RÅD FRÅN MSB

Till dig som samordnar organisationens informationssäkerhet när flera arbetar på distans

När många arbetar hemifrån leder det till att information hanteras på ett sätt som varken vi eller våra it-system är vana vid. Det i sin tur kan resultera i negativa konsekvenser för verksamheten. Här kommer råd till dig som ansvarar för organisationens informationssäkerhet.

Vilka regler gäller för distansarbete och användningen av it-system utanför organisationen? Är reglerna aktuella och relevanta eller behöver de snabbt förbättras? Kommunicera och påminn alla medarbetare om reglerna. Se till att de är lätta att hitta och publicera dem gärna på intranätet.

Vilken kapacitet har organisationen avseende hur många som kan arbeta på distans? Om ni har begränsningar i antal möjliga distansuppkopplingar behöver viktig verksamhet prioriteras och annat arbete göras lokalt på datorn, utan uppkoppling. Det kräver struktur och samordning. Se över möjligheterna att några medarbetare kan koppla upp sig på olika tider för att exempelvis hämta dokument från server till dator. På så sätt kan fler arbeta lokalt till dess att ni fått fler uppkopplingar eller mer utrymme.

Finns säkra inloggningar för distansarbete? Säkerställ att it-funktionen har de resurser som krävs för att upprätthålla säkra inloggningar för distansarbete, installera säkerhetsuppdateringar snabbt och hantera incidenter med mera. Läs mer på https://cert.se/2020/03/sakerhet-och-infrastruktur-vid-arbete-hemifran om vilka åtgärder som kan behöva göras.

Incidenter behöver hanteras skyndsamt. Säkerställ att incidenter fångas upp och följs upp så snart som möjligt så att ni snabbt kan åtgärda sårbarheter som har uppstått på grund av ändrade förutsättningar.

Finns säkra arbetssätt för behörighetstilldelning vid distansarbete? Säkerställ att den interna supporten arbetar enligt reglerna för behörighetstilldelning för uppkoppling vid distansarbete. Var medveten om att det kan förekomma falska samtal om lösenordsåterställning och även falska inloggningslänkar. Eventuell avvikelse från reglerna kan ske först efter medvetna riskbeslut.

Har ni antagit kontinuitetsplaner? Säkerställ att dessa följs. Om det saknas planer kan du stötta genom att få igång ett samtal om vilka delar i verksamheten som är kritiska för organisationen. Mer information om kontinuitetshantering för informationstillgångar finns i Metodstödet för systematiskt informationssäkerhetsarbete via www.informationssakerhet.se/metodstodet/utforma/#kontinuitetshantering-för-informationstillgångar-anchor. Information om kontinuitetshantering för andra tillgångar finns på www.msb.se/kontinuitetshantering.

Kommunicera till ledningen regelbundet, kort och koncist. Redogör för vad ni gör, varför och förklara risker och dess konsekvenser. Var aktiv och bidra med beslutsunderlag så att ledningen kan fatta riskmedvetna beslut.

Skjut upp inplanerade icke nödvändiga systemändringar.

Har du fler frågor? Kontakta oss via informationssakerhet@informationssakerhet.se

MSB Myndigheten för samhällsskydd och beredskap