SURFTOWNS SÄKERHETSMILJÖ

Databehandlingsavtal - Bilaga 1

Innehållsförteckning

Fysisk säkerhet

Surftowns data och infrastruktur är placerade i flera datacenter belägna i Danmark. Du kan därför vara försäkrad om att dina uppgifter kommer att stanna innanför Danmarks gränser. Vår datacenterleverantör är ansvarig för den fysiska miljön, exempelvis ström, kylning, brandsläckning och åtkomstkontroll, och för en strikt kontroll över att våra underleverantörer alltid efterlever de gällande säkerhetsreglerna på området.

Fysisk åtkomst till servrarna tilldelas endast anställda med arbetsrelaterade behov. Elektroniska åtkomstkort används vid ingångarna till datacentren, och dessa åtkomster loggas. Alla ingångar kameraövervakas dessutom.

Logiska åtkomster

Vi tilldelar rättigheter till de anställda utifrån arbetsrelaterade behov, och endast särskilt utvalda kan få en priviligierad åtkomst till systemen. Vi kontrollerar regelbundet om åtkomsten till systemen har tilldelats korrekt.

Nätverk

Vi använder höga segmenteringsnivåer i vårt nätverk, så att risken för spridning av ett angrepp minimeras. Brandväggar inspekterar trafik till kundernas miljöer, och DDoS-skydd begränsar den påverkan som eventuella angrepp kan ha på servrarna. Avancerad nätverksinspektion upptäcker mönster och angreppsförsök från kända, skadliga ip-adresser och varnar vår operativa avdelning vid behov.

Loggning

Vi loggar alla åtkomster till lednings- och kundmiljöer, och använder bl.a. loggningen till felsökning och utredning av eventuella händelser.

Sårbarhetshantering

För de system vi driver är vi ansvariga för att löpande övervaka huruvida nya sårbarheter kan uppstå. Vi har en process för att bedöma och hantera nya sårbarheter, och vi installerar korrigeringsfiler så fort som möjligt efter att de har publicerats.
Du är själv ansvarig för att utföra sårbarhetshantering av den programvara/kod du lägger ut på våra servrar - dvs. du ska själv hålla den uppdaterad.

Övervakning

Vi övervakar vår infrastruktur och relevanta tjänster dygnet runt. Alla avvikelser registreras i vårt incidenthanteringssystem. Som

komplement till övervakningen har vi anslutit ett 24/7-vaktschema.

Backup

Vi utför backup av våra egna interna system - för backup av kunddata, se nedan. Backupdata speglas mellan två fysiskt fristående platser i Danmark, så att det alltid finns en tillgänglig kopia i händelse av en kritisk krasch.

Backupav webbhotell inkl. e-post
Backup genomförs dagligen, och denna lagras i allmänhet i 30 dagar.

Backup av "molnservrar"
I allmänhet utförs inte backup av molnservrar. Backup kan emellertid köpas som tillval.

Kryptering

Åtkomst till administrativa system/kontrollpaneler sker via krypterade TLS-anslutningar.

Kryptering på webbhotell
Om data under transport (HTTPS) önskas krypterad, ska du själv konfigurera denna via din kontrollpanel. Överföring av filer till webbhotellet kan ske i krypterad form, om du väljer detta i ditt klientprogram.

Kryptering av e-post
Du måste aktivt välja att använda ett krypterat protokoll till överföring av e-post, eftersom e-postsystemen, för att stödja gamla e-postprogram, också tillåter användning av icke-krypterade anslutningar.

Kryptering på "molnservrar"
Du ska själv konfigurera kryptering där så önskas.

Kryptering av data
Om data (filer, databaser, osv.) ska lagras i krypterad form, ska du själv göra detta med hjälp av applikationen. Data lagras i allmänhet inte i krypterad form från vår webbplats.

Underleverantörer

Om underleverantörerna kan påverka vår säkerhetsmiljö säkerställer vi att de uppfyller samma strikta krav som vi gör. Detta gör vi via avtal, databehandlingsavtal, revisionsberättelser, egenkontroller och sekretessavtal. Vi kontrollerar löpande att våra underleverantörer uppfyller kraven.

Leverantören som driver Surftowns miljö är certifierad i enlighet med ISO 27001 och levererar årligen en revisionsberättelse avseende ISAE 3402, vilken säkerställer insyn för Surftown i huruvida leverantören uppfyller de överenskomna kraven eller ej.

Beredskap

Beredskap handlar om att vara förberedd på

händelser som kan ha en kritisk eller katastrofal påverkan på driften. Vi har därför beredskapsplaner som fastställer våra förfaranden, rutiner och roller i händelse av en katastrof. De anställda utbildas i beredskap flera gånger om året.

En del av vår beredskap är också att vi är förberedda om det skulle inträffa ett dataintrång. I det avseendet har vi rutiner för att ge råd till våra kunder och relevanta myndigheter, i enlighet med vad som krävs enligt den nya Persondataförordningen.

Kundens ansvar

Surftown säkerställer säkerheten i sin del av leveransen, dvs. de it-system som stöder webbhotells- och e-posttjänster.

Du ansvarar som kund själv för hur du konfigurerar dessa system, samt att den programvara och kod du lägger ut i systemen är säker.

Om den data som överförs till/från din webbplats kräver sekretess, bör du säkerställa HTTPS-skydd.

Om du hanterar känsliga uppgifter på e-post, bör du åtminstone säkerställa att du använder en krypterad anslutning, när du får åtkomst till e-postsystemen.