Engineer

Zero trust

en model, der ikke giver tillid ud fra netværket alene

Hvad det er

Zero trust er en sikkerhedsmodel, hvor intet nyder tillid, blot fordi det befinder sig et bestemt sted på netværket. NIST SP 800-207, den amerikanske føderale publikation, der beskrev modellen i 2020, definerer den som et paradigme rettet mod at beskytte ressourcer, ud fra den præmis at tillid aldrig gives implicit, men hele tiden skal vurderes. At sidde på kontorets netværk, være på VPN'en eller stå i samme datacenter giver ikke i sig selv en anmodning noget. Hver anmodning om en ressource afgøres for sig: hvem spørger, fra hvilken enhed, om hvad og under hvilke forhold. På dansk bruges det engelske navn, og i sammensætninger skrives det med bindestreg, som i zero trust-arkitektur, forkortet ZTA, der er betegnelsen for den plan, som omsætter modellen til praksis.

NIST navngiver parterne præcist. Et subjekt er den eller det, der fremsætter en anmodning: en person, en tjeneste eller en enhed. En ressource er alt, hvad der er værd at beskytte, og publikationen regner printere og regnekraft med på linje med data. Mellem de to står tre logiske komponenter. Politikmotoren (policy engine) afgør, om en anmodning imødekommes, og logger afgørelsen. Politikadministratoren (policy administrator) fører den ud i livet: den åbner eller lukker forbindelsen mellem subjekt og ressource og udsteder legitimationsoplysninger eller tokens til netop den session. Håndhævelsespunktet (policy enforcement point) sidder i selve forbindelsen: det lukker sessionen igennem, holder øje med den og afbryder den, når det får besked på det.

Publikationen forklarer skiftet med en lufthavn. Passagererne går gennem én kontrol, og bag den bevæger rejsende, besætning og lufthavnens personale sig rundt i terminalen og behandles alle som betroede. Terminalen er det, NIST kalder en zone med implicit tillid: et område, hvor alle nyder den tillid, det

seneste kontrolpunkt gav dem. Et fladt kontornetværk fungerer på samme måde. Zero trust gør zonen så lille som muligt ved at flytte afgørelsen og håndhævelsen tættere på ressourcen.

Brug begrebet i en beslutning

Brug »Hvad er zero trust?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Konti, adgangskoder og rettigheder sat op, så folk har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har skrevet 1.000 RBAC-regler til Linux-servere — 1,000 adgangsregler skrevet for at lukke et sikkerhedshul

Har skrevet 1.000 RBAC-regler til Linux-servere Kontakt os →

Hvorfor det betyder noget

Den ældre model trækker én grænse rundt om organisationen og stoler på det, der er indenfor. NIST's indvending er ligetil: når en angriber først er kommet gennem perimeteren, kan vedkommende bevæge sig frit fra system til system, og den slags uautoriserede sidelæns bevægelser har været en af de største udfordringer for de myndigheder, publikationen blev skrevet til. Grænsen passer heller ikke længere til arbejdet. Medarbejdere logger ind fra hjemmenetværk og hotelnetværk, private enheder får adgang til nogle systemer, og meget af det, de arbejder i, kører i en andens cloud. NIST's antagelser følger heraf: det private netværk er ingen zone med implicit tillid, en angriber kan allerede være på det, og medarbejdere, der arbejder andre steder fra, bør betragte det lokale netværk, de kobler sig på, som fjendtligt.

Det, I vinder, er, at skaden kan holdes inde. Efter det tredje af NIST's syv grundprincipper gives adgang pr. session med det mindste privilegium, opgaven kræver, og autentificering over for én ressource giver intet over for en anden. En stjålen adgangskode eller en kompromitteret bærbar når så kun det, kontoen og enheden må nå, i det øjeblik og gennem ét håndhævelsespunkt, og ikke hele det interne netværk. Afgørelserne efterlader også et spor. Politikmotoren registrerer hver tildeling og hvert afslag, så spørgsmålet om, hvem der kunne nå et system og hvorfor, besvares ud fra registreringer og ikke ud fra hukommelsen.

Sådan ser det ud i praksis

Tag et indkøbssystem, den slags system NIST foreslår at begynde med, fordi en afgrænset gruppe medarbejdere arbejder i det, i modsætning til e-mail, som hele organisationen er afhængig af. En indkøber åbner det fra en bærbar, som virksomheden ejer. Anmodningen når håndhævelsespunktet foran systemet, som spørger politikmotoren. Motorens tillidsalgoritme vejer de input, NIST opregner: selve anmodningen, herunder enhedens styresystemversion og patchniveau; databasen over subjekter; databasen over aktiver; ressourcens egne krav, som kan angive et sikringsniveau for login eller afvise adresser i udlandet; og trusselsinformation. En illustrativ afgørelse, med feltnavne, vi selv har valgt, og ikke noget produkts, kunne se sådan ud:

```
anmodning  indkøber-17 på laptop-0417 -> indkøbssystemet, læse og skrive
subjekt    indkøbsteamet; logget ind med en phishing-resistent nøgle
aktiv      virksomhedens enhed, opdateret styresystem, krypteret disk
ressource  kræver AAL2 eller højere, en administreret enhed, en dansk IP
trussel    afsenderadressen står i ingen af de trusselsfeeds, vi tjekker
afgørelse  giv læse- og skriveadgang i denne session; log som godkendt
```

Tildelingen gælder denne ene session og dette ene system. Når den samme indkøber på den samme bærbare åbner leverandørkontrakterne i et dokumentlager, træffer motoren en ny adgangsafgørelse: autentificering over for den første ressource giver ikke automatisk adgang til den anden. Konteksten tæller også. Et af NIST's eksempler er en regnskabsmedarbejder, der normalt arbejder i kontortiden og pludselig beder om adgang til økonomisystemet midt om natten fra et sted, motoren ikke genkender: en kontekstuel tillidsalgoritme kan da slå alarm og kræve, at subjektet først opfylder et strengere tillidsniveau. Et andet er en HR-medarbejder, der en almindelig dag læser 20 til 30 personalesager og så beder om mere end 100.

