Dokumentasjon på produktets sikkerhetsmekanismer og generell funksjonalitet.

Sikkerheten i programvaren

EdStep er utviklet etter gjeldende anbefalinger for sikre moderne web-applikasjoner. På utviklingssiden er det brukt rammeverk som gir god støtte på sikkerhet. Rammeverket tilbyr støtte for parametrisering av databasespørringer, beskyttelse mot kjøring av brukergenererte eller -inkluderte skript og forfalskning av forespørsler (Cross site request forgery). Det brukes en egen modul, Cerpus Auth, for autentisering.

Konfidensialitet og integritet

All kommunikasjon mellom klient og tjener sikres med SSL/TLS, Minimum TLS 1.0. Kontroll på SSL-labs gir rating A+.

Sikring av databasespørringer med parametrisering gjør at brukere ikke kan inkludere angrepskode for å hente ut informasjon om andre brukere som de ikke er autorisert for. Sperring mot kjøring av inkluderte skript forhindrer at brukere kan inkludere skript som henter ut eller endrer data som tilhører andre og beskyttelsen mot forfalskning av forespørsler gjør at tredjepartssider ikke kan brukes for å kjøre forespørsler på vegne av pålogget bruker.

Brukeres sesjoner er kryptert slik at ingen kan endre eller lese den, det er slått på at nettleseren bare skal sende med sesjonscookien over HTTPS og det cookien har med innstilling for at den ikke skal være tilgjengelig for skript i nettleseren (httponly-flagg i headeren).

Autentisering

En egen autentiseringsmodul, Cerpus Auth, brukes for autentisering og autentiseringsstandarden oAuth 2.0 brukes mellom autentiseringstjenesten og underliggende tjenester. For å sikre brukernes passord er det lagret med bruk av scrypt, som er en av de anbefalte måtene for å best mulig sikre passord.

Autentiseringstjenesten utfører epost-validering ved opprettelse av kontoer. Dette sikrer både at kontoen er knyttet til virkelige personer og at det finnes måter å gjenvinne tilgang til kontoen ved glemt passord. Det er ikke alltid krav om at kontoen knyttes til en epost-adresse. I tilfeller der kontoer opprettes uten epost-adresse disse opprettes i EdStep og være opprettet av administrator eller lærer med tilgang til å opprette kontoer.

I tillegg til tradisjonell autentisering med brukernavn og passord tilbyr Cerpus Auth også innlogging med eksterne identitetstilbydere som:

- Google, ved hjelp av en OAuth 2.0
- Facebook, ved hjelp av en OAuth 2.0
- Twitter, ved hjelp av en OAuth 1.0
- Windows Live, ved hjelp av OAuth 2.0
- Feide, ved hjelp av SAML2

