CENTER FOR CYBERSIKKERHED

Vejledning

Cybersikkerhed på rejsen – organisationens ansvar

Organisationen og ledelsen skal sørge for, at medarbejderne kan arbejde sikkert, når de rejser i arbejdsøjemed.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

Forsideillustration: Sergey Furtaev / Shutterstock

1. udgave januar 2022

Indledning

Både data og medarbejdere er vigtige aktiver for en moderne organisation. Så når både medarbejder og data befinder sig uden for organisationens vante, fysiske rammer, er det nødvendigt med ekstra sikkerhed. Derfor er det en vigtig opgave for ledelsen at sørge for, at organisationen kan håndtere sikkerheden for medarbejdere, der rejser som en del af deres arbejde.

Denne vejledning indeholder både råd til ledelsen og til resten af organisationen, som skal føre ledelsens beslutninger ud i livet. Vejledningen indeholder et kapitel om, hvordan rejser bør indgå i organisationens generelle risikovurdering, herunder at det er ledelsens ansvar at sikre, at der bliver udarbejdet en rejsepolitik. Derudover indeholder vejledningen et kapitel om nogle af de praktiske tiltag, som organisationen bør anvende for at sikre data og støtte medarbejderne på rejser.

Organisationer er forskellige. Denne vejledning tager udgangspunkt i en tilgang baseret på en risikovurdering. Men det er op til den enkelte organisation, hvordan den foretager risikovurderingen, og hvordan organisationen forankrer, formulerer og implementerer en rejsepolitik.

Man kan finde yderligere inspiration i Center for Cybersikkerheds vejledning "Opdater sikkerhedspolitikkerne til en 'ny normal'". Den handler om distancearbejde, og mange af de samme aspekter går igen i forbindelse med rejser.

Overordnede anbefalinger

Det er ledelsens ansvar at sætte rammerne for organisationens sikkerhed. Det gælder også sikring af data og information, når medarbejdere rejser som led i deres arbejde. Ledelsen skal kende til truslerne og til de sårbarheder, der er forbundet med rejser. Der skal laves en risikovurdering for rejser. På den baggrund skal der udarbejdes en rejsepolitik, som konkretiserer de tiltag, der skal sikre organisationen i forbindelse med rejser. Risikovurdering og rejsepolitik skal opdateres løbende. Ledelsen skal desuden sikre, at der afsættes de nødvendige ressourcer til at implementere rejsepolitikken i praksis.

Samlede anbefalinger på kort form

- Tænk rejser ind i organisationens risikoarbejde.
- Kend trusselsbilledet i de lande, I rejser til.
- Skab overblik over informationer, der må tilgås på rejser.
- Lav en rejsepolitik.
- Afsæt ressourcer til alle tiltag.

Ledelsens ansvar

Det er ledelsen, der har ansvaret for at sætte de overordnede rammer for organisationens sikkerhed, herunder sikkerheden i forbindelse med forretningsrejser. Ledelsens arbejde bør bygge på en risikovurdering. Det er ledelsens opgave at kende truslerne ved rejser, vurdere risikoen og på den baggrund udstikke retningslinjer og vejledning, der hjælper med at beskytte organisationen. Det er også ledelsens ansvar, at retningslinjerne implementeres og når ud til de medarbejdere, der rejser.

Vurder risici forbundet med rejser

For at kunne vurdere hvilke risici man potentielt er udsat for i forbindelse med rejser, må man først forstå, hvordan organisationen kan blive ramt. Indledningsvis kan det være en god ide, at fokusere på de områder, hvor man har en konkret frygt eller bekymring for at noget går galt. Denne frygt eller bekymring kan være baseret på faktuel viden om sårbarheder i organisationen, konkrete trusler i specifikke lande eller omfattende konsekvenser, hvis man bliver ramt. Men frygten eller bekymringen kan også blot være bundet op på formodninger eller rygter.

