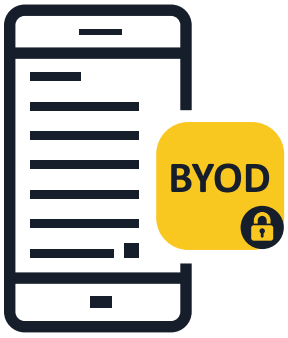
SKADEVARE PÅ MOBILEN

TIPS OG RÅD FOR VIRKSOMHETER

1 Informer ansatte om risiko ved bruk av mobile enheter

- Mobilbruk gjør skillet mellom jobb og fritid uklart. Bedrifter kan sterkt berøres av et angrep først rettet mot en enkeltpersons mobilenhet. En mobilenhet er en datamaskin og bør beskyttes som en.

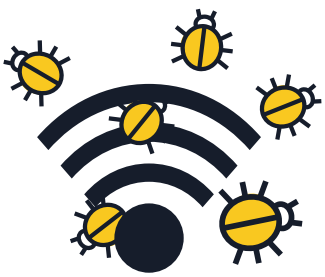


2 Implementer en policy for bruk av private enheter (Bring Your Own Device - BYOD) i bedriften

- Medarbeidere som bruker sine egne mobilenheter for å få tilgang til bedriftsdata (selv om det bare er e-post, kalender eller kontaktdatabase) må følge selskapets retningslinjer. Vær nøye med å velge hvilke teknologier som skal brukes for å administrere og sikre mobilenheter og oppfordre de ansatte til å utøve forsiktighet.

3 Inkluder retningslinjer for mobilsikkerhet som del av bedriftens sikkerhetsrammeverk

- Hvis en enhet ikke tilfredstiller kravene i sikkerhetsretningslinjer, bør den ikke få lov til å koble seg til bedriftsnettverket eller få tilgang til bedriftsdata. Selskaper bør ta i bruk deres egne løsninger for Mobile Device Management (MDM) eller Enterprise Mobility Management (EMM).
- For å supplere dette, er det kritisk å installere et system for å håndtere trussler på mobile enheter (Mobile Threat Defence solution). Dette vil gi forbedret synlighet og kontekstuell bevissthet over apper, nettverks- og operativsystemers trusselnivå.

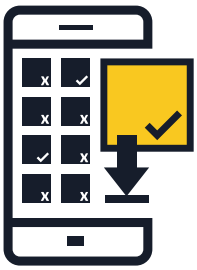


4 Vær forsiktig med å bruke offentlige WiFi-nettverk for å få tilgang til bedriftens data

- Generelt sett er offentlige WiFi-nettverk ikke sikre. Hvis en medarbeider får tilgang til bedriftsdata ved å bruke en gratis WiFi-tilkobling på en flyplass eller kafe, kan dataene eksponeres for ondsinnede brukere. Det anbefales at bedriften utvikler gode retningslinjer for slike situasjoner.

5 Hold enhetens operativsystemer og apper oppdaterte

- Anbefal de ansatte å laste ned oppdateringer til mobilenhetens operativsystem så snart den er tilgjengelig. Spesielt for Android, undersøk tjenesteleverandører og mobilprodusenters policy for oppdateringer. Å ha de nyeste oppdateringene vil sikre at enheten ikke bare er mer sikker, men også yter bedre.



6 Installer apper kun fra de offisielle butikkene

- Selskaper bør kun tillate installasjon av apper fra offisielle kilder på de mobilenhetene som kobler seg til bedriftsnettverket. Som et alternativ, vurder en egen applikasjonsbutikk for bedriften som sluttbrukere kan benytte til å laste ned og installere apper godkjent av bedriften. Konsulter din sikkerhetsleverandør for råd om oppsett, eller bygg din egen internt.

7 Unngå jailbreaking

- Jailbreaking er prosessen der man fjerner sikkerhetsbegrensningene påtvunget av operativsystemselgeren, og som gir full tilgang til operativsystemet og funksjonene. Jailbreaking av din egen enhet kan betydelig svekke dens sikkerhet, og åpner sikkerhetshull som ellers ikke er åpenbare/tilgjengelige. En jailbreaket enhet bør ikke tillates i selskapets miljø.

8 Vurder skylagringsalternativer

- Mobilbrukere vil ofte ha tilgang til viktige dokumenter ikke bare via jobb-PCene men også fra sin private telefon eller nettbrett utenfor kontoret. Selskaper bør vurdere å bygge en sikker skybasert lagring og filsynkroniseringstjenester for å legge til rette for slike behov på en sikker måte.

9 Oppfordre staben til å installere en app for mobilsikkerhet

- Alle operativsystemer står i fare for infeksjon. Hvis tilgjengelig, sørg for at de bruker en mobilsikkerhetsløsning som oppdager og forhindrer malware, spyware og ondsinnede apper, i tillegg til andre personverns- og tyverisikre funksjoner.

EUROPOL EC3 European Cybercrime Centre

POLITIET

CCIS

NTNU Norwegian University of Science and Technology

NorSIS Norsk senter for informasjonssikring

#MobileMalware