



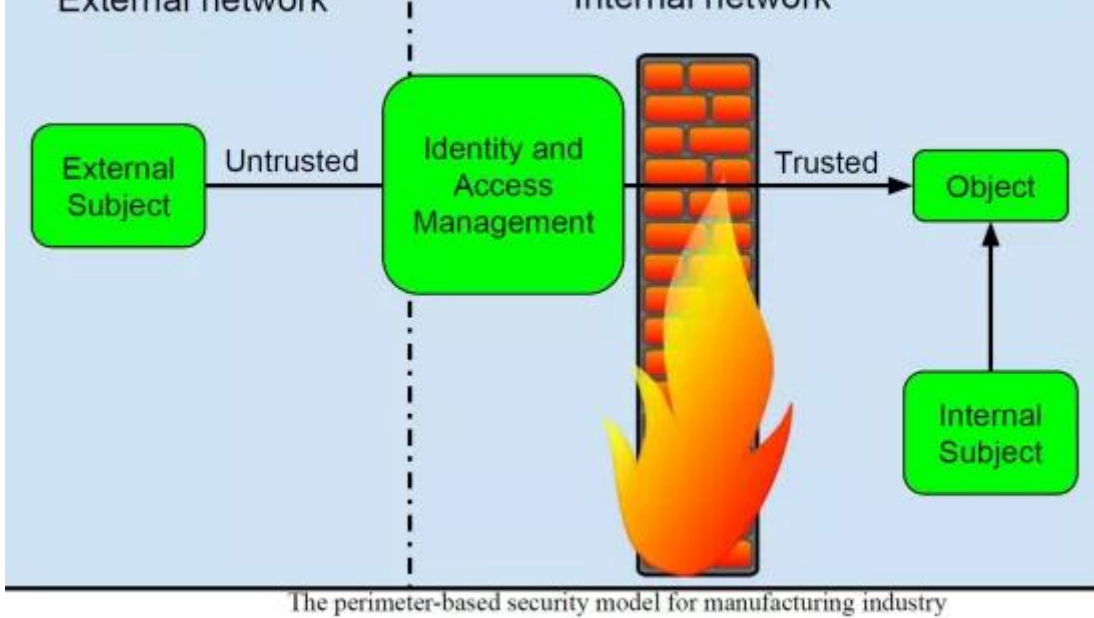
## Zero Trust: naar een veilige architectuur voor smart manufacturing

16 februari 2023, 09:46

Farhad Aghili

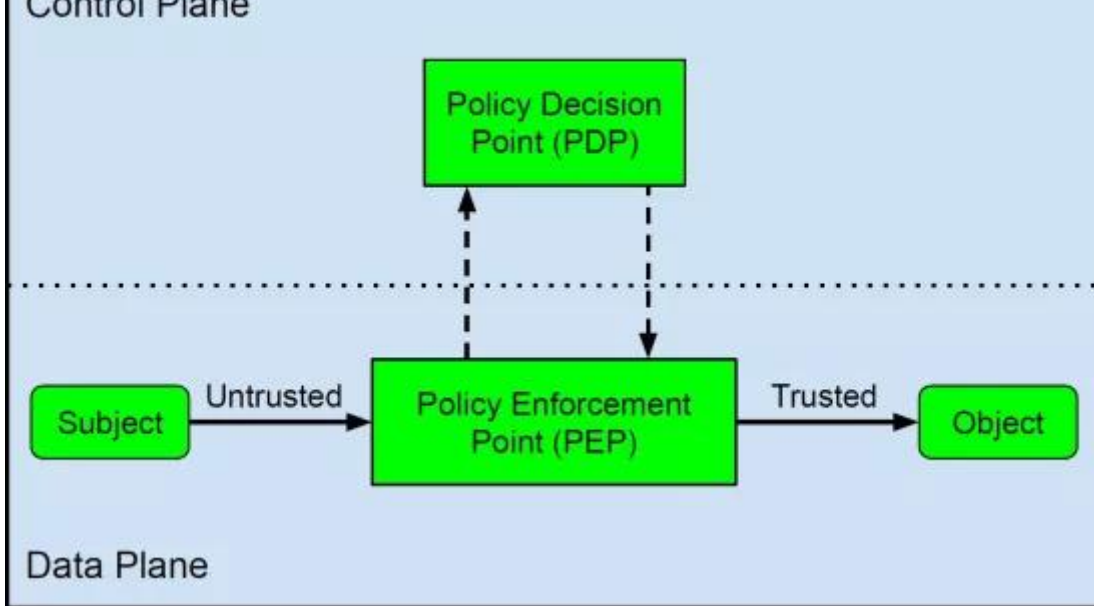
*Uitgaande van het beginsel 'nooit vertrouwen, altijd verifiëren' is Zero Trust een strategische aanpak van cyberbeveiliging die ernaar streeft de digitale veiligheid van een organisatie te handhaven door impliciet vertrouwen te elimineren en elke fase vanaf de creatie van een digitale interactie tot de voltooiing ervan doorlopend te valideren.*

