Sentinel Surveillance Systems

Bilag 1 til it-sikkerhedspolitik
Retningslinjer for drift
Version 1.0

Klassifikation: Fortrolig mellem parterne

Sentinel Surveillance Systems, den 01. oktober 2025

Hovedpunkter i it-sikkerheden

It-sikkerheden i Sentinel Surveillance Systems er baseret på disse retningslinjer.

1.1 Adgangsstyring

Udgangspunktet for tildeling af rettigheder og adgang til systemer og informationer er, at alt er låst ned og at der kun gives adgang, hvor der er et forretningsmæssigt behov. Den daglige leder beslutter hvem, der skal have adgang til system og/eller informationer. Den it-ansvarlige tildeler herefter rettighederne ud fra disse beslutninger.

Sentinel Surveillance Systems servere og bærbare pc'er beskyttes med adgangskode og skærmlås samt opdaterede antivirusprogrammer og lokale firewalls.

Bærbare pc'er med firmadata, herunder persondata, beskyttes desuden med kryptering (se afsnit 1.2).

Styring af adgangskoder sker via politik i Active Directory (AD), og følger Best Practice - minimum 15 karakterer, kombination af store/små bogstaver samt tal og specialtegn, med skift hver tredje måned.

Sentinel Surveillance Systems øvrige mobile enheder (mobiltelefoner og evt. tablets) beskyttes med en pinkode og brug af kryptering af firmadata samt mulighed for sletning (remote-wipe) af enhederne.

Sentinel Surveillance Systems fysiske lokaler er sikret med adgangssystem og forskellige alarmer. Den daglige leder beslutter hvem, der skal have adgang til hvad.
[Adgangssystemet kan være en lås med nøgler, evt. med forskellige adgange, hvor man registrerer hvem nøglerne udleveres til. Alternativt kan man bruge et adgangskortsystem, evt. et som ens udlejer tilbyder. På samme måde kan en indbrudsalarm håndteres lokalt eller som en del af en lejeaftale.]

Det kritiske it-udstyr er anbragt i adgangsstyret rum, med alarmer, hvor det er sikret mod forsyningssvigt med strømbackup (UPS) og mod miljøskader med temperaturføler, fugtighedsmåler samt med brandalarm.

Ved større problemer er der planer for driftens videreførelse andet steds, som beskrevet i Sentinel Surveillance Systems it-beredskabsplan.

Kontroller:
Den ansvarlige for et system eller de pågældende informationer gennemgår hvert halve år de tildelte rettigheder for at kontrollere, at de fortsat er gældende og at der er et forretningsmæssigt behov. Ligeledes kontrolleres medarbejdernes adgang til de fysiske lokaler.

1.2 Informationer og aktiver

Sentinel Surveillance Systems informationer findes på it-aktiver som eksempelvis pc'er, servere, tablets, smartphones, usb-nøgler, cloud-lagre og lignende, samt muligvis også cd-rom og backupbånd osv. Sikkerhedspolitikken kræver, at Sentinel Surveillance Systems informationer er beskyttet i tilfælde af tab, tyveri, kopiering mv.

Kryptering af virksomhedens informationer understøttes af en begrænsning af hvilke personer, der får rettigheder til at læse, rette eller slette informationer. Se afsnit om adgangsstyring.

Medarbejdere i Sentinel Surveillance Systems må som udgangspunkt ikke opbevare firmarelaterede data i et cloud-lager, som Dropbox, med mindre dette er stillet til rådighed af Sentinel Surveillance Systems, eller godkendt af Sentinel Surveillance Systems ledelse til firmabrug. Hvis der opstår et akut behov for at opbevare firmarelaterede data i et ikke-godkendt cloud-lager, er det medarbejderens ansvar at sørge for, at data er krypterede.

Sentinel Surveillance Systems it-aktiver (software, informationer eller fysisk udstyr) registreres i aktivlisten, og det er angivet hvilke, der er kritiske for Sentinel Surveillance Systems.

Nye it-anskaffelser skal overholde Sentinel Surveillance Systems retningslinjer, herunder krav om beskyttelse med antivirus mv. og evt. om kryptering. Er der tale om en helt ny anskaffelse, som en ny type pc'er eller et nyt økonomisystem vurderes det, om der sker ændringer i trusselsbilledet og om der i så fald skal stilles specifikke krav.
Nye it-anskaffelser dækker ikke over, at der indkøbes en ekstra bærbar pc, men derimod indkøb og anvendelse af nye typer udstyr.

1.3 Dokumentation

Sentinel Surveillance Systems it-sikkerhedspolitik, klassifikation og andre retningslinjer samt vejledninger er tilgængelige på Sentinel Surveillance Systems intranet.

