Cyber Security for IoT

Zero Trust Security Model

Opleiding: Internet of Things

Academiejaar: 2023-24

Naam: Amir HZ

AP HOGESCHOOL ANTWERPEN

AP.BE

1 Executive Summary

Cyber Security for IoT Zero Trust Security Model

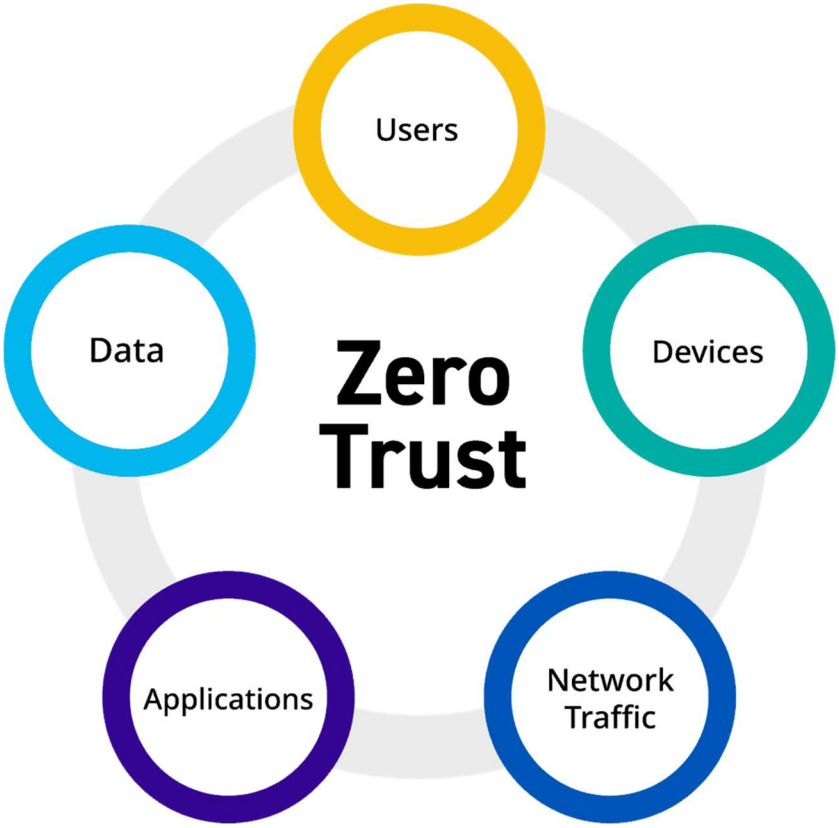
Opleiding: Internet of Things Academiejaar: 2023-24 Naam: Amir HZ

In dit verslag wordt het Zero Trust Security Model besproken, een hedendaags beveiligingsmodel dat essentieel is geworden in de steeds evoluerende wereld van cybersecurity, met een focus op Internet of Things (IoT). Zero Trust stelt dat niemand automatisch wordt vertrouwd, ongeacht hun locatie binnen of buiten het netwerk. Elke toegangspoging tot systemen en gegevens wordt voortdurend gecontroleerd en geverifieerd, waardoor de risico's van cyberaanvallen worden verminderd en gegevens beter worden beschermd.

Het rapport verkent de toepassing van het Zero Trust-model voor gebruikers, waarbij verschillende authenticatiemethoden worden besproken, zoals gebruikersnaam en wachtwoord, multi-factor authenticatie, biometrische identificatie en token-based authenticatie. Daarnaast worden verschillende controlemechanismen onderzocht, waaronder Access Control Lists (ACL), microsegmentatie en Virtual Local Area Networks (VLANs), die gebruikers toegang geven tot specifieke bronnen op basis van hun rol en rechten.

Hoewel Zero Trust belangrijke voordelen biedt voor gebruikers, zoals verhoogde beveiliging, bescherming tegen identiteitsdiefstal en verbeterde bewustwording van beveiliging, zijn er ook enkele nadelen, waaronder mogelijke vertragingen in toegang, toegenomen complexiteit en privacyzorgen.

Het rapport concludeert dat Zero Trust cruciaal is in een tijd waarin cyberdreigingen voortdurend evolueren en organisaties geconfronteerd worden met zowel externe als interne bedreigingen. Door geen enkele gebruiker of apparaat automatisch te vertrouwen en elke toegangspoging strikt te controleren en te valideren, kunnen organisaties de algehele beveiliging verbeteren en zich beter beschermen tegen potentiële aanvallen en inbreuken.



1. Gebruikers: In een Zero Trust-omgeving is het essentieel dat de identiteit van elke gebruiker, ongeacht of het werknemers, zakenpartners of klanten betreft, wordt geauthenticeerd en voortdurend gecontroleerd. Deze term verwijst naar alle individuen die proberen toegang te krijgen tot het netwerk.

