Sikkerhet i Zaphire

Zaphire gjør skybasert byggautomasjon sikkert ved å bygge plattformen på Zero Trust, hvor all tilgang verifiseres, krypteres og begrenses til det som er strengt nødvendig. Med ende-til-ende kryptert kommunikasjon, ingen flate VPN-tilganger og kontinuerlige sikkerhetsoppdateringer får du et SD-anlegg som kombinerer høy tilgjengelighet med moderne cybersikkerhet.

zaphire

Si hei til ditt sikre, alt-i-ett toppsystem for bygg automasjon

Zaphire er bygget som en moderne skyplattform basert på mikrotjenester i Azure Kubernetes-miljø, og kan kjøres i sky, lokalt eller som hybrid. Denne arkitekturen gir høy skalerbarhet, fleksibilitet og mulighet for å isolere funksjoner, slik at et problem i én modul ikke sprer seg til hele systemet. Systemet har dokumentert oppetid på over 99,99%, og redundans i flere ledd for å sikre tilgjengelighet også ved feil eller vedlikehold.
Zaphire er bygget på filosofien ”Zero Trust-prinsipper”, der utgangspunktet er at ingen enheter eller brukere automatisk er til å stole på, selv om de befinner seg «på innsiden».

I praksis betyr dette blant annet: ingen flate VPN-tilganger, segmenterte anlegg, streng tilgangsstyring, kryptert kommunikasjon hele veien, og et systemdesign som ikke er avhengig av én enkelt «yttervegg» som brannmur. På denne måten reduseres konsekvensen dersom en enkelt brukerenhet, konto eller lokal komponent blir kompromittert.

Zaphire legger stor vekt på å kombinere IT-sikkerhet og driftssikkerhet i én helhetlig løsning, slik at byggherre og rådgiver slipper å velge mellom «sikkert» og «praktisk i drift».

Hvem er Zaphire?

Zaphire er et norsk selskap med base i Drammen. Siden 2018 har vi utviklet moderne systemer for byggautomasjon og energioppfølging, med fokus på brukervennlighet, sikkerhet og pålitelighet.

Zaphire er drevet av ønsket om å skape et toppsystem bygget på moderne IT-prinsipper og åpne standarder. Før vi startet å utvikle Zaphire, så vi at prosessene i tradisjonelle bygg- og energistyringssystemer var ineffektive og komplekse. De eksisterende løsningene fremstod utdaterte, vanskelige å bruke og manglet effektiviteten som kreves for å møte moderne behov. I 2018 bestemte vi oss for å løse disse utfordringene og startet arbeidet med å utvikle et system for automatisering av bygg og energi. Resultatet ble Zaphire.

I dag er Zaphire en etablert aktør i markedet, med løsninger som brukes av både kommuner og større eiendomsforvaltere. Med Zaphire får du en komplett løsning for styring, overvåkning og energioppfølging av bygg, med høy driftssikkerhet, full mobiltilgang og lavere livssykluskostnader enn tradisjonelle systemer.

Arkitektur & sikkerhetsprinsipper

Zaphire er utviklet som en fleksibel plattform som kan kjøres i skyen, lokalt eller som en hybridløsning. Arkitekturen bygger på containerteknologi og mikrotjenester, noe som sikrer både skalerbarhet og gjenbruk av tjenester på tvers av systemnivåer. For å oppnå stabil drift er løsningen konstruert med mekanismer for høy tilgjengelighet (High Availability), hvor redundans og automatisert failover sørger for at eventuelle feil ikke påvirker brukeropplevelsen.

All kommunikasjon mellom systemets komponenter er kryptert med HTTPS og moderne sikkerhetsstandarder (TLS 1.2 eller høyere, alltid med Forward Secrecy). Dette muliggjør trygg datautveksling uten behov for VPN-løsninger – som ofte tilfører kompleksitet og øker risikoen i mer tradisjonelle systemer.

Nettverksarkitekturen bygger på prinsippene om segmentering og isolasjon. Dedikerte VLAN for tekniske systemer kombinert med streng brannmurbeskyttelse hindrer innkommende trafikk og skjermer anleggene mot uautorisert tilgang. I tillegg benyttes avansert trafikkfiltrering for å beskytte både Zaphire og kundene mot distribuerte angrep (DDoS), slik at driften forblir stabil selv under høy belastning.

