Engineer

Zero trust

en modell som inte ger förtroende enbart utifrån nätverket

Vad det är

Zero trust är en säkerhetsmodell där ingenting får förtroende bara för att det befinner sig på en viss plats i nätverket. NIST SP 800-207, den amerikanska federala publikation som beskrev modellen 2020, definierar den som ett paradigm inriktat på att skydda resurser, utifrån premissen att förtroende aldrig ges implicit utan hela tiden måste utvärderas. Att sitta på kontorsnätet, vara uppkopplad via VPN eller stå i samma datacenter ger i sig inte en begäran någonting. Varje begäran om en resurs avgörs för sig: vem som frågar, från vilken enhet, om vad och under vilka förhållanden. På svenska används den engelska benämningen, och i sammansättningar skrivs den med bindestreck, som i zero trust-arkitektur (ZTA), den plan som omsätter modellen i praktiken.

NIST namnger parterna noggrant. Ett subjekt är den eller det som skickar en begäran: en person, en tjänst eller en enhet. En resurs är allt som är värt att skydda, och publikationen räknar skrivare och beräkningskapacitet till resurserna vid sidan av data. Mellan de två står tre logiska komponenter. Policymotorn (policy engine) avgör om en begäran ska beviljas och loggar beslutet. Policyadministratören (policy administrator) verkställer det: den öppnar eller stänger förbindelsen mellan subjekt och resurs och utfärdar inloggningsuppgifter eller token för just den sessionen. Tillämpningspunkten (policy enforcement point) sitter i själva förbindelsen: den släpper igenom sessionen, håller uppsikt över den och avslutar den när den får besked om det.

Publikationen förklarar skiftet med en flygplats. Passagerarna går igenom en kontroll, och bakom den rör sig resenärer, besättningar och flygplatspersonal fritt i terminalen och behandlas alla som betrodda. Terminalen är vad NIST kallar en zon med implicit förtroende: ett område där alla har det förtroende som den senaste kontrollpunkten de passerade gav dem. Ett platt kontorsnät fungerar på samma sätt. Zero trust gör zonen så liten som möjligt genom att flytta beslutet och tillämpningen närmare resursen.

Använd begreppet i ett beslut

Använd ”Vad är zero trust?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

Skrev 1 000 RBAC-regler som säkrar Linux-servrar Hör av er →

Varför det spelar roll

Den äldre modellen drar en gräns runt organisationen och litar på det som finns innanför. NIST:s invändning är enkel: när en angripare väl har tagit sig igenom perimetern kan hen röra sig obehindrat från system till system, och sådan obehörig lateral förflyttning har varit en av de största utmaningarna för de myndigheter publikationen skrevs för. Gränsen stämmer inte heller längre med hur arbetet ser ut. Medarbetare loggar in från hemmanätverk och hotellnätverk, privata enheter släpps in i vissa system, och mycket av det de arbetar i körs i någon annans moln. NIST:s antaganden följer av detta: det privata nätverket är ingen zon med implicit förtroende, en angripare kan redan finnas där, och medarbetare som arbetar på distans bör betrakta det lokala nätverk de ansluter från som fientligt.

Vinsten för er är att skadan går att begränsa. Enligt den tredje av NIST:s sju grundprinciper ges åtkomst per session med minsta möjliga behörighet för uppgiften, och autentisering mot en resurs ger ingenting mot en annan. Ett stulet lösenord eller en komprometterad bärbar dator når då bara det som kontot och enheten får nå, i det ögonblicket och genom en tillämpningspunkt, och inte hela det interna nätverket. Besluten lämnar också spår. Policymotorn registrerar varje beviljande och varje avslag, så frågan om vem som kunde nå ett system, och varför, besvaras utifrån registreringar och inte ur minnet.

Så ser det ut i praktiken

Ta ett inköpssystem, den sortens applikation som NIST föreslår för en första migrering, eftersom en avgränsad grupp medarbetare arbetar i den, till skillnad från e-post, som hela organisationen är beroende av. En inköpare öppnar systemet från en bärbar dator som verksamheten äger. Begäran når tillämpningspunkten framför applikationen, som frågar policymotorn. Motorns förtroendealgoritm väger in de indata som NIST räknar upp: själva begäran, bland annat enhetens operativsystemversion och uppdateringsnivå; databasen över

subjekt; databasen över tillgångar; resursens egna krav, som kan ange en tillitsnivå för autentisering eller avvisa adresser i utlandet; och hotinformation. Ett illustrerande beslut, med fältnamn som vi har valt själva och inte hämtat från någon produkt, skulle kunna se ut så här:

```
begäran   inköpare-17 på laptop-0417 -> inköpssystemet, läsa och skriva
subjekt   inköpsteamet; inloggad med en nätfiskeresistent nyckel
tillgång  verksamhetens enhet, uppdaterat operativsystem, krypterad disk
resurs    kräver AAL2 eller högre, en hanterad enhet, en svensk IP-adress
hot       avsändaradressen finns inte i de hotflöden vi har kontrollerat
beslut    bevilja läsning och skrivning för sessionen; logga som godkänt
```

Beviljandet gäller den här enda sessionen och det här enda systemet. När samma inköpare på samma bärbara dator öppnar leverantörsavtalen i ett dokumentarkiv fattar motorn ett nytt åtkomstbeslut: autentisering mot den första resursen ger inte automatiskt åtkomst till den andra. Sammanhanget räknas också. Ett av NIST:s exempel är en redovisningsekonom som normalt arbetar under kontorstid och plötsligt begär åtkomst till ekonomisystemet mitt i natten från en plats som motorn inte känner igen: en kontextuell förtroendealgoritm kan då utlösa ett larm och kräva att subjektet först uppfyller en striktare förtroendenivå. Ett annat är en HR-medarbetare som en vanlig dag läser 20 till 30 personalakter och sedan begär fler än 100.

