

Richtlijnen voor verbindingen en toegang

Infrastructuur

Datum

17-02-2021

Versie

1.4

Auteur

Chris Karreman

E. van Leiden

Algemeen

Toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze informatiesystemen. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform ontsloten en beschikbaar gesteld wordt. Alle gebruikers van gemeentelijke informatiesystemen dienen, volgens toegangsbeveiligingprocedures, geautoriseerd te worden.

In dit document worden beleidsregels omtrent verbindingaanvragen vastgelegd. Het biedt tevens aanwijzingen over het inrichten van toegangsbeveiliging voor leveranciers die beheerwerkzaamheden moeten kunnen uitvoeren binnen het domein van Syntrophos. De remote access eisen worden opgesteld aan de hand van architectuuruitgangspunten en security best practices. Daarnaast wordt in dit document vastgelegd welke verbidings- en encryptieprotocollen worden toegestaan.

De eisen in dit beleid zijn gebaseerd op eisen uit de BIG en heeft raakvlakken met de onderstaande componenten:

- Dataclassificatie (classificatie van bedrijfsmiddelen en informatie);
- Geheimhoudingsverklaringen;
- ICT-beheer (oplevering, acceptatie en overdracht van (delen van) systemen,

beheerorganisatie en beheerprocessen);

- Informatiebeveiligingsbeleid van de gemeenten;
- Logging (controle, auditing en monitoring);
- Telewerken;
- Toegangsbeleid;
- Wachtwoordbeleid.

Risico's

Door het ontbreken van adequate logische toegangsbeveiliging bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot gemeentelijke informatiesystemen waardoor ongewenste acties op de diensten kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt. Onduidelijke of niet gevolgde toegangsbeveiligingprocedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van gemeentelijke informatie, maar uiteindelijk ook slecht voor het imago van de gemeente.

Uitgangspunten

Bij het ontwerpen en implementeren van toegang worden de volgende uitgangspunten gehanteerd:

- De systeemeigenaar overlegt met de betrokken gegevenseigenaren en proceseigenaren over de vraag wie geautoriseerd wordt en op welke manier dat gebeurt;
- De systeemeigenaar en/of de leverancier geeft duidelijk aan wat er nodig is om heheerwerkzaamheden uit te kunnen voeren;
- Er is een 'verzoek tot autorisatie' proces ingericht en gevolgd;
- Intern verkeer mag niet versleuteld zijn. Syntrophos moet te allen tijde en proactief, intern verkeer kunnen scannen op malware, virussen, etc. Feitelijk betekent dit dat het verkeer van encryptie wordt voorzien en wordt gedetermineerd op de edge firewall;
- Extern verkeer wordt versleuteld;
- Een Site 2 site VPN wordt alleen ingericht wanneer er geen enkele mogelijkheid bestaat om cliënt VPN te gebruiken. Met andere woorden cliënt vpn's hebben de voorkeur;
- Indien van toepassing dient met elke leverancier vooraf een bewerkersovereenkomst te worden getekend;
- Zonder een getekende verklaring Remote support leverancier en/of de verklaring remote support FAB wordt geen toegang verleend;

- Medewerkers van leveranciers worden op gebruikersniveau geauthenticeerd en geautoriseerd. Leveranciers brengen periodiek Syntrophos (min. 1x per kwartaal) op de hoogte of de opgevoerde medewerkers nog werkzaam zijn;
- Multifactor authenticatie is de norm;
- Port forwarding is niet toegestaan;
- Het encryptieniveau is minimaal 256-bits en encryptieprotocollen zijn ondubbelzinnig veilig;
- Er wordt alleen gebruik gemaakt van VPN-functies en VPN-cliëntsoftware die worden ondersteund door de edge firewall;
- Beperken ongeautoriseerde installatie van software door de gebruiker, waardoor alleen door Syntrophos goedgekeurde beheertoepassingen mogelijk zijn;
- Bestaande verbindingen worden aangepast naar dit nieuwe beleid;
- Onbeheerde systemen worden eerst gescand op vulnerabilities voordat ze worden toegelaten op ons netwerk (network access control policies);
- Er wordt maar één connectie per medewerker toegestaan. Connecties worden na een periode van inactiviteit automatisch verbroken.

Virtual Private Networks

Met een VPN-verbinding wordt beveiligd toegang tot het netwerk van Syntrophos gerealiseerd. Hiermee wordt de koppeling, gelegd via internet, veiliger. VPN's worden ingericht met een combinatie van specifieke verbindings- en encryptieprotocollen.

Grofweg zijn er twee typen VPN smaken waarvan gebruik gemaakt kan worden:

- Cliënt VPN, binnen dit scenario wordt VPN-software geïnstalleerd op de cliënts waarmee de verbinding tot de edge firewall tot stand wordt gebracht;
- Site 2 Site VPN, binnen dit scenario worden twee netwerken aan elkaar gekoppeld. In dit geval het netwerk van de leverancier en het netwerk van Syntrophos.

Het gebruik van beide scenario's wordt toegestaan. De voorkeur gaat echter uit naar cliënt VPN's. De reden hiervoor is driedelig. Ten eerste, is multi-factor authenticatie alleen mogelijk met cliënt-VPN's. Ten tweede, cliënt-VPN's maken gebruik van een authenticatie server en kunnen in combinatie met een Network Protection Server bepalen dat onveilige cliënts geen toegang krijgen d.m.v. uitgave health certificates. Ten derde, de overlapping in subnetten. In het geval van site 2 site VPN's worden netwerken gekoppeld waarbij extern overlapping in subnetten mogelijk zijn. Om dit te voorkomen worden zo veel mogelijk cliënt-VPN's gebruikt. Wanneer leveranciers overlappende subnetten hebben of er is een overlapping met een subnet van Syntrophos dan is Syntrophos hierin leidend.

Toegestane verbindings- en encryptieprotocollen

Verbindingen met het Syntrophos domein worden alleen toegestaan onder de onderstaande voorwaarden: Gebruik de protocollen die door de Nationaal Cyber Security Centrum als "Goed" wordt beoordeeld. Meer informatie hierover kunt u vinden op:

<https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging>

<https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

Het bijbehorende document vindt u:

<https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1/ICT-beveiligingsrichtlijnen+voor+Transport+Layer+Security+v2.1.pdf>