Autorisering

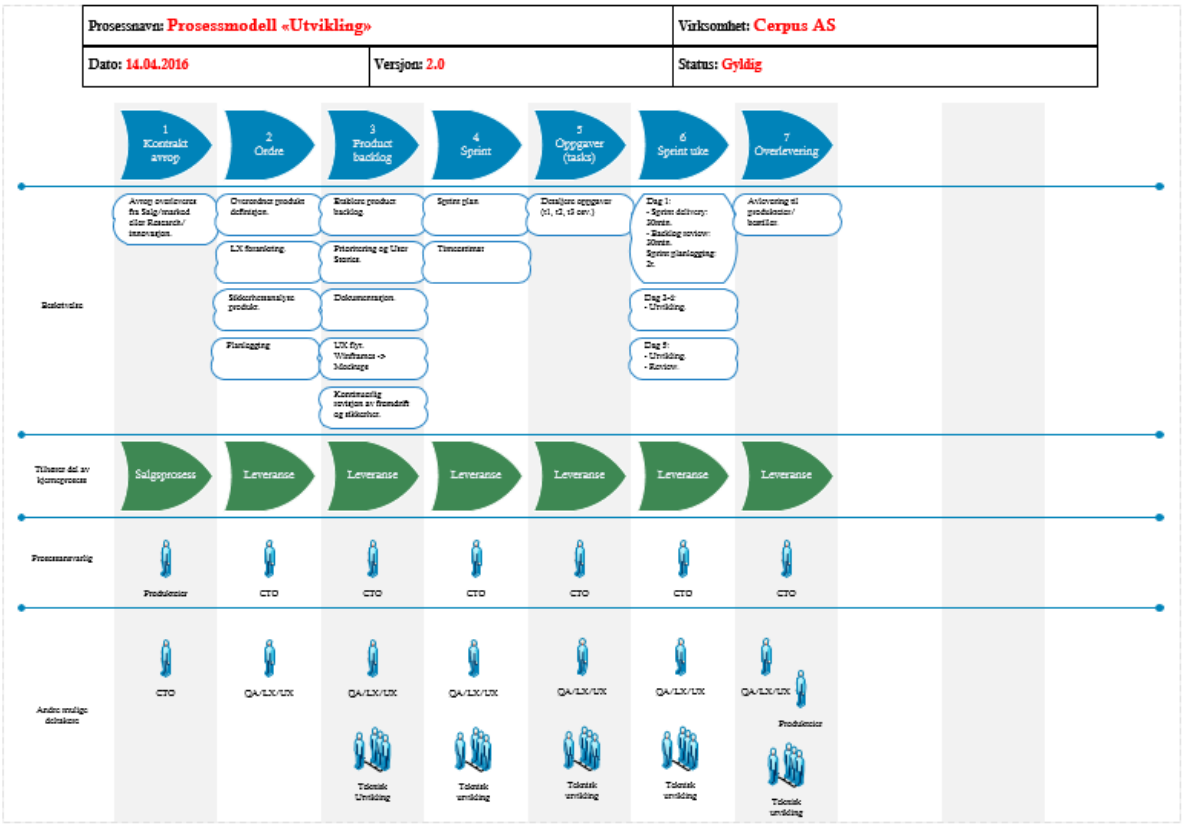
All tilgang til data kontrolleres mot tilganger for autorisert bruker.

Produkt sikkerhetsanalyse i utviklingsprosessen

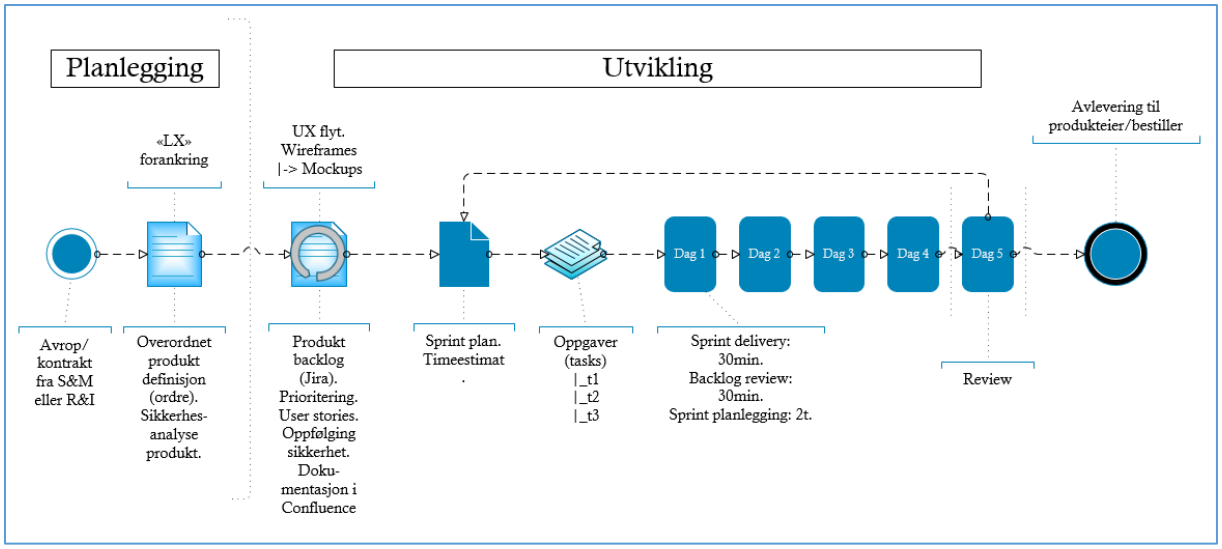
Sikkerhetsanalyse av produktet som utvikles er en viktig del av rutinene knyttet til utviklingsprosessen. I starten av utviklingsfasen analyseres «ordren» som legger grunnlaget for utviklingen, og her sikres og forankres nødvendig nivå og kvalitet på produktets sikkerhet, samt krav til senere oppfølging. Utover i utviklingsprosessen er sikkerheten i en stadig revisjon og oppfølging, og dette skjer spesielt i fasen «Product Backlog» der dette er gjenstand for kontinuerlig oppfølging og analyse.

