Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe organiseer ik identiteit en toegang?

Aan de slag met authenticeren en het voorkomen van ongeautoriseerde toegang

Identiteit en toegang | versie 1.0 | oktober 2024

Inleiding

Het beveiligen van een netwerk met maatregelen als het doen van updates en het installeren van virusscanners, firewalls en het inrichten van monitoring, detectie en response helpen om inzicht te verkrijgen en kwaadwillende actoren buiten te houden. Personen of systemen zullen altijd toegang tot het netwerk en applicaties nodig hebben om bedrijfsprocessen uit te voeren. Een belangrijk uitgangspunt is echter dat de gebruiker of het systeem enkel toegang krijgt tot de specifieke delen van het netwerk en informatiesystemen die hiervoor noodzakelijk zijn. Identiteits- en toegangsbeheer is dan ook een essentiële maatregel, evenals fysieke toegangsbeveiliging.

In deze factsheet licht het NCSC toe wat het belang van identiteits- en toegangsbeheer is. En welke eerste stappen je kunt zetten om dit beheer in te richten om effectief grip te krijgen op je gebruikers en hun toegang.

Deze publicatie maakt onderdeel uit van een publicatiereeks en biedt praktische handvatten voor het uitvoeren van een risicoanalyse in het kader van de NIS2-richtlijn. De handvatten in deze publicatie zijn geschreven om te voldoen aan de NIS2-richtlijn maar kunnen ook in bredere context gebruikt worden.

Achtergrond

Het doel van identiteits- en toegangsbeheer is het zo klein mogelijk maken van het risico op toegang van ongeautoriseerden tot het netwerk of gegevens. Dit risico kan van buitenaf komen, maar ook van binnenuit (insider threat). Vergeet daarbij niet het risico van ongeautoriseerde fysieke toegang. Bepalen wie of wat toegang krijgt tot welke netwerk en informatiesystemen, objecten en bijbehorende gegevens is een voorwaarde voor een beheerste fysieke en logische toegangsbeveiliging. Een goede toepassing van identiteits- en toegangsbeheer maakt het voor aanvallers moeilijker om zich voor te doen als legitieme gebruikers.

NIS2 en de Cyberbeveiligingswet

Artikel 21, lid 1 van de NIS2-richtlijn en art. 23 Cyberbeveiligingswet verplicht entiteiten passende en evenredige technische, operationele en organisatorische maatregelen te nemen.

In het kader van deze regelgeving valt identiteits- en toegangsbeheer onder het nemen van maatregen tegen ongeautoriseerde toegang.

Doelgroep

Deze publicatie richt zich op organisaties die onder de NIS2-richtlijn vallen en is geschreven voor personen die binnen deze organisaties een rol hebben bij het uitvoeren van een risicoanalyse in het kader van de zorgplicht. Daarnaast biedt het andere organisaties inzicht in het organiseren van identiteits- en toegangsbeheer.

Wat is identiteits- en toegangsbeheer?

Identiteits- en toegangsbeheer (Engels: identity and access management; IAM) is het bepalen wie en wat toegang heeft tot de systemen en gegevens van jouw organisatie. Identiteits- en toegangsbeheer verwijst naar de verzameling van beleid, processen en systemen die ondersteuning bieden voor het kunnen koppelen van een persoon (of in sommige gevallen een systeem) aan een gebruikersaccount en een adequate set machtigingen voor toegang binnen je netwerk- en informatiesysteem.

Met deze machtigingen kan de persoon bijvoorbeeld het volgende doen:

- Uitvoeren van functies
- Gegevens raadplegen en aanpassen
- Systemen beheren

Een organisatie moet de juiste methoden kiezen om de identiteit van gebruikers, apparaten of systemen vast te stellen. Met deze identiteit kan de organisatie bewijzen, met voldoende vertrouwen, aan wie toegang verleend kan worden.

Wat is identiteitsbeheer?

Identiteitsbeleid bestaat uit de onderdelen identificatie en authenticatie.

- **Identificatie**:
  - Beleid om te borgen dat een nieuwe gebruiker is wie hij/zij zegt dat hij/zij is.
  - Registreren van de functies, rollen en eventuele screeningniveaus die horen bij deze persoon.
- **Authenticatie**:
  - Beleid betreffende het koppelen van een geïdentificeerde gebruiker aan een identiteit/profiel binnen de systemen met een passende authenticatiemethode
  - Ervoor zorgen dat de authenticatiemethode jou voldoende vertrouwen geeft dat wanneer een identiteit wordt gebruikt, deze wordt gebruikt door de persoon van wie de identiteit eerder is gevalideerd.

Wat is toegangsbeheer?

- **Autorisatie**
  - Beleid dat de functie/rol van de medewerker koppelt aan een bepaalde mate van toegang tot het netwerk- en informatiesysteem.
  - Toepassen van de juiste toegangsmaatregelen op basis van het toegangsbeleid.