Den dagligt ansvarlige for styring af Sentinel Surveillance Systems it-sikkerhed dokumenterer risikovurderinger, hændelser, aktiviteter der understøtter medarbejdernes viden om it-sikkerhed, ændringer mv. i et katalog på intranettet, hvor adgangen er begrænset til de relevante personer.

Kontroller:
Disse dokumenter vedligeholdes af den dagligt ansvarlige for Sentinel Surveillance Systems it-sikkerhed og godkendes af ledelsen.

1.4 Driftsikkerhed

Der foretages backup af Sentinel Surveillance Systems systemer og informationer, så de kan genskabes efter et nedbrud. Dette gøres med passende intervaller, så mængden af data, der potentielt kan mistes, minimeres. Backup af data opbevares på en måde, så det sikres at data ikke mistes ved f.eks. fysisk skade på en server eller serverrum, samt at uvedkommende ikke kan få adgang til fortrolige eller kritiske data ved at tilgå backup.

Logning af aktiviteter er slået til i Sentinel Surveillance Systems systemer, og hvor der er persondata logges adgang og forsøg på adgang til de enkelte informationer også. Logs fra systemer der har indvirkning på it-sikkerhedsniveauet i Sentinel Surveillance Systems sendes til en central logserver, hvor logfilerne automatisk analyseres for potentielle trusler. Dette gælder f.eks. Windows Domain Controller servere, antivirusservere og firewalls.

Windows Server Update Services (WSUS) benyttes på alle Windows-platforme til styring af tekniske sårbarheder, for at forhindre at disse udnyttes ved et angreb. Kritiske Windows-opdateringer installeres hurtigst muligt, og andre Windows-opdateringer en gang pr. måned. Opdatering af tredjeparts applikationer sker løbende. Informationer om sårbarheder i tredjeparts applikationer indsamles med abonnement hos leverandør.

Ændringer følger en proces med strukturerede tests af løsningerne inden idriftsættelse. Idriftsættelse af ændringer på kritiske systemer foregår i videst muligt omfang i planlagte servicevinduer, for at undgå at eventuelle fejl vil påvirke tilgængeligheden.

Sentinel Surveillance Systems opretholder funktionsadskillelse hvor muligt. Som minimum kræves (ligesom det er tilfældet ved betalinger i netbanken), at en anden person, f.eks. en fra ledelsen, medvirker ifm. godkendelse af større ændringer og ved tildeling af administratorrettigheder.

Driften sikres yderligere ved at internetforbindelse og alle servere er dublerede (redundante), med spejlede (Raid-baserede) diske, aftaler med leveringstidsgarantier (Service Level Agreement) på levering af reservedele, samt ekstern opbevaret krypteret kopi af backuppen.

24/7 tilgængeligheden af Sentinel Surveillance Systems systemer dækker også bemandingen, så viden er dubleret og kritiske funktioner tilgængelige døgnet rundt.

Kontroller:
Det testes ved halvårlige øvelser, at en given backup kan genskabes på et tilsvarende system, og at funktionaliteten herefter er som forventet.

1.5 Klassifikation

Sentinel Surveillance Systems benytter følgende klassifikationer af informationer:

Offentlig – må ses/tilgås af alle.

Fortrolig – må ses/tilgås af alle i Sentinel Surveillance Systems og hos specifikke kunder/samarbejdspartnere.

Internt – må ses/tilgås af alle i Sentinel Surveillance Systems, men ingen udenfor

Følsomt – må kun ses/tilgås af en mindre gruppe med et konkret forretningsmæssigt formål.

Informationer klassificeret som andet end Offentlig, skal mærkes med deres klassifikation på papir, i mails, som en del af informationen om afsenderen, og på forsiden af dokumenter hvad enten de er på papir eller i elektronisk form.
Informationer klassificeret som Følsomt, må ikke sendes via ukrypterede mails eller over ukrypterede forbindelser.

1.6 Kommunikationssikkerhed

Sentinel Surveillance Systems interne netværk er beskyttet med en firewall, der regulerer og logger trafikken mellem Sentinel Surveillance Systems interne net og Sentinel Surveillance Systems tele-/internetleverandør (Internet Service Provider, ISP) (internettet), så kun tilladt trafik passerer igennem. Derudover er firewallen sat op med et separat netværk (DMZ) med adgang fra internettet til specifikke services og med meget begrænset adgang til Sentinel Surveillance Systems interne netværk. I DMZ findes Sentinel Surveillance Systems webserver og andre eksterne services.

Sentinel Surveillance Systems interne netværk er delt i flere netværk, et servernet, et klientnet, produktions- og administrationsnet samt et netværk til fjernadgang (remote access) fra mobile enheder og leverandører, som firewallen kontrollerer trafikken imellem. Firewallregler er så vidt muligt konfigureret i henhold til PCI-compliance, hvilket betyder at der kun åbnes for de nødvendige services og kun mellem relevante netværkssegmenter, samt at der er defineret regler for både indgående og udgående netværkstrafik.