Skissene under viser Cerpus prosess (overordnet og mer i detalj) knyttet til produkt utvikling, med de aktiviteter og ansvar som naturlig settes fokus på underveis i prosessen.

Figur 1, overordnet prosessmodell for utvikling.



Figur 2, mer detaljert (BPMN) av selve utviklingsprosessen.



Avvikhåndtering

Cerpus har en omfattende prosedyre knyttet til avvikshåndtering, og som støtter seg på ITILs rammeverk. Avvikshåndtering er en naturlig og viktig del av både utvikling, og senere i drift og forvaltning av produktet/løsningen.

Viser til dokumentet «Cerpus Helhetlige Kvalitetssystem», der avvikshåndtering er godt beskrevet i kapitlene som omhandler «Cerpus Prosjekt» og «Cerpus Scrum».

EULA and privacy policy

https://edstep.com/privacy-policy
https://edstep.com/terms-and-conditions

Sikkerhet knyttet til datasenter, drift og hosting miljø.

Cerpus sine to datasenter er plassert sentralt i Oslo området. Vår hoved lokasjon er i Nydalen og vår lokasjon 2 (backup lokasjon) er på Ulven. Vi leier datasenter fasiliteter fra Blix Solutions (www.blix.com), som igjen har avtaler med Availo (www.availo.no) for hoved lokasjon, og DigiPlex (www.digiplex.com) for lokasjon 2. Vi benytter lokasjon 2 primært for backup tjenester, altså at alt av sikkerhetskopiering tas ut av hoved lokasjon og lagres på den andre lokasjonen som en ekstra sikkerhet. Begge datahallene oppfyller de absolutt høyeste krav til kvalitet, sikkerhet og oppetidsgaranti.

Datasenter - Hoved lokasjon Oslo Nydalen.

Sikkerhet og tilgang.

Datasenteret har fått navnet DCO, Data Center Oslo. DCO er et av få kommersielle datasentre i Oslo som er plassert innenfor Ring 3. Fullt utbygget er datasenteret på ca. 2000m² og huser rundt 500 rack. Det er planlagt et totalt strømforbruk på over 3 megawatt, og med mulighet til å levere over 20kW per rack! DCO har to MMR-rom (fiberterminеringsrom) som igjen deler 3 separate fiberføringsveier fra utsiden for å sikre redundante nettverksforbindelser ut i verden.

Datahallen er bygget med tanke på høy fysisk sikkerhet. Det finnes to skallsikringslag før man kommer inn i datahallen, og deretter et lag med skallsikring før man kommer til teknisk utstyr. I motsetning til mange andre norske datahaller er teknisk infrastruktur plassert utilgjengelig utenifra. Dette gir en høyere sikkerhet med tanke på naturkatastrofer, sabotasje og lignende.

Strøm.

Bygget som huser datahallen får levert 11kV høyspent strøm, som fordeles til en ring av 5 trafoer internt i bygget. Ringen forsynes fra to ulike bydelstrafoer, med en tredje som kan kobles inn ved behov. Videre fordeles strømmen gjennom hovedtavler og UPSer, over A- og B-kurser ned mot hvert rack.

Bygget er definert som samfunnskritisk. Dette gir en høy prioritering hos strømleverandøren ved eventuelle hendelser.

Kjøling.

Det jobbes kontinuerlig for å redusere PUE (Power Usage Effectiveness). Dette gjøres ved å bruke innovative og energieffektive løsninger for kjøling. I vårt datasenter i Nydalen har vi et meget effektivt kjølesystem bestående av InRow kjølere. Det vil si at kjølerne er plassert inne i rackradene og blåser kald luft i front av rackene. Servernes egne vifter trekker da inn den kalde luften, og baksiden av kjølerne trekker inn den varme luften. Vannet inne i kjølerne varmes opp og sendes i rørsystem opp på taket der kjølemaskiner senker vanntemperaturen og sender kaldt vann ned i datahallen igjen.