2. Apparaten: Apparaten zoals smartphones, tablets, laptops en desktopcomputers worden gebruikt om toegang te krijgen tot het netwerk. Elk van deze apparaten dient geïdentificeerd en beveiligd te worden volgens het beveiligingsbeleid van de organisatie, alvorens toegang te verkrijgen tot het netwerk.

3. Netwerkverkeer: Om ongeautoriseerde toegang en afwijkingen te detecteren, houdt dit proces in dat al het netwerkverkeer wordt gecontroleerd en geïnspecteerd. Door netwerksegmentatie en strikte toegangscontroles toe te passen, wordt gegarandeerd dat gebruikers slechts toegang hebben tot de specifieke netwerkbronnen die voor hen noodzakelijk zijn.

4. Applicaties: Alle software die op het netwerk draait, valt hieronder. Het is van cruciaal belang om applicaties te controleren en te beheren, zodat veilige toegang en transacties kunnen worden gegarandeerd.

5. Data: Deze omvat alle informatie die binnen het netwerk wordt opgeslagen, verwerkt en doorgestuurd. Om ongeautoriseerde toegang en datalekken te voorkomen, is het van essentieel belang om gegevens te classificeren, te versleutelen en te beveiligen.

Wat is zero trust?

Zero Trust is een modern beveiligingsmodel dat ervan uitgaat dat niemand binnen of buiten het netwerk automatisch wordt vertrouwd. Het controleert constant elke toegangspoging tot systemen en gegevens, ongeacht de locatie van de gebruiker. Hierdoor worden de risico's van cyberaanvallen verminderd en worden gegevens beter beschermd.

Zero Trust is zo belangrijk omdat traditionele beveiligingsmodellen vaak falen tegenover geavanceerde cyberdreigingen. Met Zero Trust wordt elke toegangspoging constant geverifieerd, wat helpt om bedreigingen te minimaliseren en gegevens beter te beschermen, vooral in een tijd waarin gegevens overal zijn, van lokale netwerken tot de cloud. Het biedt een adaptieve en proactieve benadering van beveiliging die essentieel is in de moderne digitale wereld.Van Principes tot Praktijk: Verzekeren van End-to-End Security in een Grenzeloze Digitale Wereld

2. Hoe wordt deze toegepast word voor gebruiker en op welke manieren worden de controles uitgevoerd in eenvoudige taal?.

- Authenticatie van Gebruiker :

Deze kan door verschillende methoden van authenticatie

1. Gebruikersnaam en Wachtwoord
2. Multi-factor Authenticatie **(MFA)**: naast een ww een tweede vorm van authrnticatie
3. Biometrische Identificatie: de unieke fysieke kenmerken van een gebruiker gebruiken voor authenticatie.
4. oken-based Authenticatie: softwaretokens die unieke codes genereren die moeten worden ingevoerd om toegang te krijgen tot de generator.

- Bescherming van de gebruiker of de gebruiker, dit kan op verschillende manieren worden gedaan. Hierbij noem ik twee manieren:

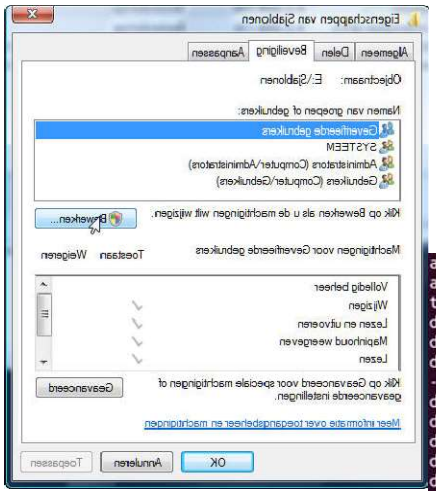
1. Access Control Lists (ACL):

Geef de gebruiker alleen toegang tot data die ze nodig hebben voor de taak die ze mogen uitvoeren.