Ledelsen kan derfor stille enkle spørgsmål som for eksempel: "Hvad er vi bekymrede for kan ske, hvis en medarbejder mister sin pc på rejsen?". Ved at spørge ind til bekymringerne ved trusler og sårbarheder kan man nå frem til en samling udsagn, der indeholder de væsentligste risici. Som for eksempel:

> "Vi er bekymrede for, at vores ledelses interne kommunikation omkring kontraktforhandlingerne i udlandet falder i modpartens hænder."
>
> "Vi er bekymrede for, at vores medbragte foreløbige forskningsresultater falder i hænderne på vores konkurrenter."
>
> "Vi er bekymrede for, at medbragt udstyr kompromitteres med malware eller bagdøre, så uvedkommende kan tilgå vores interne netværk."
>
> "Vi er bekymrede for, at vores medarbejdere ikke kan tilgå relevante informationer og it-ressourcer under deres rejse som følge af fejl, tab af udstyr eller kommunikationsproblemer."
>
> "Vi er bekymrede for, at medarbejderen ikke er i stand til at handle på sikker vis, hvis der opstår en uventet situation."
>
> "Vi er bekymrede for, at medarbejdernes adfærd ikke i tilstrækkelig høj grad sikrer organisationens kritiske aktiver."

Det er dog ikke nødvendigvis alle relevante risici, der bliver fanget på denne måde. Ledelsen bør derfor også foretage en mere systematisk vurdering af såvel trusler og sårbarheder.

Trusler på rejsen

På en rejse er der trusler ud over dem, der er relevante til hverdag. For eksempel kan medarbejderen glemme en bærbar pc med vigtige dokumenter i en taxa på vej fra hotellet til lufthavnen. Eller det trådløse netværk til en konference kan være overvåget af hackere, der arbejder på vegne af en konkurrent eller fremmed stat.

Når man fokuserer på potentielle trusler i forbindelse med rejser, bør man være opmærksom på følgende punkter:

- Mange trusler er altid til stede og gælder både, når medarbejderen sidder på kontoret, arbejder hjemmefra eller er på rejse i udlandet.
- Trusler og sårbarheder varierer fra organisation til organisation. Det land, hvor medarbejdere fra den ene organisation kan rejse med lav risiko, kan være et højrisikoland for en anden organisation. Visse brancher er for eksempel mere udsatte for industrispionage end andre.
- Trusler kan være målrettet nogle medarbejdere og ledelsen, da de eksempelvis kan være adgangsvejen til vigtige eller kritiske oplysninger. Ingen rejsende bør dog anse sig selv som irrelevant i denne sammenhæng.
- Trusler kan være højere, hvis kritiske eller specielt værdifulde informationer medbringes på rejsen.
- Truslerne varierer fra land til land. Visse trusler er højere i nogle lande, men hvilke lande det drejer sig om, afhænger af den enkelte organisation.
- Rejsens formål kan også øge truslen. Rejser man eksempelvis for at deltage i en konference eller for at deltage i et vigtigt møde?
- Mange af truslerne kan ramme én og samme sårbarhed, lige som en trussel kan ramme flere sårbarheder.

For at vurdere de konkrete trusler kan ledelsen for eksempel spørge:

- "Er der tale om et land, vi rejser til ofte?"
- "Kender vi regionen, landet, området eller byen godt?"
- "Har vi medarbejdere fast i landet?"
- "Har vi et kontor der?"
- "Bruger vi de lokale kommunikationsplatforme, sociale medier og betalingssystemer?"
- Medbringer vi kritiske, følsomme eller meget værdifulde informationer på rejsen?
- "Er vi i tvivl om, hvorvidt rejsen gennemføres på betryggende vis?"
- "Opfatter organisationen landet som et højrisikoland?"

For de generelle cybertrusler kan man bruge Center for Cybersikkerheds trusselsvurderinger. Til støtte i vurderingen af truslerne kan man med fordel anvende Udenrigsministeriets rejsevejledninger for de pågældende lande.

Anbefaling: Kend trusselsbilledet i de lande, I rejser til
Organisationen bør vurdere, om der er specifikke lande, hvor der er særlige risikomæssige forhold, der gør sig gældende. Brug Center for Cybersikkerheds trusselsvurderinger og Udenrigsministeriets rejsevejledninger som støtte.

Sårbarheder på rejsen

For at en given trussel i sidste ende kan resultere i en risiko for organisationen, skal der være en sårbarhed, som truslen kan udnytte.

