Kompromitterte leverandørkjeder

Kompromitterte leverandørkjeder – hvordan trusselen sprer seg via tredjeparter

Av Árvakr – sikkerhetspartner for virksomheter med internasjonalt utsyn

Når norske virksomheter inngår samarbeid med utenlandske partnere, vurderes ofte faktorer som pris, kapasitet og teknologisk kompetanse. En kritisk faktor får derimot langt mindre oppmerksomhet: den sikkerhetsmessige risikoen forbundet med leverandørkjeden. Tredjeparter har vært inngangsporten til flere av de mest alvorlige sikkerhetsbruddene i moderne tid – og trusselen er like relevant for norske selskaper som for globale konsern.

En usynlig inngangsdør

Tradisjonelt har virksomheter fokusert på å beskytte egne systemer, ansatte og data. Man har investert i brannmurer, antivirus, sikkerhetsopplæring og interne rutiner. Men i en globalisert virkelighet, der drift, utvikling og datalagring ofte er satt ut til eksterne – gjerne internasjonale – leverandører, flyttes angrepsflaten. Trusselen går ikke nødvendigvis gjennom hovedinngangen. Den kan komme via noen man samarbeider med, og som allerede har tilgang.

Slike samarbeid kan inkludere alt fra skytjenester og konsulentbistand til utvikling og drift av hele IT-plattformer. I praksis betyr det at eksterne aktører gis tilgang til kjernefunksjoner, ofte med høyere privilegier enn mange interne brukere. Dersom disse aktørene kompromitteres, får angriperen et effektivt bakdørsgrep.

Et av de mest kjente eksemplene på dette er SolarWinds-hendelsen i 2020, der russiske aktører kompromitterte programvare levert av et amerikansk selskap. Gjennom en tilsynelatende legitim oppdatering fikk angriperne tilgang til nettverkene til over 18 000 organisasjoner, inkludert myndigheter og private virksomheter i mange land. Hendelsen illustrerte at et brudd i ett ledd i kjeden kan få katastrofale følger for hele nettverket. Dette var ikke bare et teknisk angrep – det var et strategisk inngrep med global rekkevidde.

Også norske virksomheter er utsatt

Selv om mange av de store sakene har rammet utenlandske aktører, er risikobildet direkte relevant for norske forhold. Norske selskaper benytter i økende grad globale utviklings- og driftspartnere, og deltar i internasjonale prosjekter som krever datadeling og samhandling på tvers av grenser. I tillegg til dette arbeider mange norske virksomheter innenfor sektorer som energi, forsvar, teknologi og offentlig infrastruktur – områder som er av særlig interesse for statlige aktører.

Dette innebærer en eksponering for risikofaktorer som:

- Leverandører med drift i lavkostland med svak rettsstat eller uklar etterretningslovgivning.

- Underleverandører brukt uten at kunden informeres.
- Skytjenester eller programvare utviklet i land med høy etterretningsaktivitet og lav transparens.

Disse forholdene gjør at mange norske virksomheter – uten å være klar over det – kan være en indirekte målskive for fremmede etterretningstjenester eller organiserte trusselaktører. Selv om slike løsninger ofte er kostnadseffektive, kan de introdusere risikoer som i praksis er umulige å oppdage før skade har skjedd. Når hendelsen først skjer, er konsekvensene ofte omfattende: økonomisk tap, tap av omdømme, kundetillit og ikke minst – regulatoriske konsekvenser.

Derfor er leverandørkjeder attraktive mål

Angripere utnytter den asymmetrien som ligger i tillit. Det er ofte langt enklere å kompromittere en svakere tredjepart enn en godt sikret sluttbruker. Hvis denne tredjeparten allerede har legitim tilgang – gjennom driftstjenester, programvareoppdateringer eller systemvedlikehold – gir det en skjult inngang med høy verdi.

