & Privacy Officer
Andreas Forbech Havre
Intility

Med stadig økende digitalisering vil konsekvensene av et digitalt angrep være betydelig større for den enkelte virksomhet. Nasjonal sikkerhetsmyndighet (NSM)skriver i sin rapport «*Risiko 2022*» at de siden 2019 har sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge. Gjennom media har vi blant annet kunnet lese om angrepene mot Amedia, Nortura og Nordic Choice. Å bli utsatt for et slikt angrep har ofte store og alvorlige konsekvenser både økonomisk og omdømmemessig.

Under har vi listet opp de viktigste punktene virksomheten og du bør ta stilling når du jobber andre steder enn på kontoret i forbindelse med f.eks. reise. Disse punktene er i hovedsak aktuelle ved reise, men kan også være forebyggende i andre situasjoner der du jobber utenfor kontoret, eksempelvis på hytta eller den lokale kafeen.

Før du reiser

Risikovurdering

Det er viktig at du og din bedrift tar de forhåndsregler som dere mener er nødvendige for deres virksomhet, basert på risikoer dere har identifisert, i forbindelse med reise til utlandet. Vær oppmerksom på at din virksomhet kan ha informasjon som utenlandske aktører er interessert i.

Under stiller vi opp noen punkter det kan være greit å tenke gjennom før avreise.

1. Hvor går reisen? Sjekk gjerne om PST eller NSM har uttalt seg om trusselbildet for landet du skal reise til.
2. Identifiser risikoer – er landet du skal reise til kjent for å overvåke besøkende? Kan utstyr bli beslaglagt av myndighetene? I så fall bør du vurdere om det i det hele tatt er nødvendig å ta med jobb-PCen.
3. Etter å ha identifisert de konkrete risikoene, bør du vurdere hvor sannsynlig det er at et scenario inntreffer, og hva konsekvensen av dette kan bli. Er det eventuelle tiltak du kan ta som reduserer enten sannsynligheten eller konsekvensen av en risiko? Basert på de risikovurderingene dere og din bedrift gjør, er det opp til den enkelte virksomheten å vurdere hvilke tiltak som er «gode nok» sett ut fra det trussel/risikobildet virksomheten er utsatt for.

Enheter og informasjon

Før du reiser, anbefaler vi at du vurderer behovet for å ta med deg en PC/enhet som inneholder virksomhetskritisk eller sensitiv informasjon. For de enhetene du velger å ta med, anbefaler vi at du sørger for at disse alltid er beskyttet med et godt passord/kode – ikke fødselsdatoer eller lignende som er lett å gjette. Videre er det viktig å sørge for å ha god fysisk kontroll på enhetene under hele reisen. Vi anbefaler derfor å ta med enhetene i håndbagasjen når du er ute og reiser. Sørg alltid for å låse enhetene/skru dem av når de ikke er i bruk.

- Hold enheter oppdatert med nyeste programvare/sikkerhetsoppdatering for å begrense sårbarheter på enheten. Dette gjelder også for applikasjoner du benytter.
- Bruk sikkerhetsprogramvare/antivirusprogramvare. –Vurder eventuelt om det er ønskelig å aktivere eventuelle tilleggsprodukter innenfor sikkerhet.

Dersom du av ulike årsaker er nødt til å ta i bruk et åpent nettverk, bør du i utgangspunktet legge til grunn at andre kan se hva du gjør.

- Bruk gode passord – jo lengre jo bedre.
- Vi anbefaler sterkt å aktivere to-faktor autentisering (MFA) der det er mulig. Dette er et enkelt og effektivt tiltak for å minimere risikoen for at utenforstående får tilgang til din konto og informasjon.
- Aktiver mulighet for fjernsletting av PC og mobil, slik at denne kan tømmes raskt dersom enheter blir mistet eller blir borte.