Sårbarheder er typisk bundet op på specifikke aktiver som eksempelvis den rejsende medarbejder, det medbragte udstyr samt kommunikationen mellem medarbejder/udstyr og omverdenen, herunder organisationen der hjemme. For eksempel:

- En medarbejder kan være sårbar som følge af uhensigtsmæssig adfærd ifm. arbejdsopgaver, der udføres uden for organisationen.
- Medarbejderens pc kan være sårbar som følge af manglende opdatering af software.
- En telefonsamtale mellem medarbejderen og organisationen kan være sårbar som følge af utilstrækkelig kryptering – eller fordi den foregår i et åbent rum.

Ledelsen bør involvere relevante parter i forbindelse med identifikation af sårbarheder. Det kan eksempelvis være organisationens it-funktion i forbindelse med afdækning af tekniske sårbarheder.

Risikoen ved rejser

Når ledelsen har identificeret trusler og sårbarheder, skal risikoen vurderes. De to elementer i risiko er sandsynlighed og konsekvens. Mens sandsynligheden kan være svær at vurdere, så er konsekvenserne ofte nemmere at anskueliggøre.
Samlet set bør man afklare, hvorledes de identificerede forhold (trusler, sårbarheder og konsekvenser) passer ind i organisationens generelle risikobillede og dermed generelle risikohåndtering. Er forholdene allerede dækket af identificerede risici, eller er forholdene ikke dækket.

Når man rejser, skal man være opmærksom på, at der er nye sårbarheder. Samtidig blotter man nogle af de sårbarheder, man har beskyttet medarbejderne for på kontoret.

Anbefaling: Tænk rejser ind i organisationens risikoarbejde
Alle rejseaktiviteter bør være underlagt organisationens generelle risikostyring.

Sikkerhedspolitik for rejser

Ledelsen har ansvaret for at udarbejde en it-sikkerhedspolitik. Tilsvarende bør der udarbejdes en politik for sikkerhed ved rejser. Det kan være som et tillæg eller en integreret del af den generelle it-sikkerhedspolitik.

Sikkerhedspolitikken skal tage udgangspunkt i risikovurderingen. It-sikkerhedspolitikken skal tage hånd om de bekymringer, der er identificeret. Risikoen kan aldrig helt elimineres, men den kan reduceres. Et element er teknik, men processer, adfærd og støtte fra organisationen er lige så vigtigt.

Rejsepolitikken

Rejsepolitikken skal udstikke de konkrete rammer for organisationens arbejde med at sikre data og medarbejdere på rejser. Den skal være konkret, håndgribelig og principiel, så den både kan anvendes som praktisk støtte ved planlægning af rejser, men også hjælpe, når noget uforudset opstår.

Ledelsen bør følge op på rejsepolitikken hvert år. Det kan for eksempel ske i forbindelse med opdatering af organisationens risikovurdering.

Ligesom den generelle it-sikkerhedspolitik skal rejsepolitikken afspejle topledelsens holdning til organisationens risikoappetit i forhold til det aktuelle risikobillede. Det skal udmøntes i konkrete regler og retningslinjer. Rejsepolitikken skal også gøre det klart, hvem der har ansvar for hvad og hvornår. Det er op til den enkelte organisation at finde frem til den ansvarsfordeling, der passer bedst til måden, hvorpå organisationen har fordelt arbejdsopgaverne med både håndtering af it og it-sikkerhed.

For at fungere som et dokument, der kan anvendes af organisationen i praksis, bør rejsepolitikken konkret dække en række emner:

- Fastlæggelse af roller og ansvar i forbindelse med rejser.
- Bestemmelse af et centralt sted, der støtter medarbejderne it- og vidensmæssigt med cybersikkerhed på rejser.
- Afklaring af, hvem der godkender eventuelle behov for at afvige fra retningslinjerne.
- Eventuelle sammenhænge med andre politikker og retningslinjer.
- Retningslinjer for hvilke informationer og systemer, der må tilgås og ikke tilgås under rejser.
- Retningslinjer for særlige rejsemål og højrisikolande.
- Retningslinjer for, hvornår medarbejderne kun må medbringe særligt it-udstyr på rejsen.
- Beskrivelse af særligt it-udstyr, der skal være til rådighed for rejsende medarbejdere.
- Beskrivelse af, hvordan særligt udstyr til rejser skal håndteres efter hjemkomsten.

