Engineer

Zero trust

en modell som ikke gir tillit ut fra nettverket alene

Hva det er

Zero trust er en sikkerhetsmodell der ingenting får tillit bare fordi det befinner seg et bestemt sted i nettverket. NIST SP 800-207, den amerikanske føderale publikasjonen som beskrev modellen i 2020, definerer den som et paradigme rettet mot å beskytte ressurser, ut fra premisset om at tillit aldri gis implisitt, men hele tiden må vurderes. Å sitte på kontornettet, være koblet til via VPN eller stå i samme datasenter gir ikke i seg selv en forespørsel noe som helst. Hver forespørsel om en ressurs avgjøres for seg: hvem som spør, fra hvilken enhet, om hva og under hvilke forhold. På norsk ser man også betegnelsen nulltillit, og planen som setter modellen ut i livet, kalles en zero trust-arkitektur, forkortet ZTA.

NIST navngir partene presist. Et subjekt er den eller det som sender en forespørsel: en person, en tjeneste eller en enhet. En ressurs er alt som er verdt å beskytte, og publikasjonen regner skrivere og regnekraft på linje med data. Mellom de to står tre logiske komponenter. Policymotoren (policy engine) avgjør om en forespørsel innvilges, og logger avgjørelsen. Policyadministratoren (policy administrator) gjennomfører den: den åpner eller stenger forbindelsen mellom subjekt og ressurs og utsteder påloggingsopplysninger eller tokener for akkurat den økten. Håndhevingspunktet (policy enforcement point) sitter i selve forbindelsen: det slipper økten gjennom, følger med på den og avslutter den når det får beskjed om det.

Publikasjonen forklarer skiftet med en flyplass. Passasjerene går gjennom én kontroll, og bak den beveger reisende, besetning og flyplassansatte seg fritt rundt i terminalen, og alle behandles som klarerte. Terminalen er det NIST kaller en sone med implisitt tillit: et område der alle har den tilliten det siste kontrollpunktet de passerte, ga dem. Et flatt kontornett fungerer på samme måte. Zero trust gjør sonen så liten som mulig ved å flytte avgjørelsen og håndhevingen nærmere ressursen.

Bruk begrepet i en beslutning

Bruk «Hva er zero trust?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Kontoer, passord og tilganger ordnet slik at folk har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Skrev 1 000 RBAC-regler for å sikre Linux-servere — 1,000 tilgangsregler skrevet for å tette et sikkerhetshull

Skrev 1 000 RBAC-regler for å sikre Linux-servere Ta kontakt →

Hvorfor det er viktig

Den eldre modellen trekker én grense rundt organisasjonen og stoler på det som er innenfor. NISTs innvending er enkel: når en angriper først har kommet seg gjennom perimeteren, kan vedkommende bevege seg uhindret fra system til system, og slik uautorisert sidelengs bevegelse har vært en av de største utfordringene for etatene publikasjonen ble skrevet for. Grensen passer heller ikke lenger med arbeidet. Ansatte logger på fra hjemmenett og hotellnett, private enheter slippes inn på noen systemer, og mye av det de jobber i, kjører i noen andres sky. NISTs antakelser følger av dette: det private nettverket er ingen sone med implisitt tillit, en angriper kan allerede være der, og ansatte som jobber andre steder fra, bør regne det lokale nettverket de kobler seg til, som fiendtlig.

Gevinsten for dere er at skaden holdes innenfor. Etter det tredje av NISTs sju grunnprinsipper gis tilgang per økt med så få privilegier som oppgaven krever, og autentisering mot én ressurs gir ingenting mot en annen. Et stjålet passord eller en kompromittert bærbar når da bare det kontoen og enheten har lov til å nå, i det øyeblikket og gjennom ett håndhevingspunkt, og ikke hele det interne nettverket. Avgjørelsene etterlater også et spor. Policymotoren registrerer hver innvilgelse og hvert avslag, slik at spørsmålet om hvem som kunne nå et system, og hvorfor, besvares ut fra registreringer og ikke ut fra hukommelsen.

Slik ser det ut i praksis

Ta et innkjøpssystem, den typen applikasjon NIST foreslår for en første migrering, fordi en avgrenset gruppe ansatte bruker den, i motsetning til e-post, som hele organisasjonen er avhengig av. En innkjøper åpner systemet fra en bærbar som virksomheten eier. Forespørselen når håndhevingspunktet foran applikasjonen, som spør policymotoren. Motorens tillitsalgoritme vekter de inndataene NIST lister opp: selve forespørselen, blant annet enhetens operativsystemversjon og oppdateringsnivå; databasen over subjekter; databasen over eiendeler;

ressursens egne krav, som kan angi et sikkerhetsnivå for autentisering eller avvise adresser i utlandet; og trusselinformasjon. En illustrerende avgjørelse, med feltnavn vi har valgt selv og ikke hentet fra noe produkt, kunne sett slik ut:

```
forespørsel  innkjøper-17 på laptop-0417 -> innkjøpssystemet, lese og skrive
subjekt      innkjøpsteamet; pålogget med nøkkel motstandsdyktig mot phishing
eiendel      virksomhetens enhet, oppdatert operativsystem, kryptert disk
ressurs      krever AAL2 eller høyere, administrert enhet, norsk IP-adresse
trussel      avsenderadressen står ikke i trusselstrømmene vi har sjekket
avgjørelse   innvilg lesing og skriving for denne økten; logg som godkjent
```

Tildelingen gjelder denne ene økten og dette ene systemet. Når den samme innkjøperen på den samme bærbare åpner leverandørkontraktene i et dokumentlager, tar motoren en ny avgjørelse om tilgang: autentisering mot den første ressursen gir ikke automatisk tilgang til den andre. Konteksten teller også. Et av NISTs eksempler er en regnskapsmedarbeider som vanligvis jobber i kontortiden, og som plutselig ber om tilgang til økonomisystemet midt på natten fra et sted motoren ikke kjenner igjen: en kontekstuell tillitsalgoritme kan da utløse et varsel og kreve at subjektet først oppfyller et strengere tillitsnivå. Et annet er en HR-medarbeider som en vanlig dag leser 20 til 30 personalmapper og så ber om mer enn 100.