Under reisen

Vurder bruken av nettverk
Bluetooth og wifi bør være avslått når de ikke brukes. Åpne gjestenettverk er ofte dårlig sikret og bør derfor helst unngås når det er mulig. Dersom du har mulighet til å benytte 4G/5G nettverk istedenfor et åpent gjestenettverk vil det være et bedre sikkerhetsmessig valg. Grunnen til dette er at 4G-trafikken er kryptert mellom telefonen og basestasjonen.

Så lenge du er tilkoblet et nettverk som ikke er bedriftens eget, bør du bruke en VPN-tilkobling, dersom det er tilgjengelig og mulig å benytte der du befinner deg. Ved bruk av VPN vil all internett-trafikk være kryptert.

Dersom du av ulike årsaker er nødt til å ta i bruk et åpent nettverk, bør du i utgangspunktet legge til grunn at andre kan se hva du gjør. Du bør derfor unngå å logge på tjenester som inneholder viktig og sensitiv informasjon.

Bevissthet rundt tilkobling av enheter
Vær varsom med å koble til andre enheter til PCen/mobilen din, slik som minnepinner og printere, da disse potensielt kan inneholde skadelig programvare. Vær også forsiktig med å koble enheter til ladestasjoner da disse potensielt kan være tuklet med. Bruk derfor gjerne ordinær lader tilkoblet stikkontakt så langt det lar seg gjøre. Ha god kontroll på enhetene dine.

Unngå å la pc, mobil eller nettbrett ligge ubevoktet.

Når du kommer hjem

- Vær kritisk til ukjente e-poster/sikkerhetsvarsler.
- Om du har opplevd noe mistenkelig under reisen og er redd for at passord har kommet på avveie, anbefaler vi at du bytter disse.

Til slutt ønsker vi å understreke at det viktigste sikkerhetstiltaket er at du som bruker er bevisst på risikoen du er eksponert for og tar forholdsmessige forhåndsregler:

- Ikke trykk på linker du ikke vet hva er eller vedlegg fra ukjente.
- Ikke surf på tvilsomme nettsider.
- Ikke oppgi personlig informasjon til hvem som helst.
- Bruk to-faktor på alle kontoer og bruk gode og unike passord på alle brukerkontoene du har.

Frykten for inflasjonen

Da jeg vokste opp på 1970-tallet, skjedde det noe med en styrke som menneskeheten aldri hadde opplevd før – en global inflasjonsbølge som tilsynelatende ikke lot seg temme, skyllet over verden. Inflasjonen i det tiåret var mer for en langvarig storm å regne, enn bare et forbigående uvær.

Samfunnsøkonom
Jan Ludvig Andreassen
Sjeføkonom i Eika Gruppen

Det var først med omleggingen av pengepolitikken i 1980, da den amerikanske sentralbanken satte renta så høyt at økonomien fikk en dyp og seig lavkonjunktur, at man fikk bukt med den trøblete inflasjonen.

Stor smerte – stående applaus
Den økonomiske smerten var stor da rentene skjøt i været, men det betød ikke at den stramme pengepolitikken var upopulær. Da den økonomiske krisen var som verst, talte den amerikanske sentralbanksjefen Paul Volcker på en konferanse for boligbyggere. Dette var rentefølsomme bedrifter som var hardt rammet av det økonomiske tilbakeslaget som sentralbanken hadde forårsaket. Han forklarte at det å knekke inflasjonen var nødvendig, men dessverre kun mulig gjennom en smertefull hestekur med høye renter, mange konkurser og midlertidig ubehagelig stor arbeidsledighet. – Kan dere støtte meg slik at vi blir kvitt inflasjonsåket en gang for alle? – spurte han retorisk. Forsamlingen reiste seg, og ga ham stående applaus!

Hva er det som er så ille med inflasjonen?
Det er mye moralisme ute og går. Folk flest synes fortsatt at du skal ha lønn for innsats, ikke ved at eiendommer og andre investeringer skyter i været bare