- Beskrivelse af, hvordan sikkerhedshændelser og andre krisesituationer skal håndteres, herunder hvordan medarbejderen kan rapportere en sikkerhedshændelse.
- Procesbeskrivelse for opsamling af medarbejderes oplevelser og erfaringer med it-sikkerhed på rejser.
- Beskrivelse af hvornår, hvordan og i hvilket omfang medarbejderne skal briefes før afrejse og de-briefes ved hjemkomst.
- Retningslinjer for sikkerhedsmæssig adfærd på rejser.

Anbefaling: Lav en rejsepolitik
Topledelsens holdning til, hvordan organisationens systemer, data og informationer må anvendes og tilgås på en rejse, skal nedfældes i organisationens rejsepolitik. Denne politik skal samle organisationens risikobillede og risikoappetit i forhold til rejser og konkretisere det i en række regler og retningslinjer.

Begræns adgang

Begrænsning af adgang er måske den vigtigste overordnede politik. Sårbarhederne er ofte tilknyttet adgang til data, og visse data er mere følsomme end andre for organisationen. For at mindske risikoen bør man derfor som det første skridt skabe et overblik over, hvilke data og informationer der må tilgås på rejser. Som hjælp til at skabe overblik kan man for eksempel spørge:

> "Er der informationsaktiver, der er så følsomme, at de normalt ikke må medbringes, tilgås eller omtales uden for organisationens fysiske rammer?"
>
> "Hvordan kan man bedst beskytte de informationer, der medbringes, både i relation til fortrolighed, integritet og tilgængelighed?"
>
> "Hvordan kan vi sikre vores medarbejderes adgang til kritiske informationer, hvis de har behov for at tilgå dem på rejsen?"
>
> "Hvordan kan vi sikre, at vi ved, hvad der tilgås på rejsen, og hvor kan vi tjekke, at medbragte data eller informationer ikke er blevet ændret?"

Anbefaling: Skab overblik over informationer, der må tilgås på rejser
Organisationen bør have klare regler og procedurer for, hvilke informationsaktiver der må medbringes og tilgås på rejser. Det skal fremgå, hvorvidt adgangen afhænger af andre forhold som for eksempel det land, der rejses til.

Rejsepolitikken i praksis

Organisationen bør afsætte ressourcer til, at rejsepolitikken kan efterleves i praksis. Det er topledelsens ansvar at afsætte de nødvendige ressourcer.

For eksempel bør man sikre, at der er det nødvendige personale til støttefunktioner, udstyr til rejsende og ressourcer til at uddanne medarbejdere og opbygge viden om sikkerhed ved rejser i organisationen. Uden de fornødne ressourcer er det svært at opfylde intentionerne om at sikre organisationen og medarbejderne i forbindelse med rejser.

Anbefaling: Afsæt ressourcer til alle tiltag

Ledelsen bør sikre, at der afsættes de nødvendige ressourcer til både det forebyggende og det opfølgende arbejde før, under og efter rejser.

Understøttelse af sikkerhed på rejser

Forberedelse, støtte og opfølgning er forudsætninger for en sikker rejse. Her spiller it-afdelingen en central rolle. I praksis afhænger sikkerheden i forbindelse med rejser af, at den understøttes af en række funktioner i organisationen. It-afdelingen og den funktion, der håndterer sikkerhed, er derfor vigtige aktører i implementeringen af ledelsens retningslinjer.

Uafhængig af om medarbejderen medbringer sine standard it-arbejdsenheder eller lånt udstyr, bør it-afdelingen være klar til at bistå medarbejderen før, under og efter rejsen med råd og vejledning i sikker brug af de it-løsninger, som medarbejderen har behov for at have adgang til. Uden nogen form for støtte er der risiko for, at medarbejdere, der ikke har tilstrækkelig viden om sikker it-anvendelse, netop udsætter sig selv og organisationen for unødig risiko både under, men også efter rejsen er gennemført.

Før rejsen

Det er vigtigt at organisationen har processer på plads, der forud for en rejse kan hjælpe medarbejderne med at agere sikkert på rejsen.