Brugernes webadgang til internettet scannes i en cloud/proxy-løsning for at tilsikre at der ikke tilgås usikre eller upassende hjemmesider. Adgang til usikre hjemmesider blokeres og filer, der downloades, bliver scannet for virus og andet malware.

Alle indgående e-mails, der modtages i Sentinel Surveillance Systems mailsystem, bliver scannet for usikre links til eksterne hjemmesider og for om det er en potentiel phishing-mail. Derudover scannes vedhæftede filer for virus og andet malware.

Al ekstern adgang til Sentinel Surveillance Systems netværk og systemer sker via krypterede (VPN) forbindelser. Sentinel Surveillance Systems website og webservices benytter https-kryptering baseret på Transport Layer Security (TLS), ligesom mailserveren også håndterer TLS.

Adgang til andre servere/services og Sentinel Surveillance Systems interne netværk sker via klientkryptering beskyttet af 2-faktor autentifikation.

Overførsel af, eller adgang til, Sentinel Surveillance Systems informationer til/fra eksterne samarbejdspartnere eller myndigheder må kun ske efter aftale med disse, baseret på informationernes klassifikation, herunder om evt. brug af kryptering.

Pc'er og mobile enheder, der kobler sig på virksomhedens netværk og systemer eksternt fra, skal overholde virksomhedens retningslinjer. Dette er kun tilladt for virksomhedens udstyr. Medarbejdernes egne pc'er og mobile enheder (Bring Your Own Device, BYOD) er ikke tilladt på virksomhedens netværk.

1.7 Leverandørstyring og outsourcing

Leverandører som Microsoft, der står for drift af Sentinel Surveillance Systems systemer, skal overholde Sentinel Surveillance Systems krav til it-sikkerhed. De skal også give Sentinel Surveillance Systems mulighed for løbende at kunne kontrollere disse sikringsforanstaltninger og én gang om året, af sig selv, levere den dokumentation for dette, som er omtalt i aftalen mellem Sentinel Surveillance Systems og leverandøren.

Kontroller:
Der skal foreligge en aftale, og om nødvendigt også en databehandleraftale, som lever op til kravene i databeskyttelsesloven. Det kontrolleres årligt, om leverandørerne lever op til aftalerne.

Inden indgåelsen af aftalen har Sentinel Surveillance Systems vurderet om der er nogen specielle risici, som aftalen skal tage højde for. Skal personale fra f.eks. rengøringsfirmaet personligt underskrive en fortrolighedserklæring og/eller er der behov for, at de fremviser en straffeattest.

1.8 Medarbejdersikkerhed og awareness

I forbindelse med stillingsopslag/ansættelser vurderer den daglige/enkelte leder, om der er særlige sikkerhedsmæssige krav, herunder om det for eksempel er nødvendigt at bede om at se en straffeattest/børneattest.

Som en del af ansættelsesproceduren, dog senest ved første arbejdsdag, orienteres den nye medarbejder om tavshedspligt og andre sikkerhedskrav.

Via awareness-træning sikres, at nye medarbejdere og alle brugere har den nødvendige it-kyndighed, også dem, som ikke har en it-uddannelse, samt en god sikkerhedsadfærd, eksempelvis med hensyn til adgang til informationer. Dette gælder også, når en medarbejder skifter rolle i virksomheden. Det er den daglige/enkelte leders ansvar, at dette sker.

Når en medarbejder fratræder, gør HR vedkommende opmærksom på, at tavshedspligten og fortroligheden også gælder efter ansættelsens ophør.

1.9 Sikkerhedshændelser og it-beredskab

Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette ledelsen om dette
Den ansvarlige for den daglige styring af Sentinel Surveillance Systems informationssikkerhed foretager en vurdering af de rapporterede sikkerhedshændelser hurtigst muligt efter at de er anmeldt. Det vurderes om de kan vente til senere behandling, om de skal håndteres her og nu (eventuelt ved hjælp af ændringer, yderligere awareness eller kontakt til tredjepart) eller om de er så alvorlige, at de kræver aktivering af Sentinel Surveillance Systems it-beredskabsplan.
Er der tale om hændelser med persondata, aktiveres Sentinel Surveillance Systems procedurer for.

Når hændelsen er behandlet, vurderes om sagen kan lukkes eller om der skal ske en opdatering af risikobilledet, som evt. kræver nye sikkerhedstiltag.

Den ansvarlige for den daglige styring af informationssikkerheden rapporterer om større sikkerhedshændelser ifm. ledelsens årlige review.

Såfremt eksterne parter berøres af sikkerhedshændelser hos Sentinel Surveillance Systems, er den daglige ledelse ansvarlig for eventuel kommunikation over for berørte parter.