Voorbeeldscenario

Bij de indiensttreding van een nieuwe medewerker wordt er op basis van de fysieke identiteit van de persoon een digitale identiteit/gebruikersaccount aangemaakt. Hierbij gebruik je bijvoorbeeld een identiteitsbewijs als basis.

Vervolgens kan de gebruiker toegang worden verleend tot de bij deze account behorende gegevens en systemen. Dit gebeurt door middel van het koppelen van de juiste toegangsrechten aan het account.

Vervolgens dient de gebruiker zichzelf bij het inloggen op het gebruiksaccount te authenticeren om aan te tonen wie hij is.

Risico's bij het authenticeren ontstaan wanneer anderen (kwaadwillenden) toegang kunnen hebben tot authenticatiegegevens.
Wanneer enkel gebruik gemaakt wordt van iets dat je weet, zoals een wachtwoord, kan een kwaadwillende deze informatie eenvoudiger misbruiken. Aanvallers kunnen wachtwoorden buit maken bij datalekken van andere systemen indien de gelekte wachtwoorden elders worden herbruikt.

Door de toepassing van MFA (multifactorauthenticatie) wordt de kans kleiner dat een kwaadwillende toegang heeft tot de volledige set aan authenticatiegegevens. Door toepassing van *least privilege* en *need-to-know* wordt de toegang van gebruikers beperkt tot de hoogst noodzakelijke. Hiermee kan de impact van compromitatie van een gebruikersaccount worden beperkt.

Stappenplan identiteits- en toegangsbeheer

Met behulp van onderstaand stappenplan maak je een start met het inrichten of verbeteren van identiteits- en toegangsbeheer. Maak daarbij een keuze om het identiteits- en toegangsbeheer in eigen beheer in te richten, het gehele proces uit te besteden of een combinatie hiervan.

Stap 1: Inventariseer het landschap waar je identiteits-en toegangsbeheer voor wilt inrichten.

Inventariseer de architectuur, netwerkinfrastructuur en applicaties in de organisatie. Dit zijn niet alleen applicaties die gebruikt worden door werknemers maar ook applicaties die door systeemgebruikers benaderd kunnen worden. Denk hierbij dus ook aan interfaces tussen systemen.

Deze holistische kijk is belangrijk voor het begrijpen van de beveiligingsbehoeften van elke applicatie en netwerkonderdelen.

Stap 2: Ontwikkel identiteits- en toegangsbeleid

Om identiteits- en toegangsbeheer goed toe te passen is de eerdergenoemde beleidsontwikkeling essentieel. In vele normen en standaarden wordt dit als randvoorwaarde genoemd om goede keuzes te maken waarop je je identiteits-en toegangsbeheer kan inrichten. Dit beleid bevat de uitgangspunten en regels voor toegang tot systemen, apparatuur, faciliteiten en informatie. Raadpleeg hiervoor de BIO of de ISO-standaard. Zie bijvoorbeeld ook het kennisproduct van de Informatiebeveiligingsdienst '*Beleid logische toegangsbeveiliging*'.

Bepaal welk beleid wordt toegepast voor identificatie, authenticatie en autorisatie.

- Identificatie gaat over het vaststellen van de identiteit van een mogelijke gebruiker. Beleid dat hierbij van belang is:
  - De identiteit vaststellen door middel van een identiteitsbewijs.
  - Het screenen van de medewerker, dit is afhankelijk van het risicoprofiel. Het nagaan van referenties kan hier ook een onderdeel van zijn.
  - Het bepalen van het *need to know* niveau, afhankelijk van de rol en functie.
- Authenticatiebeleid
  Authenticatie gaat over het verifiërenvan de juistheid van de opgegeven identiteit met het gebruikersaccount. Belangrijk is in beleid vast te leggen wannneer welke wijze van authenticatie moet worden toegepast. Deze authenticatie kan op verschillende wijzen plaatsvinden, voorheen was dat vaak door middel van invoeren van een pincode of wachtwoord, maar tegenwoordig is *multi-factor authenication* (MFA) een standaardmaatregel. Deze bestaat uit een combinatie van meerdere authenticatie-elementen. Hiermee bewijst een gebruiker de authentieke persoon te zijn die toegangsrechten heeft. Dit kan door middel van:
  - Iets wat je weet; bijvoorbeeld een wachtwoord of pincode.
  - Iets wat je hebt: een cryptografisch identificatie-apparaat, telefoon (met authenticatie-app) of token
  - Iets wat je bent: biometrische. gegevens (vinger/hand/irisscan).
- Kies voor MFA waar dat kan. Gebruik eventueel een risicoanalyse om te bepalen waar dit noodzakelijk en mogelijk is.
  Indien gebruik wordt gemaakt van wachtwoorden, implementeer dan een sterk wachtwoordenbeleid.
  Leg vast in het beleid hoe authenticatiegegevens bewaard worden.