Anbefalinger til it-afdelingen før en rejse

- Udarbejd retningslinjer og rutiner for støtte i forbindelse med rejser.
- Opbyg en pulje af it-udstyr og -tjenester til udlån ved rejser.
- Synliggør rammerne for it-support under rejsen.
- Sikring af it-udstyr, der medbringes på tjenesterejser.
- Aktiver kryptering af alle lagerenheder, der skal medbringes på tjenesterejser.
- Aktiver internetdeling og data roaming på medarbejderens arbejdstelefon.
- Ekstern adgang til organisationens interne systemer bør beskyttes med VPN.
- Ekstern adgang til organisationens interne systemer bør beskyttes med flerfaktor-autentifikation.
- Etabler backup-funktion, så interne informationer og data på medarbejderens pc kan sikres inden tjenesterejse.
- Stil om nødvendig sikkerhedsposer til rådighed for medarbejdere, der skal på tjenesterejse.

Udarbejd retningslinjer og rutiner for støtte i forbindelse med rejser

It-afdelingen bør støtte organisationen og medarbejderne før, under og efter tjenesterejser. Dette gælder både i relation til udlån af it-udstyr, samt bistand med råd og vejledning før, under og efter rejsen i, hvorledes it-udstyr anvendes sikkert, når det medtages på rejser. Arbejdet med disse opgaver skal ske på baggrund af ledelsens sikkerheds- og rejsepolitikker. It-afdelingen bør derfor udarbejde retningslinjer og rutiner, således at de kan være forberedt på at hjælpe en medarbejder i forbindelse med en tjenesterejse.

It-afdelingen bør samtidig overveje at udarbejde en kort skriftlig guide, som medarbejderen kan medbringe på rejsen. Heri bør der ud over gode råd og tips også stå oplysninger om, hvordan medarbejderen kan henvende sig til en kontakt i it-afdelingen, hvis der opstår problemer.

Synliggør rammerne for it-support ved rejser

For at medarbejderne kan gøres bevidst om, hvilken hjælp de kan få i forbindelse med tjenesterejser, anbefales det, at rammerne for it-afdelingens hjælp og bistand synliggøres på organisationens intranet. Eventuelle tidsfrister for anmodning om bistand bør ligeledes fremgå. Det samme bør reglerne for at tilsidesætte tidsfristerne.

Opbyg en pulje af it-udstyr og -tjenester til udlån ved udenlandsrejser

It-afdelingen bør stille relevante it-løsninger til rådighed for medarbejderen til brug under deres tjenesterejser. Det skal ske på baggrund af organisationens rejsevejledning og generelle overvejelser omkring risici.

Konkret kan det dreje sig om:

- Hardware (telefoner, tablets, pc'er, lagermedier).
- Supplerende udstyr (strømforsyninger, powerbank, kabler, konverterstik, skærmfilter mv.).
- Supplerende applikationer. Her tænkes eksempelvis på applikationer, der understøtter afholdelse af virtuelle møder. Se eventuelt CFCS' vejledning om "Råd om sikkerhed på virtuelle mødeplatforme".
- Tjenester (for eksempel ekstern mail-service, sikker fil-udveksling, sikker chat eller sikker telefoni).

Sikring af it-udstyr, der medbringes på rejser

It-afdelingen skal i forbindelse med udlån af udstyr sikre, at udstyret har fået de seneste relevante sikkerhedsopdateringer installeret og er konfigureret i overensstemmelse med organisationens sikkerhedspolitikker og retningslinjer. Herunder at der er foretaget en begrænsning af funktionaliteten til de applikationer og funktioner, som organisationen har godkendt. Herved er de med til at minimere risikoen for, at udstyret kompromitteres, når det benyttes uden for organisationens interne netværk.

Hvis medarbejderen skal medbringe organisationens standard it-arbejdsenheder, skal it-afdelingen om nødvendigt bistå med sikre disse yderligere i henhold til organisationens retningslinjer. Se i øvrigt CFCS' vejledning om "Sikkerhed på mobile enheder".

Endelig bør it-afdelingen om nødvendigt afprøve medarbejderens it-løsning sammen med medarbejderen. På den måde sikres det, at løsningen fungerer efter hensigten, og at medarbejderen forstår at bruge den efter de beskrevne retningslinjer.