Gebruikers krijgen enkel toegang naar data dat ze nodig hebben en krijgen specifieke rechten op bepaalde data.(niet elke gebruiker kan op deze manier toegang hebben tot gevoelige data bij lekkage of rechten op verwijzingen of erger dan dat vernietigen hier van)

Hier voor kunnen verschillende tools gebruikt worden zoals:

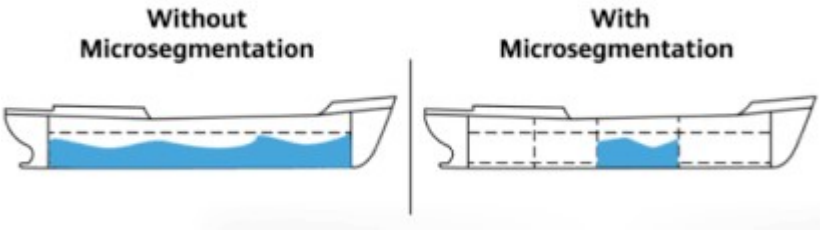
- **Bestands- en mappenrechten**: Besturingssystemen zoals Windows en Linux bieden ingebouwde functionaliteit voor het beheren van bestands- en maprechten. Met deze tools kun je specifieke gebruikers of groepen toegang geven tot bepaalde bestanden of mappen, en de mate van toegang (lezen, schrijven, uitvoeren) bepalen.



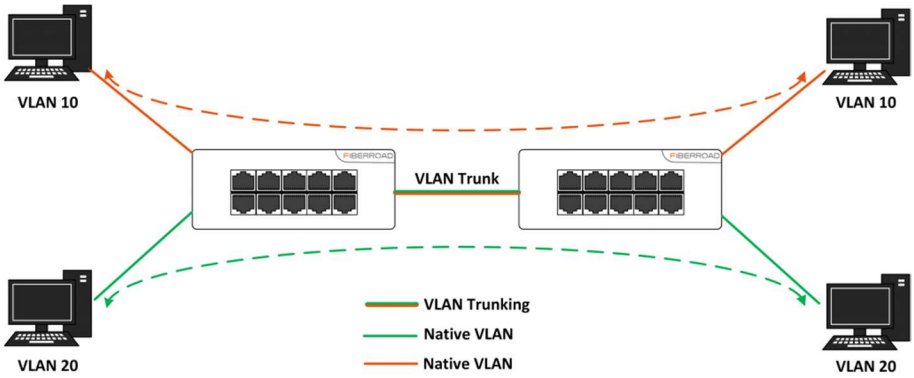
```
administrator@administrator-VirtualBox:~$ cd ~
administrator@administrator-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Desktop
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Documents
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Downloads
-rw-r--r-- 1 administrator administrator  179 2012-09-14 15:24 examples.desktop
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Music
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Pictures
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Public
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Templates
drwxr-xr-x 2 administrator administrator 4096 2012-09-16 09:45 Videos
```

- **Microsegmentatie**

  Microsegmentatie is een netwerkbeveiligingsmethode waarbij het netwerk wordt opgedeeld in kleinere segmenten om de toegang tussen applicaties, services en gebruikers te beperken. Elke segment heeft zijn eigen specifieke beveiligingsregels, waardoor de aanvalsoppervlakte wordt verminderd en de beveiliging wordt verbeterd. Het stelt organisaties in staat om het verkeer binnen het netwerk te controleren op een zeer gedetailleerd niveau, waardoor ze de impact van een eventuele inbreuk kunnen beperken.



2. Netwerkarchitectuur VLANs (Virtual Local Area Networks)



wat een VLAN doet in een netwerk. In plaats van één groot netwerk te hebben waar alle apparaten met elkaar kunnen praten, delen we het netwerk op in verschillende "kamers" of VLANs. Elk VLAN heeft zijn eigen groep apparaten die met elkaar kunnen communiceren, maar niet met apparaten in andere VLANs, tenzij daar specifieke regels voor zijn ingesteld.

Dus, net zoals je alleen toegang hebt tot de kamer waar je moet zijn in een kantoor, hebben apparaten in een VLAN alleen toegang tot de andere apparaten in dezelfde VLAN, waardoor het netwerk veiliger en georganiseerder wordt.

- ## Voordelen van de gebruiker:

Hoewel Zero Trust bepaalde uitdagingen met zich meebrengt voor gebruikers, biedt het ook aanzienlijke voordelen die hun algehele veiligheid en gebruikservaring verbeteren. Hieronder worden enkele van de belangrijkste voordelen voor gebruikers besproken:

3.1.1 Verhoogde Beveiliging Een van de belangrijkste voordelen van Zero Trust voor gebruikers is de verhoogde beveiliging van hun gegevens en accounts. Door strenge verificatie en toegangscontroles worden gebruikersaccounts beschermd tegen ongeautoriseerde toegang en potentiële inbreuken.

3.1.2 Bescherming tegen Identiteitsdiefstal Zero Trust vermindert het risico op identiteitsdiefstal door het gebruik van multi-factor authenticatie (MFA) en continue monitoring van gebruikersactiviteit. Deze maatregelen helpen ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot systemen en gegevens.

