Præsentation af **ServicePoints sikringsmiljø**

Indholdsfortegnelse

Indledning

Som leverandør af hosting og cloud-ydelser er vores vigtigste sikkerhedsopgave at passe godt på dine data og sørge for, at du til enhver tid lever op til sikkerhedskravene fra dine kunder. Sikkerhed er derfor et område, som vi tager meget seriøst - på alle niveauer.

Formålet med dette dokument er at give dig et indblik i, hvordan vi sikrer vores platform, så du som kunde ikke behøver at bekymre dig om sikkerhed, men i stedet kan bruge tid og energi på at udvikle din forretning.

Politikker, procedurer og standarder

Vi har defineret et sæt af politikker, procedurer og standarder for, hvordan vi opererer i virksomheden og bedst passer på dine data.

Dokumenterne opdateres løbende, i takt med at trusselsbilledet ændrer sig. På den måde sikrer vi, at vi hele tiden prioriterer vores indsats dér, hvor der er mest brug for den.

Hvordan vi prioriterer indsatsen, afhænger af vores risikovurdering, der opdateres løbende, og som udgør kernen i vores informationssikkerhedsprogram.

Medarbejdersikkerhed

Alle medarbejdere og konsulenter med adgang til systemer og faciliteter er underlagt vores sikkerhedspolitikker. Alle gennemgår obligatorisk undervisning, hvor de bliver præsenteret for alle relevante og aktuelle privacy- og sikkerhedsemner. Dette sker både ved start og løbende gennem deres ansættelse. Formålet er at ruste medarbejderne til at modstå aktuelle trusler mod virksomhedens og kundernes data.
For at højne det generelle niveau i branchen og for at vedligeholde egne kompetencers deltager vores medarbejdere aktivt i Communities og ERFA-grupper. Vi opfordrer vores medarbejdere til hele tiden at være på forkant med den nyeste udvikling og til at erhverve de højeste certificeringer inden for sikkerhed, netværk, osv.

Dedikerede sikkerheds- og persondatakompetencer

Vores sikkerhedschef er ansvarlig for at implementere og vedligeholde vores sikkerhedsprogram. Vores interne revisor gennemgår regelmæssigt vores sikkerhedssetup og rapporterer direkte til ledelsen. Endelig har vi interne, juridiske kompetencer inden for persondata, som sikrer, at persondata behandles efter de gældende regler både internt i virksomheden og på vegne af vores kunder.

Operationel sikkerhed og beskyttelse af kundedata

Den vigtigste opgave i vores sikkerhedsprogram er at passe godt på dine data. Vores sikringsmiljø inddelt i flere lag:

Fysisk sikkerhed
Vores datacentre er state-of-the-art med placeringer i hele verden. Du kan derfor selv styre placering af dine data. Vores datacenterleverandører er ansvarlig for de fysiske rammer som fx strøm, køl, brandslukning og adgangskontrol, og vi fører skarp kontrol med, at vores underleverandører til en hver tid efterlever de gældende sikkerhedsregler på området.

Netværk
Vores netværk er segmentet, så kunder er beskyttet mod hinanden og mod trusler, der bevæger sig på tværs i netværket. Next Generation firewalls, SDNs og VLANs begrænser angreb mod kundernes miljøer, og DDoS-beskyttelse begrænser den påvirkning, som evt. angreb måtte have på serverne. Avanceret netværksinspektion opfanger mønstre og angrebsforsøg fra kendte, ondsindede ip-adresser og alarmerer vores driftsafdeling ved behov.

Logiske adgangsniveauer
Vi tildeler kun rettigheder til de medarbejdere, der har brug for dem, og vurderer dem løbende. Kun særligt privilegerede medarbejdere har adgang til at administrere interne systemer.

Overvågning
Vi overvåger vores infrastruktur og relevante services døgnet rundt. Alle afvigelser registreres i vores incident management-system. Som supplement til overvågningen har vi tilknyttet en 24/7-vagtordning. Overvågning kan også tilkøbes enkelte servere og services og leveres herfor iht. den indgåede aftale.

Logning
Vi logger alle adgange til management og kundemiljøer. På den måde sikrer vi integritet og sporbarhed og kan sammenkøre hændelser. Vores centrale logplatform sikrer, at vi hurtigt kan korrelere logs fra mange kilder.

Backup
Vi udfører backup i 2 lag, hhv. filbackup og snapshotbackup. Backup udføres iht. den indgåede aftale.

a) Filbackup udføres til et fysisk uafhængigt datacenter placeret i Microsoft Azures europæiske datacentre. Alle data krypteres med højeste standard (AES 128bit) og nøglen kendes kun af særligt privilegerede medarbejdere ved ServicePoint A/S. Eksterne leverandører har ingen adgang til læsbare data.

b) Snapshotbackup er et billede af serveren, som den så ud da snapshottet blev taget. Snapshottet opbevares i samme datacenter som serveren, hvilket muliggør ekstremt hurtig disaster-recovery. Snapshots kan manuelt eksekveres af kunden via kundecenteret.

2-faktor
Vores kundepanel er beskyttet med 2-faktor sikkerhed som kræver både et gyldigt login med brugernavn og kodeord samt en unik nøgle der fremsendes til kundens mobiltelefon via SMS. 2-faktor kan også tilkøbes til server-adgange (Remote Desktop og SSH) og leveres herfor iht. den indgåede aftale.

Beredskab og disaster recovery

Beredskab handler om at være forberedt på 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.
For at sikre vores tekniske infrastruktur og sprede risikoen ved kritiske nedbrud bruger vi flere uafhængige datacenterleverandører. Vi opbevarer altid mindst én kopi af backupdata i et datacenter, hvor vi ikke har produktionsdata.

Håndtering af underleverandører

For at vi kan operere så effektivt som muligt, bruger vi underleverandører til udvalgte services. Hvis underleverandørerne kan have påvirkning på vores sikringsmiljø, sørger vi for,

at de efterlever samme strenge krav som os selv. Det gør vi via kontrakter, databehandleraftaler, revisionserklæringer, egenkontrol og/eller fortrolighedsaftaler. Vi kontrollerer løbende, at vores underleverandører efterlever kravene.

Revision og compliance

Vi har et omfattende compliance-program, som sikrer, at vores datacentre efterlever vedtagne standarder og relevant lovgivningen på området, med det formål at understøtte og sikre din forretning:

ISO27001
ISO 27001 er en international standard for håndtering af informationssikkerhed. Alle vores datacentre er certificeret ISO27001. Der kan hentes information om vores datacentre på terms.servicepoint.dk

SoC 2 (ISAE 3000)
ISAE 3000 (SoC 2) beskriver, hvordan vores datacentre sikrer de ydelser, som vi leverer til vores kunder, og indeholder en uafhængig revisors konklusion på, om beskrivelsen af vores datacentres kontroller er retvisende, hensigtsmæssigt udformet, og om kontrollerne har fungeret effektivt i hele erklæringsperioden. Der kan hentes information om vores datacentre på terms.servicepoint.dk

Penetration testing
Vi udfører regelmæssigt penetration tests mod kritiske komponenter i vores infrastruktur for at se, hvordan vores systemer forsvarer sig mod eksterne trusler. Kunder kan også udføre penetration tests mod egne systemer efter forudgående aftale med os.