

Checklista - grundläggande cybersäkerhet

Organisatoriska säkerhetsåtgärder		Ja	Nej	Inte tillräckligt
	Behörigheter (läs, skriv, ingen)			
	Lagring (veta var, hur, vem ansvarar)			
	Säkerhetskopia (rutin)			
	Dela (känslig, affärskritisk, publik)			
	GDPR (kunskap om)			
	Utbildning (SME säkerhetsskyddsamordnare) samt olika utbildningar för personalen i cybersäkerhet			
	Policys (informationshantering)			
	Dataskyddsombud (DPO)			

Medvetenhet

	Förståelse för effekterna för företagets cybersäkerhet (eller brist därav) t.ex., kostnader, regelbrott, kundkredibilitet osv.			
	Om fördelarna med att investera i cybersäkerhet som en konkurrensfördel.			
	Om de vanligaste riskerna och tillvägagångssätten t.ex. sårbarheter i värdekedjor.			
	Om de vanligaste och enklaste åtgärderna som jag som enskild person eller företag kan göra som minskar riskerna att bli utsatt för digitala brott.			

Kunskap

	Om digitala hot och dess konsekvenser.			
	Om de vanligaste sätten och tillvägagångssätten kopplat till digitala brott, t.ex. phishing och ransomware attacks.			
	Om de enklaste och mest effektiva åtgärderna för att minska risken för att bli utsatt för digitala brott.			
	Om relevant lagstiftning samt kraven som ställs på verksamheten när det kommer till cybersäkerhet.			
	Om kontinuitetshantering för att upprätthålla verksamheten oavsett händelse.			

Aktiviteter

	Skaffa praktiska färdigheter i att säkra nätverk, hantera slutpunkter (endpoints), och åtgärdshantering.			
	Genomföra de enklaste och effektivaste åtgärderna för att minska riskerna för digitala brott, t.ex. se över och administrera behörigheter.			
	Agera på ett sådant sätt så att risken för att bli utsatt för digitala brott minskas kraftigt samt vidta enkla åtgärder för att minska effekten av att ha blivit utsatt för ett genomfört brott.			
	Genomföra grundläggande informationsklassningar och riskanalyser.			
	Kontinuitetshantering för att upprätthålla verksamheten oavsett händelse.			
	Åtgärdsplan om ni drabbas av it-intrång, digitala brott och bedrägerier			
	Åtgärder vid eventuell incident, vilka åtgärder ska utföras av användare respektive tjänsteleverantör.			

Tekniska säkerhetsåtgärder		Ja	Nej	Inte tillräckligt
Hårdvara				
	Lösenord (starka, unika, lösenordsfras)			
	Kryptering (Bitlocker), krypteringstjänst som har aktiverats på samtliga datorer			
	Uppdatering (enheter, säkerhetsuppdatering)			
	Tvåfaktorsautentisering (så fort möjlighet finns)			
	Support (outsourcing, anställd)			
	Utbildning (när man har IT-support)			
	Kunskapsinhämtning (självlärande)			
	Antiviruskydd på anställdas mobiltelefoner			

Mjukvara

	Appar (från godkända platser)			
	Antivirusprogram (schemaläggning)			
	Uppdatering (alla program, säkerhetsuppdatering)			
	Tvåfaktorsautentisering (så fort möjlighet finns)			
	Lösenord (starka, unika, lösenordsfras)			
	VPN (server, mjukvara) VPN-lösning som säkrar datatrafiken för anställda som arbetar från andra platser än företagets lokaler			
	Support (outsourcing, anställd)			
	Kunskapsinhämtning (självlärande)			
	Säkra digitala plattformar, webbsidor och betalningslösningar.			

Nätverk

	Lösenord (starka, unika, lösenordsfras)			
	Router (total kontroll, hos internetleverantör)			
	Uppdatering (enheter, säkerhetsuppdatering)			
	Brandvägg (aktiverad, konfigurerad)			
	Publika nätverk (policy)			
	Gästnätverk (WiFi)			
	Support (outsourcing, anställd)			
	Kunskapsinhämtning (självlärande)			

Molntjänster

	E-tjänster (etablerade molntjänster)			
	E-post (etablerade e-posttjänster)			
	Digital brevlåda (Kivra, myndighetspost)			
	Två- eller multi-faktoraautentisering (så fort möjlighet finns)			
	Avtal (incidenter, vem ansvarar för åtgärder)			

Utbildning

	Ja	Nej	Inte tillräckligt
Har ni idag utbildning för er personal i cybersäkerhet eller informationssäkerhet?			
Om Ja, beskriv kort vad dessa innehåller och vilket format de har			
	Introduktion/ grundläggande	Fortsättnings- nivå	Avancerad nivå
Hur många av era anställda har behov av de olika nivåerna av utbildning i cybersäkerhet? Ange ungefärligt antal.			
Behöver ni inriktad utbildning mot en specifik målgrupp (t.ex. upphandlingsansvariga, chefer)? Beskriv vilka.			

	Ett par timmar	En dag	Flera dagar	Längre
Vilken arbetsbelastning får utbildning medföra?				
	Platsbunden	WEB-baserad med fysiska träffar	Online med moment i realtid	Helt online, självstudier
Vilket format skulle ni vilja ha utbildning i? Flera val är möjliga.				
	Svenska	Engelska		
Vilket språk föredrar ni att undervisningen ges på?				
	Svenska	Engelska		
Vilket språk föredrar ni gällande kursmaterial?				
	Ja	Nej		
Är det viktigt att era medarbetare kan arbeta i egen takt och efter egen plan?				
	Ja	Nej		
Är det viktigt att era medarbetare får pröva vad de kan i kurserna?				
	Ja	Nej		
Är det viktigt för er att ni kan använda egna fallstudier i kursen?				
	Ja	Nej		
Är det önskvärt att organisera studiegrupper av egna anställda?				
	Ja	Nej		
Är det önskvärt att era egna experter kan medverka i utbildningen?				
	Ja	Nej		
Är det viktigt att ni/era medarbetare kan påverka kursinnehållet?				



	Ja	Nej
Är det viktigt att era medarbetare får repetition och uppdatering av kursinnehåll efter kurslut?		
	Ja	Nej
Skulle det tillföra något om utbildningen avslutades med ett test och certifikat?		
	Ja	Nej
Är det önskvärt med formella poäng som HP/ECTS?		
	Ja	Nej
Är det viktigt för er att era medarbetare slutför påbörjad utbildning?		