Aktiver drevkryptering på alle lagerenheder, der skal medbringes på tjenesterejser.

Når it-udstyr og eksterne lagringsmedier som eksempelvis USB-lagerenheder bringes uden for organisationens fysiske rammer, bør der anvendes kryptering. Det sikrer blandt andet fortroligheden af de informationer, der ligger på lagermediet.

Normalt er it-udstyr og lagringsmedier beskyttet af organisationens interne sikkerhedsløsninger. Men når it-udstyr og lagringsmedier bringes uden for organisationen, skal de sikres i henhold til det ændrede risikobillede. It-afdelingen skal derfor specifikt sørge for, at it-udstyr, der medbringes på tjenesterejser anvender fuld diskkryptering.

Aktiver internetdeling og data roaming på medarbejderens arbejdstelefon

Risikoen for en kompromittering af medarbejderens it-udstyr og organisationens systemer øges, hvis der anvendes usikre, åbne wifi-netværk. It-afdelingen bør derfor medvirke til, at medarbejderne vælger en mere sikker netværksopkobling på tjenesterejser. Derfor bør man åbne op for medarbejders brug af arbejdsmobiltelefonens funktion til internetdeling (hotspot-funktion). Denne funktion skal beskyttes med kode. Bemærk at dette kan kræve ændringer i medarbejderens mobiltelefonabonnement.

Ekstern adgang til organisationens interne systemer bør beskyttes med VPN.

CFCS anbefaler generelt altid at anvende VPN i forbindelse med ekstern adgang til organisationens interne systemer og informationer. Det er særlig vigtigt i forbindelse med ekstern adgang fra udenlandske lokaliteter.

Når VPN anvendes i andre lande, kan der være tekniske og lovmæssige begrænsninger, som har betydning for funktionaliteten af VPN-løsningen. It-afdelingen bør bistå medarbejderne i en afdækning af sådanne udfordringer og eventuelt tilbyde alternative løsninger.

Ekstern adgang til organisationens interne systemer bør beskyttes med fler-faktor autentifikation.

CFCS anbefaler generelt, at der altid anvendes fler-faktor-autentifikation (MFA) i forbindelse med ekstern adgang til interne systemer og informationer. Det er ekstra vigtigt i forbindelse med rejser.

Etabler backup-funktion, så interne informationer og data på medarbejderens pc kan sikres inden tjenesterejse.

Der bør altid foreligge en intern kopi, hvis en medarbejder medbringer informationer og data, der ligger lokalt på deres it-udstyr. Herved er informationer og data sikret i tilfælde af, at medarbejderens it-udstyr mistes eller ødelægges. Det anbefales derfor, at it-afdelingen etablerer en backup-funktion, der gør det let for medarbejderne at tage en fuld backup af deres it-udstyr, inden de medbringer det på en rejse.

Stil om nødvendigt sikkerhedsposer til rådighed for medarbejdere, der skal på tjenesterejse

I tilfælde af at en medarbejder medbringer særlig følsom information, kan det være en løsning at anvende såkaldte sikkerhedsposer. Især hvis viden om en potentiel kompromittering er væsentligt. Sikkerhedsposer er for eksempel specielle forseglede plastposer eller tasker med plombering, hvor det er muligt at se, om der har været uvedkommende, som har forsøgt at få adgang til indholdet. Det er dog vigtigt at være opmærksom på, at traditionelle sikkerhedsposer ikke forhindrer en kompromittering. De kan derimod synliggøre, om det kan være sket.

Under rejsen

Ligesom i hverdagen kan det være nødvendigt for medarbejderen at komme i kontakt med it-afdelingen for at få teknisk hjælp. For rejsende medarbejdere kan både praktiske problemer som tidsforskel i forhold til normal kontortid og de særlige sikkerhedsmæssige udfordringer gøre det væsentligt at have et kontaktpunkt hos it-afdelingen.

Anbefalinger til it-afdelingen under rejsen

- Etabler en ”hotline”/supportmulighed tilgængelig for medarbejderne på rejse.
- Etabler et fast kontaktpunkt til brug for rejsende medarbejderes rapportering af sikkerhedsrelaterede hændelser.
- Sikkerhedsopdatering af medbragt it-udstyr bør ske uafhængigt af, om udstyret fysisk befinder sig i eller uden for organisationen.

