JmNet.dk's SIKRINGSMILJØ

Databehandleraftalen - Bilag 1

1

Indholdsfortegnelse

Fysisk sikkerhed

JmNet.dk's data og infrastruktur er placeret i flere datacentre beliggende i Danmark og Frankrig. Du kan derfor være sikker på, at dine data bliver inden for EU's grænser. Vores datacenterleverandør er ansvarlig for de fysiske rammer som f.eks. strøm, køl, brandslukning og adgangskontrol.

Fysisk adgang til serverne er kun tildelt medarbejdere med arbejdsbetinget behov.

Logiske adgange

Vi tildeler rettigheder til medarbejderne ud fra arbejdsbetinget behov, og kun særligt udvalgte kan få privilegeret adgang til systemerne. Vi kontrollerer periodisk om adgang til systemerne er tildelt korrekt.

Netværk

Vi anvender høj grad af segmentering i vores netværk, så risikoen for at et angreb kan sprede sig, minimeres. Firewalls inspicerer trafik mod kundernes miljøer, og DDoS-beskyttelse begrænser den påvirkning, som eventuelle angreb måtte have på serverne. Avanceret netværksinspektion opfanger mønstre og angrebsforsøg fra kendte, ondsindede ip-adresser og alarmerer ved behov.

Logning Vi logger alle adgange til management- og kundemiljøer og bruger bl.a. logningen til fejlfinding og efterforskning af eventuelle hændelser.

Sårbarhedsstyring

For de systemer, vi driver, er vi ansvarlige for løbende at overvåge, om nye sårbarheder skulle opstå. Vi installerer patches hurtigst muligt, efter de er offentliggjort. For den software/kode du selv ligger på vores servere, er du selv ansvarlig for at udføre sårbarhedsstyring – dvs. du selv skal holde den opdateret.

Overvågning

Vi overvåger vores infrastruktur og relevante services. Alle afvigelser registreres i vores incident management-system.

Backup

Vi udfører backup af vores egne interne systemer.

Backup af webhoteller inkl. e-mail Der tages daglig backup, og denne opbevares som udgangspunkt i 3 -21 dage, alt efter hvilken aftale kunden har med JmNet.dk.

Kryptering

Kryptering på webhoteller:
Hvis data under transport (HTTPS) ønskes krypteret, skal du selv opsætte dette via dit Kontrolpanel. Overførsel af filer til webhotellet kan ske krypteret, såfremt du vælger dette i dit klient-program.

Kryptering af e-mail:
Du skal aktivt tilvælge at anvende en krypteret protokol, da e-mail systemerne, for at understøtte gamle e-mail programmer, også giver mulighed for at anvende ikke-krypterede forbindelser.

Kryptering af data:
Hvis data (filer, databaser, osv.) skal opbevares krypteret, skal du selv gøre dette igennem applikationen. Data bliver som udgangspunkt ikke opbevaret i krypteret form fra vores side.

Underleverandører
Hvis underleverandørerne kan have påvirkning på vores sikringsmiljø, sørger vi for, at de efterlever samme strenge krav, som vi gør. Det gør vi via kontrakter, databehandleraftaler, egenkontrol og fortrolighedsaftaler. Vi kontrollerer løbende, at vores underleverandører efterlever kravene.

Beredskab
Beredskab handler om at være forberedt på Tekniske og organisatoriske sikringsforanstaltninger

hændelser, som kan have kritisk eller katastrofal påvirkning på driften. Vi har derfor beredskabsplan, som fastlægger vores procedurer, rutiner og roller i tilfælde af en katastrofe.

En del af vores beredskab er også, at vi er forberedte, hvis der skulle ske et databrud. I den forbindelse har vi procedurer for advisering af vores kunder og relevante myndigheder, som det kræves efter den nye Persondataforordning.

Kundens ansvar
JmNet.dk sørger for sikkerheden i sin del af leverancen, dvs. de it-systemer, som står bag ydelserne webhotel og e-mail.

Du har som kunde selv ansvar for, hvordan du opsætter disse systemer, samt at den software og kode du ligger på systemerne er sikker.

Hvis de data, som transmitteres til/fra dit website kræver fortrolighed, bør du sørge for HTTPS-beskyttelse.

Håndterer du følsomme data på e-mail, bør du som minimum sikre dig, at du anvender en krypteret forbindelse, når du tilgår e-mailsystemerne.
Det er også til enhver tid kundens ansvar at sikre at de adgangskoder mv. der anvendes er tilstrækkelig stærke.