3.1.3 Verbeterde Bewustwording van Beveiliging Zero Trust moedigt gebruikers aan om meer bewust te worden van beveiligingskwesties en best practices. Door regelmatig te worden geconfronteerd met verificatie- en toegangscontroles, worden gebruikers aangemoedigd om veilige wachtwoorden te gebruiken, verdachte activiteiten te melden en zich bewust te zijn van potentiële beveiligingsrisico's.

3.1.4 Flexibele Toegang tot Bronnen Hoewel Zero Trust strikte toegangscontroles hanteert, biedt het tegelijkertijd flexibiliteit voor gebruikers om veilig toegang te krijgen tot bronnen vanaf elke locatie en elk apparaat. Door het gebruik van MFA kunnen gebruikers bijvoorbeeld veilig inloggen vanaf externe locaties zonder dat dit ten koste gaat van de beveiliging.

3.1.5 Vermindering van Datalekken Zero Trust helpt het risico op datalekken te verminderen door gebruikers alleen toegang te geven tot de gegevens die ze strikt nodig hebben voor hun taken. Dit minimaliseert de kans dat gevoelige informatie per ongeluk wordt blootgesteld of gecompromitteerd.

3.1.6 Verbeterde Vertrouwelijkheid en Privacy Door continue monitoring van gebruikersactiviteit kan Zero Trust verdachte gedragingen detecteren en snel reageren op mogelijke bedreigingen. Dit draagt bij aan de vertrouwelijkheid en privacy van gebruikersgegevens.

Hoewel Zero Trust bepaalde uitdagingen met zich meebrengt voor gebruikers, biedt het ook aanzienlijke voordelen die hun algehele beveiliging en gebruikservaring verbeteren. Door strengere verificatie en toegangscontroles kunnen gebruikers gerust zijn dat hun gegevens veilig zijn en dat hun accounts beschermd zijn tegen ongeautoriseerde toegang. Bovendien moedigt Zero Trust gebruikers aan om meer bewust te worden van beveiligingskwesties en best practices, waardoor ze een actievere rol kunnen spelen in het beschermen van hun digitale identiteit en gegevens.

- **Nadelen van de gebruiker:**

Hoewel Zero Trust belangrijke voordelen biedt voor de beveiliging, zijn er ook enkele nadelen en uitdagingen die gebruikers kunnen tegenkomen bij het gebruik van dit beveiligingsmodel. Hieronder worden enkele van de belangrijkste nadelen besproken:

3.2.1 Mogelijke Vertragingen in Toegang

Strikte verificatie- en toegangscontroles kunnen leiden tot vertragingen bij het verkrijgen van toegang tot systemen en gegevens. Gebruikers moeten mogelijk meerdere verificatiestappen doorlopen of goedkeuring krijgen van beheerders voordat ze toegang krijgen tot bepaalde bronnen, wat de productiviteit kan verminderen.

3.2.2 Toegenomen Complexiteit

Zero Trust kan leiden tot een toegenomen complexiteit van het beveiligingslandschap, met name voor gebruikers. Het vereist extra verificatiestappen en controles, wat kan resulteren in een minder naadloze gebruikerservaring en mogelijk meer tijd en moeite om toegang te krijgen tot benodigde bronnen.

3.2.3 Mogelijke Privacyzorgen

De voortdurende monitoring van gebruikersactiviteit in een Zero Trust-omgeving kan privacyzorgen veroorzaken bij gebruikers. Ze kunnen zich ongemakkelijk voelen bij het idee dat al hun acties op het netwerk worden gevolgd en geanalyseerd, wat kan leiden tot vertrouwenskwesties.

4 Waarom Zero Trust zo belangrijk

Het basisprincipe van Zero Trust is dat je ervan uitgaat dat hackers zich zowel binnen als buiten het netwerk kunnen bevinden. Dit betekent dat geen enkele gebruiker, machine of apparaat automatisch wordt vertrouwd, ongeacht of ze binnen de fysieke grenzen van het bedrijf opereren of verbinding maken van buitenaf. Door deze aanpak te hanteren, wordt elke toegangspoging beschouwd als een potentiële bedreiging totdat deze grondig is geverifieerd en gevalideerd. Deze denkwijze helpt organisaties om niet alleen bescherming te bieden tegen externe aanvallen, maar ook tegen interne bedreigingen, zoals kwaadwillende insiders of gecompromitteerde accounts. Het betekent dat elke gebruiker en elk apparaat voortdurend gecontroleerd en gevalideerd moet worden, zonder uitzondering. Of het nu gaat om een werknemer die vanaf kantoor werkt, een externe partner die toegang zoekt tot bepaalde bedrijfsapplicaties, of een medewerker die vanuit huis werkt, niemand krijgt zomaar toegang zonder eerst te worden gecontroleerd en goedgekeurd.