Etabler en ”hotline” eller supportmulighed tilgængelig for medarbejdere på rejse

Når en medarbejder rejser, skal det være muligt at få hjælp fra it-afdelingen, hvis teknikken driller, fejler, eller man har været ude for en hændelse som eksempelvis tab af udstyr. Uafhængig af, hvor eller hvornår det sker, bør der være et kontaktpunkt, som medarbejderen altid kan få fat i. Afhængig af den konkrete situation vil der ellers være risiko for, at medarbejderen ikke kan udføre sine opgaver. Eller at medarbejderen forsøger at omgå problemerne og dermed potentielt udsætter sig selv eller organisationen for it-sikkerhedsmæssige risici. Bemærk, at supportfunktionen også bør være tilgængelig uden for almindelig arbejdstid i Danmark, især hvis medarbejdere rejser i andre tidszoner.

It-afdelingen skal også være klar til at tilbyde eller etablere alternative løsninger, hvis en medarbejder står i en situation, hvor den medbragte it-løsning er utilstrækkelig.

Etabler et kontaktpunkt til brug for rejsende medarbejderes rapportering af sikkerhedsrelaterede hændelser

Hvis medarbejderen kommer ud for en sikkerhedsrelateret hændelse, er det vigtigt, at organisationen får besked så hurtigt som muligt. Dermed kan eventuelle konsekvenser for medarbejderen eller organisationen afbødes i størst mulig omfang. Organisationen bør derfor have ét specifikt kontaktpunkt, hvor medarbejderen kan rapportere hændelsen. Det kan være hensigtsmæssigt, at dette kontaktpunkt er sammenfaldende med det, medarbejderen kan anvende i tilfælde af behov for teknisk support. Det kan altså være it-afdelingen, der tager imod henvendelsen fra medarbejderen, selvom sikkerhedsområdet er forankret uden for it-afdelingen.

Sikkerhedsopdatering af medbragt it-udstyr bør ske uafhængig af om udstyret er i eller uden for organisationens fysiske lokalitet.

It-afdelingen skal aktivt bidrage til, at medarbejderens medbragte it-udstyr løbende holdes opdateret og fri for malware. Hvis softwaren på det medbragte it-udstyr ikke opdateres i løbet af rejsen, risikerer man, at alvorlige sårbarheder i softwaren står åbne for angreb. Dermed øges risikoen for en kompromittering af it-udstyret og potentielt også organisationen derhjemme. Hvis organisationens sædvanlige processer for sikkerhedsopdateringer ikke fungerer med distance-arbejdspladser, anbefales det derfor, at man bruger leverandørens indbyggede automatiske opdateringsfunktion.

Efter rejsen

Når en medarbejder har afsluttet sin rejse, er der en risiko for, at medarbejderen hjembringer kompromitteret it-udstyr. Principielt kan dette ske ved en vilkårlig rejse, men særligt ved rejser til højrisikolande skal it-afdelingen være meget opmærksom på denne risiko.

Efter rejsen

- Der skal være mulighed for en gennemgang og sletning af medbragt it-udstyr.
- Alt låneudstyr bør inddrages og herefter slettes efter gennemført rejse.
- Der skal være mulighed for de-briefing af medarbejdere.
- Der skal følges op på alle rejserelaterede sikkerhedshændelser.

Der skal være mulighed for de-briefing af medarbejdere

Har medarbejderen mistanke om en potentiel kompromittering i forbindelse med en rejse, bør der være mulighed for de-briefing af medarbejderen. På den måde kan erfaringerne indgå i organisationens samlede læringsproces. Rammerne for en sådan de-briefing skal dokumenteres i rejsepolitikken.

Der skal være mulighed for en gennemgang og sletning af medbragt it-udstyr

Når en medarbejder vender hjem fra en rejse, kan der under visse omstændigheder være et behov for en gennemgang af medarbejderens it-udstyr. Det kan for eksempel være ved mistanke om kompromittering. I den forbindelse bør it-afdelingen også vurdere, om it-udstyret skal gennemgås af sikkerhedsspecialister med henblik på en afdækning af omfang og karakter af den mulige kompromittering, eller om it-udstyret skal slettes og derefter geninstalleres, eller i særlige tilfælde bortskaffes forsvarligt. Retningslinjer for hvornår og hvordan det bør ske skal dokumenteres i rejsepolitikken.