Ved å endre på antall kjølere i rackraden kan man justere kjøleeffekten opp i de områdene som genererer mye varme, og trekke ned kjøleeffekten der behovet er lavere. Med kjølemaskiner i friluft på taket kan vi bruke mer frikjøling i perioder med kaldere uteluft, noe som gir overlegen energieffektivitet. Frikjølingen brukes i lufttemperaturer opp til 15 °C. Sensorer ved hvert rack styrer luftstrømmen og kjøling for stabil temperatur til servere avhengig av den varmen som genereres i racket. I dette strengt kontrollerte miljøet holdes luftfuktigheten innenfor bransjens standarder.

Skallsikring.

Det tekniske utstyret som er plassert ute er montert på byggets tak (15 m over bakken) og er usynlig og utilgjengelig for uvedkommende.

Datasenteret er plassert inne i bygget og har egen skallsikring, i tillegg til hovedbyggets skallsikring.

Innbruddsikring.

Bygget er sikret med alarm, i tillegg har datasenteret et eget avansert alarmsystem med ulike sensorer i samtlige rom og dører.

Innbruddsalarmen er tilkoblet et vaktselskap via sikre alarmoverføringer i tillegg til at lokalene patruljeres av sikkerhetsvakter døgnet rundt. Det er til enhver tid personell på plass i bygget, noe som er med på å forebygge innbrudd og hærverk.

Kameraovervåkning.

Datahallen har kameraovervåking med høykvalitetsbilder av alle viktige punkter. Kameraene har bevegelsessensorer som aktiverer både videoopptak og alarm. Autoriserte teknikere overvåker kameraene samtidig fra forskjellige lokasjoner, og alle bilder lagres i et annet datasenter på en egen server. Overvåkingen gjøres i henhold til lover og forskrifter.

Overvåkingssystemet.

Datasenterets overvåkingssystem samler inn og håndterer alarmer for hele infrastrukturen (strøm, generatorer, UPS-er, kjølesystem, sikkerhet og miljø). Temperatursensorer finnes i hele datasenteret, og det er installert fuktsensorer under alle kjølemaskiner. Andre sensorer kontrollerer sikkerhets- og miljømessige trusler. All data fra overvåkingssystemet presenteres i grafer, delvis for direkte advarsler, men også for trendanalyse.

Adgangskontroll.

Tilgang til datasenteret er mulig 24/7/365 for alle som leier. Det deles ut nøkkelkort til de personene som skal ha adgang. Nøkkelkortene er personlige, og kan ikke lånes ut. All trafikk inn og ut av datahallen loggføres. Rack installeres med egen lås.

Brannsikkerhet.

Datasenteret er delt inn i flere brannceller, dette betyr at slukkesystemet kun aktiveres i berørte celler ved brann. Vegger holder brannklasse EI60 (60 minutters brannmotstand). Dører klassifiseres i A60 som tilsvarer kravet EI2 og er både isolerte og tette. Alle kabeltrekk er brannsikret med forseglede åpninger.

Slukkesystem.

Fellesareal er utstyrt med brannalarm og gass-slukkesystem. Datasenteret har et avansert inergen slukkesystem. Det er følsomme detektorer som reagerer og gir alarm før synlig røyk har brutt ut. Inergengassen slukker brannen på mindre enn 60 sekunder ved å senke oksygennivået til et nivå der mennesker fortsatt kan puste, men hvor brannen kveles. Slukkesystemet er også installert under datagulv, tekniske rom og batterirom. Det er i tillegg satt ut håndslukkeapparater, disse er fylt med karbondioksid.

Energigjenvinning.

Foran kjølemaskinene på taket står det varmeveksler som henter ut mest mulig varme fra kjølevannet. Dette gjør at man kan bruke overskuddsvarmen til snøsmelting og oppvarming av bygg, samt å ha lavere forbruk på kjølemaskinene. I planleggingsfasen er det gjort arbeid for å bruke de mest energieffektive systemene, for å få ned den generelle strømbruken i hallen.