Traditionele beveiligingsarchitecturen voor smart manufacturing maken gebruik van een **op een perimeter gebaseerd beveiligingsmodel** waarbij operators die zich in het interne netwerk bevinden standaard als betrouwbaar worden beschouwd. Bijgevolg kunnen zij toegang hebben tot interne bedrijfsmiddelen. De op een perimeter gebaseerde beveiliging beschermt externe netwerken met een firewall, een inbraakpreventiesysteem (IPS) enz. Gebruikers op externe netwerken moeten bijgevolg worden geauthenticeerd voordat zij kunnen worden vertrouwd. Bovendien wordt een gebruiker, zodra hij is geauthenticeerd, lange tijd vertrouwd en kan hij toegang hebben tot interne bedrijfsmiddelen als hij daartoe gemachtigd is.



In deze aanpak wordt het dus, zodra een concurrent toegang krijgt tot het interne netwerk (bv. door een vertrouwde exploitant/identiteit te compromitteren), gemakkelijk voor hem om op dezelfde manier als legitieme gebruikers toegang te krijgen tot interne middelen. Bovendien kan een concurrent die toegang heeft gekregen tot het interne netwerk zich lateraal door het netwerk bewegen en andere kritieke hosts, servers en infrastructuur compromitteren. VMware-rapport 2022: Laterale beweging werd gezien in 25% van alle aanvallen.

Omgekeerd is **Zero-Trust (ZT)** gebaseerd op het concept van nooit vertrouwen en altijd verifiëren. Zo past ZT dezelfde beveiligingscontrole en toegangscontrole toe op interne en externe gebruikers. ZT beperkt ook interne zijwaartse bewegingen door de gegevensbrug te controleren en elke toegang per sessie te valideren. Het in ZT gebruikte toegangscontrolemodel maakt niet alleen gebruik van statisch beleid, maar ook van dynamisch beleid dat rekening houdt met gebruikers, geraadpleegde bronnen en omgevingskenmerken zoals de locatie waar het verzoek om toegang vandaan komt. **Bovendien is het essentieel om het risico af te stemmen op het niveau van vertrouwen dat wordt toegekend aan een bepaalde gebruiker of een bepaald apparaat dat toegang wil tot specifieke bronnen.** De logische weergave van ZT voor een bedrijfssysteem wordt geïllustreerd in de onderstaande figuur.



## Modellen voor toegangscontrole

Om een ZT-architectuur (ZTA) te ontwerpen, moet goed worden nagedacht over algoritmen voor **identiteitsauthenticatie, toegangscontrole en vertrouwensevaluatie**. In een ZTA is een overzicht vereist van de toegangscontrolemodellen die al dan niet geschikt zijn voor het domein van smart manufacturing. Het is absoluut noodzakelijk te benadrukken dat er toegangscontrole moet zijn voor zowel gebruikers als apparaten. Meer bepaald moet het ZT-systeem toezicht houden op de verschillende apparaten die toegang proberen te krijgen tot het netwerk voor smart manufacturing en ervoor zorgen dat elk apparaat daartoe gemachtigd is.

Smart manufacturing maakt met name gebruik van lokale servers of cloudsysteem om informatie en systeemiteiten (gebruikers, apparaten) op te slaan. Entiteiten hebben toegang tot deze gegevens met een aantal vooraf gedefinieerde toegangscontrolerregels en kunnen specifieke acties uitvoeren (bv. gegevensanalyse, ML, AI). Deze mechanismen maken gebruik van statische toegangscontrolemodellen (d.w.z. eenmaal gedefinieerd - vele malen gebruikt) zoals rolgebaseerde toegangscontrole (RBAC), discretionaire toegangscontrole (DAC) en verplichte toegangscontrole (MAC). Zoals reeds vermeld, is ZT gebaseerd op het uitgangspunt van 'nooit vertrouwen en altijd verifiëren' en moet het gebruikersvertrouwen altijd in verhouding staan tot het risico en dynamisch beleid. Toegangscontrolemodellen die gebaseerd zijn op vooraf gedefinieerde regels voor toegangscontrole zijn dus niet geschikt voor gebruik in ZTA.