Statlige aktører har lenge brukt denne typen strategisk tilgang for å omgå tradisjonelle forsvarsmekanismer. Det handler ikke bare om å stjele informasjon – det handler om langsiktig posisjonering, påvirkning og uthuling av tillit. I tillegg til statlige aktører benytter også kriminelle miljøer leverandørkjeder som angrepsflate – særlig ved målrettede løsepengeangrep.

For angriperne er dette en metode med lav risiko og høy uttelling. Ofte vil det gå uker eller måneder før kompromitteringen oppdages – hvis den oppdages i det hele tatt.

Uklarhet i kjeden skaper ukontrollert risiko

En av hovedutfordringene er manglende innsikt i egen leverandørkjede. Mange virksomheter kjenner til sin primærleverandør, men har lite eller ingen oversikt over hvem som leverer tjenester i neste og tredje ledd. Dette gjør det vanskelig å gjennomføre helhetlige risikovurderinger.

Eksempel: Et norsk selskap bruker en tysk leverandør for datasystemer. Den tyske leverandøren benytter imidlertid utviklingsressurser i India, som igjen samarbeider med et lite selskap i Kina for kodevedlikehold. Selv om det norske selskapet tror de har kontroll, har de i realiteten eksponert seg for flere risikoområder – både teknisk, juridisk og geopolitisk.

I slike tilfeller hjelper det lite å ha god sikkerhetskontroll internt, dersom kjeden man er en del av ikke holder samme nivå. Risikoen blir systemisk.

Spørsmål alle virksomheter bør stille

For å sikre at internasjonale samarbeidspartnere ikke blir en akilleshæl, bør virksomheter stille seg selv følgende spørsmål:

- Hvor er leverandøren fysisk og juridisk lokalisert? Er den underlagt lovgivning som åpner for statlig innsyn i data?

- Hva vet vi om eierskapet og styringen i selskapet? Finnes det bånd til myndigheter eller sikkerhetstjenester?
- Benytter leverandøren selv underleverandører? I hvilke land, og med hvilke sikkerhetsprosedyrer?
- Hvordan ivaretas informasjonssikkerhet? Er det krav til tilgangsstyring, logging, revisjon og kryptering?

Disse spørsmålene bør ikke være engangsvurderinger, men en del av en kontinuerlig prosess for risikostyring.

Hvordan Árvakr bistår

Árvakr tilbyr målrettede tjenester for å hjelpe virksomheter med å kartlegge og redusere risiko knyttet til internasjonale samarbeidspartnere og leverandørkjeder. Dette inkluderer:

- **Sikkerhetsmessig due diligence:** Vurdering av eierskap, jurisdiksjon, teknisk arkitektur og bakgrunnsforhold.
- **Kartlegging av skjulte avhengigheter:** Analyse av hvilke tredje- og fjerdeparter som inngår i leverandørkjeden.
- **Trusselvurderinger knyttet til nasjonal sikkerhet:** Geopolitisk analyse av aktører og miljøet de opererer i.
- **Rådgivning knyttet til kontrakter og sikkerhetskrav:** Hvordan formulere krav til informasjonssikkerhet, audit-rettigheter og håndtering av sikkerhetsbrudd.
- **Bevisstgjøring i ledelse og innkjøpsfunksjoner:** Hvordan integrere sikkerhetsvurderinger i beslutningsprosesser.

Tillit må være strukturert – ikke automatisk

Det moderne sikkerhetslandskapet stiller nye krav til hvordan virksomheter vurderer samarbeid. Tillit kan ikke lenger baseres på forutsetninger om at alle aktører opererer med samme forståelse av risiko og ansvar. Det må bygges gjennom strukturert innsikt, kontrollmekanismer og kontinuerlig oppfølging.

Kompromitterte leverandørkjeder er ikke et hypotetisk fremtidsscenario – de er en etablert realitet. Ved å ta proaktive grep kan virksomheter unngå at skjulte svakheter i leverandørnettet utvikler seg til kritiske hendelser. Árvakr bistår med nettopp dette: Å gi virksomheter verktøyene de trenger for å forstå og kontrollere sikkerhetsrisiko i internasjonale samarbeid – før det er for sent.