Datasenter DigiPlex – Lokasjon 2 Oslo Ulven.

DigiPlex Oslo Ulven datasenter er lokalisert i området Økern ved Oslo, historisk sett et senter for industri og produksjonsaktiviteter. Kjent som «SDS Posten bygningen» var bygget opprinnelig designet og bygget i 1981 til den Norske stat som et datasenter og kommunikasjons knutepunkt. Bygget har mer enn 4700m² med hvitt teknisk område og er konstruert som en betongramme over fire plan med alle nødvendige datasenter krav. Bygget beslaglegger et område i en triangel form, og er omgitt av en sone med sikker parkering og en 360° omkrets sikkerhets gjerde.

Fasiliteter og sikkerhet er på lokasjon 2 veldig likt som det man finner på hoved lokasjon.

Fasilitetene i datasenteret.

- Redundant strøm med UPS og diesel aggregat.
- Redundant nødstrøm, også denne med UPS og diesel aggregat.
- Datasenteret har drivstoff klart for å kunne operere med nødstrøm ved bruk av diesel aggregat i opptil 48 timer.
- Seks redundante HVAC kjølere.
- Brannsikring basert på Argonite brannslokking og tidlig røykdeteksjon.
- Redundant fiber gravd ned i bakken.
- Høy sikkerhet rundt tilgangskontroll.

Viser til dokument «Digiplex Ulven.pdf» for nærmere beskrivelse av lokasjon 2.

Generelt om vårt hosting- og driftsmiljø.

Kommunikasjon mellom våre to lokasjoner (hoved lokasjon og lokasjon 2) er sikret med Q-in-Q tunnelling (VLAN over VLAN). Pga sentral beliggenhet er avstanden til NIX («Norwegian Internet Exchange» - altså internett aksessen inn/ut av Norge) veldig kort. Dette betyr nærmest ingen forsinkelse på internett trafikk til vår løsning (maks 1-2ms, gjerne mindre). Cerpus sin internett aksess er på 10Gigabit, og i tillegg har vi en backup internett aksess på 1Gigabit. Dette sikrer maksimal båndbredde inn til våre løsninger. Alt av brannmurer er bygget opp rundt HA (High Availability), og sikrer at løsningen er oppe og fullt responsiv selv om en av brannmurene stopper. Det samme gjelder interne switcher som knytter alt av utstyr og infrastruktur sammen, alt er bygget opp med HA. Hastighet på nettverk internt i datasentral, altså mellom servere, lagring, switcher, brannmurer, etc., er på 10Gigabit, så det er ingen flaskehalser mtp hastighet ift internett aksess.

Alt av utstyr som kjører våre løsninger er topp moderne, og siste store investeringer av servere, lagring og nettverksutstyr ble gjort høsten 2015. Vår lagringsløsning er basert på Dell Compellent, denne prioriterer automatisk (automatisk TIER) for å optimalisere hastighet på lesing og skriving. Lagringen yter maksimal sikkerhet og hastighet siden denne er utstyrt med SSD disker (Solid State harddisker). Alle servere er utstyrt med 4 x 10Gigabit HA nettverksforbindelser, som ikke bare gir høy hastighet, men også høy sikkerhet og redundans.

Mao så er denne løsningen så sikker og optimal som mulig, og vil kunne by på den aller beste hastighet og stabilitet.

Verktøy for overvåking og sikkerhet.

Cerpus benytter en rekke verktøy i forvaltning av kundens løsninger for å sørge for sikkerhet og kvalitet, og for at systemene til enhver tid er tilgjengelig for sluttbruker. Flere av disse verktøyene kan rapportere og knyttes opp mot evt. SLAer som ligger til grunn for en avtale mellom partene. Cerpus søker så langt det er mulig etter verktøy basert på open source eller skybaserte tjenester. Dette gir løsningene større fleksibilitet og lavere kostnader for alle parter.

Cerpus benytter i hovedsak følgende verktøy for å overvåke og forvalte kundens løsning.

- New Relic.
- Icinga.
- Munin.
- Monitis.

Viser til dokumentet "Cerpus Helhetlige Kvalitetssystem" der våre tjenester og verktøy er ytterlige beskrevet i detalj.

Kilder: www.availo.no, www.digiplex.com, www.blix.com