For skytjenester påpeker NIST at klientene kan gå rett til tjenesten, mens virksomhetens håndhevingspunkter kontrollerer policyen underveis, i stedet for først å bli ført inn i det interne nettverket via VPN. Alle disse avgjørelsene forutsetter et klart bilde av hvem som skal nå hva, og NIST ber om en kartlegging av eiendeler, subjekter, dataflyt og arbeidsflyter før noe bygges. Det forarbeidet tilsvarer samlingen vi beskriver i caset vårt om tilgangsstyring på tvers av M365 og SSO: identitetene og tilgangene samlet i M365, 1Password, Red Hat SSO og OKTA SSO, minste privilegium håndhevet og onboarding og offboarding standardisert, slik at tilganger ble gitt og trukket tilbake raskt og konsekvent.

Hvor det går galt

Det kjøpes som et produkt. NIST slår fast at zero trust er et sett veiledende prinsipper og ikke én bestemt arkitektur, og at det ikke finnes ett samlet sett verktøy eller tjenester for en virksomhet bygget på zero trust. En ny gateway for fjerntilgang med riktig merkelapp på esken endrer lite hvis hvert subjekt den slipper inn, fortsatt når hele nettverket bak den. Se heller overgangen slik NIST

gjør, som en reise og ikke en utskifting av alt på én gang, og ta én forretningsprosess om gangen. Vurder hvert produkt mot prinsippene det skal oppfylle, også om dataformatene lar dere bytte til en annen leverandør senere.

Policyen skrives før kartleggingen. Policymotoren kan bare avgjøre ut fra det den vet om subjekter, eiendeler og prosesser. Der den kunnskapen er ufullstendig, advarer NIST, er det vanlige resultatet en forretningsprosess som stopper opp fordi motoren avviser forespørsler i mangel av opplysninger, og skygge-IT, altså systemer satt opp utenfor IT-avdelingens styring, gjør det verre. Kartlegg derfor først eiendeler, subjekter, dataflyt og arbeidsflyter, skygge-IT medregnet, og skriv først deretter kriteriene for prosessen som skal flyttes.

Administratorene beholder full tilgang. I mange eldre oppsett kan utviklere og systemadministratorer nå alle ressurser, og NIST peker ut nettopp disse kontoene for ekstra oppmerksomhet. Flytter man alle andre bak avgjørelser per økt mens administratorkontoene beholder sin faste rekkevidde, blir de mest verdifulle påloggingsopplysningene den korteste veien inn. Send derfor også de privilegerte kontoene gjennom den samme motoren, gi dem tilgangen den aktuelle oppgaven krever, og bruk logging og revisjon til å lære de normale mønstrene deres, slik at avvik skiller seg ut.

Policymotoren blir den nye perimeteren. Ingen ressurs snakker med en annen uten at motoren og administratoren godkjenner det. Den som har tilgang til motorens regler, kan gjøre endringer uten godkjenning eller rene feil, og en angriper som forstyrrer håndhevingspunktene eller administratoren, kan stanse virksomheten. Logg og revider derfor hver endring av konfigurasjonen, kjør håndhevingen i et forsvarlig sikret skymiljø eller repliker den flere steder, og gi de lagrede nettverksdataene og policyen den strengeste tilgangen av alle, bare fra egne administratorkontoer.

Alt håndheves fra første dag. Få policysett blir riktige på første forsøk, og NIST regner med en innkjøringsfase der forespørsler som burde gått gjennom, blir avvist. Går man rett til streng håndheving, blir hvert hull i policyen til ansatte som står uten tilgang til arbeid de trenger å gjøre. Kjør heller den nye arbeidsflyten en periode i en modus der avgjørelsene bare rapporteres. Innvilg de fleste forespørslene, sammenlign loggene med den tiltenkte policyen, og håndhev bare det grunnleggende, som å avvise forespørsler der MFA feiler, eller som kommer fra adresser man vet er fiendtlige. Stram inn policyen når det normale mønsteret er forstått.

MFA blir målstreken. MFA reduserer risikoen ved et stjålet passord, men NIST påpeker at en angriper med gyldige påloggingsopplysninger, eller en ondsinnet innsider, fortsatt kan nå alt kontoen har lov til. Hold derfor hver kontos rekkevidde smal, og bruk en kontekstuell tillitsalgoritme som vekter tidspunkt, sted og mengde, slik at gyldige påloggingsopplysninger brukt på en uvanlig måte likevel utløser et varsel.

Les mer

- NIST SP 800-207, Zero Trust Architecture — publisert i august 2020: definisjonen, de sju grunnprinsippene, de logiske komponentene, truslene og et veikart for omleggingen.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — NISTs praksisveiledning fra juni 2025, som beskriver 19 eksempler på implementeringer bygget sammen med 24 samarbeidspartnere.
- NIST SP 800-207A — publisert i september 2023: tilgangskontroll for skybaserte applikasjoner på tvers av flere skyer, basert på API-gatewayer, sidecar-proxyer og tjenesteidentiteter i stedet for nettverksadresser.
- NIST SP 800-63B-4 — sikkerhetsnivåene for autentisering som kravene til en ressurs kan vise til, der AAL3 krever motstandsdyktighet mot phishing.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er zero trust?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

welcome@engineer.company +45 50 10 61 84 København, Danmark

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/zero-trust/