Een ander bekend toegangscontrolemodel dat de laatste tijd veel wordt gebruikt, is de **Attribuutgebaseerde Toegangscontrole** (Attribute-Based Access Control, ABAC), een uitstekend alternatief voor RBAC. Met ABAC wordt toegang verleend aan een gebruiker/apparaat als en alleen als hij/het voldoet aan de attributen van het model. Het basis-ABAC-model steunt alleen op vooraf gedefinieerde statische attributen zoals 'identiteit', 'rol' enz. De problemen met dit model zijn (1) dat er geen onmiddellijke verificatie is en (2) dat het mobiele apparaat van de gebruiker alle statische attributen in het apparaat opslaat. Door het volledige potentieel van ABAC te benutten, meer bepaald door gebruik te maken van zowel statische als dynamische attributen die zijn afgeleid van het gebruikersgedrag (bv. 'tijd' en 'locatie'), kan het model nu altijd het gedrag verifiëren om toegang te krijgen. Naast hetgeen hierboven is vermeld, moet het voor ZT gebruikte toegangscontrolemodel rekening houden met de recente geschiedenis van de gebruiker of het

netwerk tijdens de evaluatie van de toegangsverzoeken.

Gezien de dynamische omgeving van smart manufacturing en het feit dat het ZT-systeem onmiddellijke beslissingsmogelijkheden vereist, kan een **risicobewust toegangscontrolemodel** worden gebruikt om toegangsproblemen op te lossen op basis van actierisiconiveaus. Bij de berekening van het risico kunnen vele factoren in aanmerking worden genomen, waaronder contextuele en omgevingsfactoren en de betrouwbaarheid van de/het verzoekend(e) gebruiker/apparaat. In het algemeen bestaat het risicotogangscontrolemodel uit 'risicofactoren', 'risico-inschatting' en een 'toegangscontrolemodule'. De toestemming van de gebruiker, de gevoeligheid van de toegang, de ernst van de actie, de risicogeschiedenis, het gedrag van de gebruiker, de voordelen, de resultaten van de acties en de kenmerken van de context kunnen worden beschouwd als een reeks essentiële risicofactoren in de context van smart manufacturing. Risico-inschattingstechnieken voor risicogebaseerde toegangscontrolemodellen zouden gebaseerd kunnen zijn op fuzzy logic, machinelereen, speltheorie en risicobeoordeling. Het belangrijkste probleem in de context van smart manufacturing is echter het ontbreken van een dataset om de waarschijnlijkheid en de impact van elk risico weer te geven. Door een risicobewust toegangscontrolemodel te integreren met een ABAC-model waarin de risicofactor als attribuut wordt behandeld, kan het worden gebruikt als een praktisch toegangscontrolemodel om ZTA voor te stellen voor smart manufacturing.

## Op weg naar veilige en betrouwbare ZTA

In de loop der tijd is de ZT-architectuur (bijvoorbeeld de ZTA die in 2020 door NIST is voorgesteld) voornamelijk toegepast op bedrijfssystemen (meestal commerciële aanbiedingen). De toepassing van ZT in operationele technologieën (OT), zoals smart manufacturing, bevindt zich echter nog in een vroeg stadium en er zijn nog veel uitdagingen met betrekking tot de beginselen, de architectuur en de implementatie ervan. Sirris-experts met grondige kennis van ZT-modellen en beveiligingsarchitectuur voor smart manufacturing op uiteenlopende gebieden zullen u het leven gemakkelijker maken. Zo kunt u een veilige en betrouwbare ZTA ontwerpen voor uw smart manufacturing.

Meer informatie over ZT-modellen en -praktijken:

- Onze masterclass [Masterclass cyberbeveiliging - Manufacturing | Sirris](#)
- Ons collaboratief kennisopbouw-/verspreidingsproject [Cybersecurity 4.0 | Strategische en gevalsspecifieke cyberbeveiliging - voor Industry 4.0 in kmo's | Sirris](#)

Sirris coördineert momenteel ook verschillende projecten op dit gebied in het kader van **ITEA** van de EU. Meer weten? Neem contact met ons op! Er kunnen nog steeds nieuwe partners worden toegevoegd.

## Auteurs



Farhad Aghili