Til tjenester i skyen påpeger NIST, at klienterne kan gå direkte til tjenesten, mens organisationens håndhævelsespunkter kontrollerer politikken undervejs, i stedet for først at blive ført ind i det interne netværk over en VPN. Alle disse afgørelser forudsætter et klart billede af, hvem der skal kunne nå hvad, og NIST beder om en kortlægning af aktiver, subjekter, dataflow og arbejdsgange, før noget bygges. Det forarbejde svarer til den samling, vi beskriver i vores case om adgangsstyring med M365 og SSO: identiteter og adgange samlet i M365, 1Password, Red Hat SSO og OKTA SSO, least privilege håndhævet og on- og offboarding standardiseret, så adgang blev givet og frataget hurtigt og ensartet.

Hvor det går galt

Det købes som et produkt. NIST slår fast, at zero trust er et sæt vejledende principper og ikke én bestemt arkitektur, og at der ikke findes ét samlet sæt værktøjer eller tjenester til en virksomhed bygget på zero trust. En ny gateway til fjernadgang med det rigtige mærkat på æsken ændrer ikke meget, hvis hvert subjekt, den lukker ind, stadig kan nå hele netværket bagved. Se i stedet overgangen, som NIST gør, som en rejse og ikke en udskiftning af det hele på én gang, og tag én forretningsproces ad gangen. Vurdér hvert produkt ud fra de principper, det skal opfylde, herunder om dets dataformater lader jer skifte til en anden leverandør senere.

Politikken skrives før kortlægningen. Politikmotoren kan kun afgøre ud fra det, den ved om subjekter, aktiver og processer. Hvor den viden er ufuldstændig, advarer NIST, er det typiske resultat en forretningsproces, der går i stå, fordi motoren afviser anmodninger af mangel på oplysninger, og skygge-it, altså systemer sat op uden om it-afdelingens styring, gør det værre. Løsningen er først at kortlægge aktiver, subjekter, dataflow og arbejdsgange, skygge-it medregnet, og først derefter skrive kriterierne for den proces, der skal flyttes.

Administratorerne beholder fuld adgang. I mange ældre opsætninger kan udviklere og systemadministratorer nå alle ressourcer, og NIST udpeger netop de konti til ekstra opmærksomhed. Flytter man alle andre bag afgørelser pr. session, mens administratorkontiene beholder deres faste rækkevidde, bliver de mest værdifulde loginoplysninger den korteste vej ind. Send derfor også de privilegerede konti gennem den samme motor, giv dem den adgang, deres aktuelle opgave kræver, og brug logning og revision til at lære deres normale mønstre, så afvigelser springer i øjnene.

Politikmotoren bliver den nye perimeter. Ingen ressource taler med en anden, medmindre motoren og administratoren godkender det. Den, der har adgang til motorens regler, kan lave uautoriserede ændringer eller rene fejl, og en angriber, der forstyrrer håndhævelsespunkterne eller administratoren, kan bringe forretningen i stå. Log og revidér derfor hver ændring af konfigurationen, kør håndhævelsen i et forsvarligt sikret cloudmiljø eller repliker den flere steder, og giv de lagrede netværksdata og politikken den mest restriktive adgang af alle, kun fra dedikerede administratorkonti.

Alt håndhæves fra første dag. Få politiksæt er rigtige i første forsøg, og NIST regner med en indkøringsfase, hvor anmodninger, der burde gå igennem, bliver afvist. Går man direkte til streng håndhævelse, bliver hvert hul i politikken til medarbejdere, der står uden adgang til arbejde, de har brug for. Kør i stedet den nye arbejdsgang i en tilstand, hvor afgørelserne kun rapporteres, et stykke tid. Imødekom de fleste anmodninger, sammenlign logfilerne med den tilsigtede politik, og håndhæv kun det grundlæggende, som at afvise anmodninger, hvor MFA slår fejl, eller som kommer fra adresser, man ved er fjendtlige. Stram politikken, når det normale mønster er forstået.

MFA bliver målstregen. MFA mindsker risikoen ved en stjålen adgangskode, men NIST påpeger, at en angriber med gyldige loginoplysninger, eller en ondsindet insider, stadig kan nå alt det, kontoen har lov til. Hold derfor hver kontos rækkevidde snæver, og brug en kontekstuel tillidsalgoritme, der vejer tidspunkt, sted og mængde, så gyldige loginoplysninger, der bruges på en usædvanlig måde, stadig udløser en alarm.

Læs mere

- NIST SP 800-207, Zero Trust Architecture — udgivet i august 2020: definitionen, de syv grundprincipper, de logiske komponenter, truslerne og en køreplan for omlægningen.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — NIST's praksisvejledning fra juni 2025, der beskriver 19 eksempler på implementeringer bygget sammen med 24 samarbejdspartnere.
- NIST SP 800-207A — udgivet i september 2023: adgangskontrol til cloud-native applikationer på tværs af flere clouds, baseret på API-gateways, sidecar-proxyer og tjenesteidentiteter frem for netværksadresser.
- NIST SP 800-63B-4 — de sikringsniveauer for autentificering, som en ressources krav kan henvise til, hvoraf AAL3 kræver phishing-resistens.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er zero trust?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/zero-trust/