- Beschrijf wat het autorisatiebeleid is. Denk eraan de volgende onderwerpen te behandelen:
  - **Gebruikersbeheer**: het proces voor het aanvragen, wijzigen en verwijderen van gebruikers.
  - **Toegangsbeheer**: het proces voor het aanvragen, goedkeuren, wijzigen en verwijderen van autorisaties. De proces- en/of data-eigenaar zijn hier verantwoordelijk voor.
    Toegangsbeheer kan op basis van verschillende methodieken, waaronder de vaak gebruikte Role-Based Access control, gebaseerd

op de functie en rol van de medewerker. Daarbij kun je ook kiezen om uitsluitend via verstrekte endpoints (werklaptop) of uitsluitend vanuit een bepaalde geografische zone en tussen bepaalde tijdstippen toegang te verlenen.

- **Functiescheiding**: functiescheiding moet je inrichten zodat afzonderlijke functionarissen zijn aangewezen die autorisaties aanvragen/toekennen, wijzigen, intrekken en/of verwijderen en controleren.

Houd in het beleid rekening met de in-, door- en uitstroom van medewerkers. Dit beleid ziet toe op het toevoegen van accounts voor nieuwe medewerkers, het verwijderen van accounts en het voorkomen van stapeling van autorisaties door wisselende functies.

Leg in het beleid vast hoe logging helpt om autorisatie-aanpassingen te monitoren. Dit om ongeautoriseerde wijzigingen, zoals *privilege escalation* te kunnen waarnemen. Met name voor geprivilegieerde toegang, zoals beheerder-accounts dienen toegangsaanpassingen goed gemonitord te worden.

Zero Trust

Zero trust gaat uit van de basisgedachte "never trust, always verify". Zero trust kan toegepast worden op externe gebruikers, bring-your-own-device (BYOD) en cloudgebaseerde activa die zich niet binnen een bedrijfseigen netwerkgrens bevinden. Zero Trust vereenvoudigt gedetailleerde conditionele gebruikerstoegangscontrole. Zie verder Factsheet Bereid u voor op Zero Trust | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl) en What about zero trust? | Expertblogs | Nationaal Cyber Security Centrum (ncsc.nl)

Stap 3: Identificeer welke gegevens of systemen het meest kritiek zijn voor de organisatie

De meest kritieke gegevens of systemen worden ook wel je *te beschermen belangen* (TBB) of *kroonjuwelen* genoemd. Het NCSC biedt in het kennisproduct '*Hoe breng ik mijn te beschermen belangen in kaart*?' een handreiking voor deze inventarisatie.

Breid de hierin genoemde referentietabel uit met een extra kolom waarin je opneemt in welke applicaties en netwerkonderdelen de TBB's voorkomen.

Stap 4: Bepaal welke methode je gaat gebruiken bij het inrichten van identiteits- en toegangsbeheer

Vervolgens is het belangrijk te starten met het ontwerpen van toegangsbeheer voor de applicaties en systemen die al eerder in je risicomanagementproces zijn geïdentificeerd als kroonjuwelen.

Maak hierbij gebruik van een autorisatiematrix voor iedere applicatie of netwerkonderdeel. Hiermee bepaal je welke rollen/gebruikers of groepen toegang zouden moeten krijgen tot welke bronnen, wanneer die gebruikers toegang nodig hebben en welke mate van toegang ze krijgen. Een gebruiker kun je toewijzen aan een of meerdere rollen of groepen om dit proces efficiënt beheersbaar te maken.

Veelgebruikte principes voor het bepalen van de mate van toegang zijn:

- Least privilege[1]
  Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van informatiesystemen en/of gegevens Toegangsrechten worden voor iedere gebruiker tot een minimum beperkt. Deze worden uitsluitend verleend in de mate dat deze nodig zijn voor het uitvoeren van iemands taken.
- Need-to-know
  De toegang van een gebruiker tot informatie wordt beperkt of uitgebreid op basis van de informatiebehoefte die volgt uit de actuele werkzaamheden van de gebruiker.

[1] *Least Privilege Principe*: Het principe waarbij een security architectuur zo ontworpen is dat een entiteit de minimale systeemtoegang en resources krijgt die noodzakelijk zijn voor de uitvoering van de functie.

Stap 5: Implementeer, beheer en borg identiteits- en toegangsbeheer

Het doel van identiteits- en toegangsbeheer is het voorkomen van toegang door ongeautoriseerden. Bij het nemen van de maatregelen is het doel om uitsluitend de juiste bevoegde personen conform de autorisatiematrix of ander ontwerp uit Stap 4 toegang te verlenen tot infrastructuur, applicaties en gegevens van de organisatie op basis van het vastgestelde beleid. Zorg dat dit beleid correct wordt geïmplementeerd, beheerd en regelmatig geëvalueerd.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

oktober 2024