Alt låneudstyr bør inddrages og herefter slettes efter gennemført rejse

I tilfælde af at medarbejderen har lånt it-udstyr til brug under en rejse, skal it-afdelingen sikre, at det afleveres igen. Herefter skal it-afdelingen afgøre, hvorvidt det udlånte udstyr skal undergå en total sletning af indbyggede lagerenheder, eller om det ligefrem bør destrueres. Dette afhænger blandt andet af, hvortil rejsen er foretaget, samt om der er konstateret eller er mistanke om kompromittering af it-udstyret under rejsen.

Der skal følges op på alle rejserelaterede sikkerhedshændelser

Hvis der reelt har været en sikkerhedsmæssig hændelse, bør it-afdelingen sikre, at hændelsen registreres, og at der følges op på den. Herved kan sikkerhedshændelsen også indgå i organisationens læringsproces.

Rejser til højrisikolande

Der kan være en særlig høj risiko ved at rejse til visse lande. Organisationen kan kategorisere disse lande som højrisikolande. Det kan eksempelvis være lande, hvor hacker-grupper i særlig grad har intentioner om og kapacitet til at indhente kommercielle og beskyttelsesværdige oplysninger fra digitale enheder og netværk. Andre lande kan også være højrisikolande ud fra organisationens specifikke kontekst og virke. Rejser man til disse lande, bør man tage særlige forholdsregler.

Disse forholdsregler bygger derfor oven på både organisationens grundlæggende sikkerhedsniveau og på den generelle rejsepolitik.

Ledelsens ansvar ved rejser til højrisikolande

- Rejsepolitikken bør indeholde et afsnit med en liste over højrisikolande. Desuden bør der være en beskrivelse af, hvordan medarbejderne og organisationen opretholder det ønskede sikkerhedsniveau i rejser til disse lande.
- Ledelsen bør følge udviklingen i de højrisikolande, der rejses til, og gennemføre en særlig risikovurdering og opdatere rejsepolitikken ud fra den.
- Alle informationsaktiver, som medbringes eller tilgås på tjenesterejser til højrisikolande, bør være vurderet og kategoriseret ud fra deres værdi for organisationen.
- Ledelsen bør til enhver tid kunne få et overblik over, hvilke informationsaktiver der medbringes eller tilgås under rejser til højrisikolande.
- Der bør foreligge særlige retningslinjer og prioriteres ressourcer til indkøb og installation af særligt rejse-it-udstyr til brug i forbindelse med rejser til højrisikolande.

Organisatorisk støtte til rejser til højrisikolande

- Hav en udlånspulje af it-udstyr, som udelukkende bruges i forbindelse med rejser til højrisikolande. Denne pulje skal kunne stilles til rådighed med kort varsel.
- Tag stilling til, om der skal stilles en alternativ mailkonto til rådighed for medarbejderen for at undgå, at den normale arbejdsmail bliver kompromitteret på rejsen.
- Alt it-udstyr, som har været med på rejsen, bør makuleres eller bortskaffes. Passwords til tjenester, der er tilgået, bør skiftes.
- Overvej om medarbejderens familie skal have en lånetelefon, så medarbejderens privatliv også sikres.

Referencer

Center for Cybersikkerhed (2021): *Cyberforsvar der virker*

Center for Cybersikkerhed (2020): *Beskyt din organisation mod phishing*

Center for Cybersikkerhed og Digitaliseringsstyrelsen (2021): *Opdater sikkerhedspolitikkerne til en »ny normal«*

Center for Cybersikkerhed (2021): *Råd om sikkerhed på virtuelle mødeplatforme*.

Center for Cybersikkerhed og Digitaliseringsstyrelsen (2021): *God kultur ved distancearbejde*

Center for Cybersikkerhed og Politiets Efterretningstjeneste (2018): *Råd om sikkerhed på mobile enheder*

Politiets Efterretningstjeneste: Sikkerhed på tjenesterejsen

Udenrigsministeriet: Rejseklar-app