Zaphire er utviklet som «managed code» og oppdateres kontinuerlig. Kjente sårbarheter lukkes dermed raskt og automatisk, uten behov for manuell inngripen fra driftspersonell. Resultatet er en plattform som kombinerer moderne IT-sikkerhet med praktisk driftssikkerhet – og som gir rådgivere et robust fundament for planlegging og spesifikasjon i sine prosjekter.

Nettverksssikkerhet og VPNer

Tradisjonelt har fjernaksess til SD-anlegg ofte skjedd via VPN, som i praksis gir bred nettverkstilgang når en bruker først er pålogget. Dette øker risikoen dersom en PC eller konto kompromitteres, fordi angriperen kan bevege seg lateralt videre i nettverket.

Zaphire har derfor bevisst valgt en arkitektur uten tradisjonell VPN-tilgang for leverandører og brukere. I stedet skjer all kommunikasjon via applikasjonslaget og sikre API-er, slik at brukere aldri får direkte nettverksnivå-tilgang til byggenes tekniske nett. Tilgang begrenses til én konkret sesjon og ett definert endepunkt, og det er ikke mulig å hoppe mellom anlegg eller systemer via portalen.

Dette følger prinsippene om segmentering og «least privilege», hvor brukeren bare får det minimale tilgangsnivået som trengs for å utføre en oppgave, og angrepsflaten på nettverksnivå holdes svært liten.

Kryptert kommunikasjon

All informasjon som utveksles mellom brukere, anlegg og skytjenester i Zaphire er kryptert over HTTPS med TLS 1.2 og 1.3. Dette gjelder både ekstern kommunikasjon mot portal og API, og intern trafikk mellom mikrotjenester i skyløsningen, slik at et eventuelt kompromiss i én del ikke gir fri tilgang videre.

Zaphire følger prinsippet om «stengt som standard» - API-er og funksjoner må eksplisitt åpnes gjennom rettighetsstyring før de kan brukes. Dette reduserer risikoen for feilkonfigurasjon og gjør det enklere å ha kontroll på hvem som kan gjøre hva, spesielt i miljøer med mange brukere, integrasjoner og bygg. I tillegg åpner ikke systemet porter direkte mot internett fra anleggene, kommunikasjonen går via kontrollerte og sikre endepunkter i plattformen.

DDoS-Beskyttelse

På nettverksnivå bygger Zaphire på prinsipper om segmentering og isolasjon. Tekniske systemer legges på egne VLAN, og innkommende trafikk til anleggenes nett begrenses kraftig med brannmurregler, slik at uautorisert trafikk stoppes tidlig.

Plattformen er i tillegg beskyttet mot volumangrep gjennom avansert trafikkfiltrering og DDoS-beskyttelse i underliggende infrastruktur, slik at tjenesten forblir tilgjengelig selv under høy belastning. Dette bidrar til at SD-anlegget oppleves stabilt, også når det er økt risiko eller pågående angrep mot internett-eksponerte tjenester generelt.

Implementeringsmodell og skalerbarhet

Tradisjonelle SD-prosjekter har ofte lange utrullingsfaser, komplekse integrasjoner og tidkrevende idriftsettelser. Zaphire gjør det annerledes. Løsningen er bygget for å være rask, sikker og enkel å ta i bruk - uten å måtte gjøre store endringer i eksisterende infrastruktur.

Takket være vår modulbaserte arkitektur og åpne protokoller kan Zaphires løsning faktisk kobles til et eksisterende SD-anlegg på under 20 minutter. Alt som trengs er at en elektriker etablerer fysisk tilkobling mot byggets SD-system (for eksempel via BACnet/IP, Modbus eller MQTT).

Elektrikeren står for fysisk tilkobling og signaltilgang, mens Zaphire tar ansvar for datainnsamling, sikkerhet, analyse og visualisering. Når signalene er tilgjengelige, kobles Zaphires skyplattform automatisk til, og datainnsamlingen starter umiddelbart. Dermed er det ikke behov for VPN, tunge IT-konfigurasjoner eller komplekse integrasjonsprosjekter.

Skalerbarhet

Når ett bygg er koblet opp, kan løsningen enkelt skaleres til flere lokasjoner. Zaphire benytter samme sikre tilkoblingsmetode, slik at nye bygg kan aktiveres med minimalt fotavtrykk og uten behov for nye installasjoner. Dette gjør systemet ideelt for porteføljer som ønsker rask utrulling, standardisert datatilgang og ensartet rapportering.

zaphire

Interessert i å vite mer?
Kontakt oss i dag!

info@zaphire.no
+47 40 00 88 00