



UNOEURO SIKRINGSMILJØ

Databehandleraftalen - Bilag 1

Indholdsfortegnelse

Fysisk sikkerhed	2
Logiske adgange	2
Netværk	2
Logning.....	2
Sårbarhedsstyring	2
Overvågning	2
Backup.....	3
Kryptering.....	3
Underleverandører	3
Beredskab	3
Kundens ansvar.....	4

Tekniske og organisatoriske sikringsforanstaltninger

Fysisk sikkerhed

UnoEuro's data og infrastruktur er placeret i flere datacentre beliggende i Danmark. Du kan derfor være sikker på, at dine data bliver inden for Danmarks grænser. Vores datacenterleverandør er ansvarlig for de fysiske rammer som f.eks. strøm, køl, brandslukning og adgangskontrol, og vi fører skarp kontrol med, at vores underleverandører til enhver tid efterlever de gældende sikkerhedsregler på området.

Fysisk adgang til serverne er kun tildelt medarbejdere med arbejdsbetinget behov. Der anvendes elektronisk adgangskort ved indgange til datacentrene, og disse adgange logges. Der er ligeledes kameraovervågning af alle indgange.

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 vores driftsafdeling 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 har en proces for at vurdere og håndtere nye sårbarheder, samt 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 døgnet rundt. Alle afvigelser registreres i vores incident management-system. Som

Tekniske og organisatoriske sikringsforanstaltninger

supplement til overvågningen har vi tilknyttet en 24/7-vagtordning.

Backup

Vi udfører backup af vores egne interne systemer - for backup af kundedata, se nedenfor.

Backupdata spejles mellem to fysisk uafhængige lokationer i Danmark, så der altid er en tilgængelig kopi i tilfælde af et kritisk nedbrud.

Backup af webhoteller inkl. e-mail

Der tages daglig backup, og denne opbevares som udgangspunkt i 30 dage.

Backup af ”cloud servere”

Der tages som udgangspunkt ikke backup af cloud servere. Backup kan dog tilkøbes.

Kryptering

Adgang til administrative systemer/kontrolpaneler sker via krypterede TLS-forbindelser.

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 krypte-

ret protokol, da e-mail systemerne, for at understøtte gamle email programmer, også giver mulighed for at anvende ikke-krypterede forbindelser.

Kryptering på ”cloud servere”

Du skal selv opsætte kryptering, hvor det ønskes.

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, revisionserklæringer, egenkontrol og fortrolighedsaftaler. Vi kontrollerer løbende, at vores underleverandører efterlever kravene. Leverandøren, som driver UnoEuro's miljø, er ISO 27001 certificeret og leverer årligt en ISAE 3402 erklæring, som sikrer UnoEuro indsigt i, hvorvidt leverandøren efterlever de aftalte krav.

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 beredskabsplaner, som fastlægger vores procedurer, rutiner og roller i tilfælde af en katastrofe. Medarbejdere trænes i beredskabet flere gange årligt.

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

UnoEuro 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.