För molntjänster påpekar NIST att klienterna kan gå direkt till tjänsten, medan organisationens tillämpningspunkter kontrollerar policyn på vägen, i stället för att först föras in i det interna nätverket via VPN. Alla dessa beslut förutsätter en tydlig bild av vem som ska nå vad, och NIST ber om en kartläggning av tillgångar, subjekt, dataflöden och arbetsflöden innan något byggs. Det förarbetet motsvarar ett av projekten här på webbplatsen, behörighetshantering i M365 och SSO, där identiteterna och åtkomsten samlades i M365, 1Password, Red Hat SSO och OKTA SSO. Principen om minsta behörighet upprätthölls, och onboarding och offboarding standardiserades, så att åtkomst beviljades och återkallades snabbt och konsekvent.

Var det går fel

Det köps som en produkt. NIST slår fast att zero trust är en uppsättning vägledande principer och inte en enda arkitektur, och att det inte finns någon enskild uppsättning verktyg eller tjänster för en verksamhet byggd på zero trust. En ny gateway för fjärråtkomst med rätt etikett på kartongen ändrar lite om varje

subjekt den släpper in fortfarande når hela nätverket bakom den. Se i stället övergången som NIST gör, som en resa och inte ett utbyte av allt på en gång, och ta en affärsprocess i taget. Bedöm varje produkt mot de principer den ska uppfylla, och kontrollera också om dess dataformat låter er byta till en annan leverantör senare.

Policyn skrivs före kartläggningen. Policymotorn kan bara besluta utifrån det den vet om subjekt, tillgångar och processer. Där den kunskapen är ofullständig, varnar NIST, blir det vanliga resultatet en affärsprocess som stannar av eftersom motorn avvisar begäranden i brist på information, och skugg-IT, alltså system som satts upp utanför IT-avdelningens styrning, gör det värre. Kartlägg därför först tillgångar, subjekt, dataflöden och arbetsflöden, skugg-IT inräknat, och skriv först därefter kriterierna för den process som ska flyttas.

Administratörerna behåller full åtkomst. I många äldre upplägg kan utvecklare och systemadministratörer nå alla resurser, och NIST pekar ut just de kontona för särskild uppmärksamhet. Flyttar man alla andra bakom beslut per session medan administratörskontona behåller sin fasta räckvidd, blir de mest värdefulla inloggningsuppgifterna den kortaste vägen in. Låt därför även de privilegierade kontona gå genom samma motor, ge dem den åtkomst som den aktuella uppgiften kräver, och använd loggning och granskning för att lära känna deras normala mönster, så att avvikelser sticker ut.

Policymotorn blir den nya perimetern. Ingen resurs talar med en annan utan att motorn och administratören godkänner det. Den som har åtkomst till motorns regler kan göra ändringar utan godkännande eller rena misstag, och en angripare som stör tillämpningspunkterna eller administratören kan få verksamheten att stanna. Logga och granska därför varje ändring av konfigurationen, kör tillämpningen i en ordentligt skyddad molnmiljö eller replikera den på flera platser, och ge lagrade trafikdata och policyn den mest restriktiva åtkomsten av alla, enbart från dedikerade administratörskonton.

Allt tillämpas skarpt från första dagen. Få policyuppsättningar blir rätt på första försöket, och NIST räknar med en inkörningsfas där begäranden som borde gå igenom avvisas. Går man direkt till strikt tillämpning blir varje lucka i policyn till medarbetare som står utan åtkomst till arbete de behöver göra. Kör i stället det nya arbetsflödet en tid i ett läge där besluten bara rapporteras. Bevilja de flesta begäranden, jämför loggarna med den avsedda policyn och tillämpa

bara det grundläggande, som att avvisa begäranden där MFA misslyckas eller som kommer från adresser som man vet är fientliga. Skärp policyn när det normala mönstret är förstått.

MFA blir mållinjen. MFA minskar risken med ett stulet lösenord, men NIST påpekar att en angripare med giltiga inloggningsuppgifter, eller en illasinnad insider, fortfarande kan nå allt som kontot har rätt till. Håll därför varje kontos räckvidd snäv, och använd en kontextuell förtroendealgoritm som väger in tidpunkt, plats och mängd, så att giltiga inloggningsuppgifter som används på ett ovanligt sätt ändå utlöser ett larm.

Läs mer

- NIST SP 800-207, Zero Trust Architecture — publicerad i augusti 2020: definitionen, de sju grundprinciperna, de logiska komponenterna, hoten och en färdplan för omställningen.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — NIST:s praktiska vägledning från juni 2025, som beskriver 19 exempel på implementeringar byggda tillsammans med 24 samarbetspartner.
- NIST SP 800-207A — publicerad i september 2023: åtkomstkontroll för molnnativa applikationer i flera moln, baserad på API-gatewayer, sidecar-proxyer och tjänsteidentiteter i stället för nätverksadresser.
- NIST SP 800-63B-4 — tillitsnivåerna för autentisering som kraven för en resurs kan hänvisa till, där AAL3 kräver nätfiskeresistens.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är zero trust?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/zero-trust/