# Leeruitkomst 3: Security Engineer

Luc van den Acker

Cyber Security Semester 4

Contents

[Leeruitkomst 3: Security Engineer 1](#_Toc124949029)

[Protect the Network 2](#_Toc124949030)

[Network Seperation and Segmentation with Firewalls 2](#_Toc124949031)

[Firewall Rules 3](#_Toc124949032)

[Secure Network Connections(HTTPS/TLS/SSH) 4](#_Toc124949033)

[HTTPS 4](#_Toc124949034)

[TLS 4](#_Toc124949035)

[SSH 4](#_Toc124949036)

[VPN Setup 5](#_Toc124949037)

[Identity & Access Management 6](#_Toc124949038)

[IT System Hardening 8](#_Toc124949039)

# Protect the Network

Information security policies zetten eisen voor de beschikbaarheid, integriteit en de betrouwbaarheid van data. Om de risico´s op datalekken en dergelijken te verminderen, worden zakelijke netwerken opgedeeld in gesegmenteerde netwerken. Ook wordt verkeer dat het netwerk uit gaat gefilterd, om onveilig verkeer zoveel mogelijk af te houden.

### Network Seperation and Segmentation with Firewalls

Een gesegmenteerd netwerk is altijd veiliger dan een netwerk dat niet gesegmenteerd is. Hieronder staat beschreven hoe een gesegmenteerd netwerk opgezet is. Het netwerk bestaat uit drie segmenten:

* VLAN-A met subnet 172.16.0.0/24. Apparaten op dit subnet kunnen verbinding maken met vanaf het internet beschikbare systemen. Een subnet als dit wordt vaak de ‘DMZ Zone’ genoemd(demilitarized zone).
* VLAN-B met subnet 172.16.1.0/24. Dit subnet is voor de kantooromgeving en Active Directory(AD). Een subnet als dit wordt vaak de ‘Management Zone’ genoemd.
* VLAN-C met subnet 172.16.2.0/24 voor monitoring en eventueel beheer. Een subnet als dit wordt vaak de ‘LAN Zone’ genoemd.

Diagram

Description automatically generatedDe onderstaande afbeelding laat zien hoe het hierboven beschreven netwerk eruit komt te zien. Helemaal links, in het rode vak, is een apparaat te zien dat van buitenaf verbinding maakt met de router via een VPN. Wanneer er geen VPN-verbinding opgezet is vanaf de thuiswerkplek, is het niet mogelijk om de eerste router(R1) te benaderen, en dus is het onmogelijk om de services op het netwerk te benaderen. R1 zorgt ervoor dat het netwerk verbonden is met het internet. Vervolgens is er een switch(S1) aangesloten. Onder S1 valt het eerste subnet, de DMZ Zone. Dit netwerk is dus te benaderen vanaf het internet. Hierop wordt een webserver en een NextCloud server gehost. In het witte vak aan de rechterkant zien we de LAN Zone. Binnen dit subnet vinden we de AD/file server en een werkstation. Omdat op beide hosts natuurlijk vrij gevoelige data kan staan, hoort deze afgeschermd te zijn van de buitenwereld. Daarom zit het afgesloten achter een tweede router(R2). R2 zorgt ervoor dat er geen verkeer toegestaan is vanaf de andere subnetten, of van buitenaf, naar de LAN zone toe. R2 zet ook nog een laatste subnet op, namelijk VLAN-C. Op VLAN-B(groen vak) wordt enkel een Monitoring Server aangesloten. Deze server heeft toegang tot alle subnetten, zodat het gehele systeem vanaf een veilige omgeving gemonitord kan worden.

Door het segmenteren van het netwerk zijn de kwetsbaarheden beperkt. Wanneer een aanvaller toegang weet te krijgen tot het VLAN-A subnet, heeft hij echt alleen toegang tot dat subnet, en niet tot de andere subnetten. Ook wordt de hack geregistreerd door de monitoring server, waardoor de beheerder van het netwerk bewust is van de hack en actie kan ondernemen.

## Firewall Rules

Een firewall is een service die inkomend en uitgaand netwerkverkeer bewaakt en bepaalt welk verkeer wel of niet toegestaan wordt. Op basis van ingestelde firewall rules wordt bepaald wat er wel en niet toegestaan wordt. Het gesegmenteerde netwerk dat in hoofdstuk 6 beschreven staat, kan uiteraard ook wat firewall rules gebruiken. Hieronder staat, in een tabel welke regels ingesteld dienen te worden, met een korte beschrijving waarom de specifieke regels relevant zijn.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Router 1 |  |  |  |  |  |  |
| Source | Destination | Protocol | Poort | Applicatie | Allow/Deny | Verklaring |
| DMZ-subnet | LAN | TCP | 10051 | Zabbix Client | Allow | Monitoring van webserver |
| Buitenaf | DMZ | TCP | 443 | HTTPS | Allow | Benaderen webserver van buitenaf |
| Thuiswerkstation | LAN | TCP | 22 | SSH | Allow | Vanuit huis werken mogelijk maken |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Router 2 |  |  |  |  |  |  |
| Source | Destination | Protocol | Poort | Applicatie | Allow/Deny | Verklaring |
| LAN-subnet | \* | TCP | 80 | HTTP | Deny | HTTP is onveilig |
| LAN-subnet | \* | TCP | 443 | HTTPS | Allow | Veilig internetten |
| LAN-subnet | \* | TCP | 22 | SSH | Allow | Secure remote acces werknemersportaal |
| LAN-subnet | \* | UDP | 53 | DNS | Allow | Voor time-sensitive transmissies |
| LAN-subnet | \* | ICMP | nvt | Ping | Allow | Testen of een host nog wel online is |
| MON-subnet | LAN | TCP | 10051 | Zabbix Client | Allow | Netwerk monitoring vanaf werk-PC |
| DMZ-subnet | LAN | TCP | 389 | LDAP | Allow | LDAP moet gegeven uit AD-server halen |

## Secure Network Connections(HTTPS/TLS/SSH)

Een goede verbinding is natuurlijk veilig. Om deze veiligheid te waarborgen zijn verschillende protocollen beschikbaar. Hieronder staan een aantal beschreven:

### HTTPS

Jaren geleden gebruikten wij allemaal HTTP voor ons webverkeer. HTTP(HyperText Transfer Protocol) is een protocol dat gebruikers de mogelijkheid geeft om te communiceren over het internet. Nagenoeg iedere URL begint met “http://” of “https://”. Deze protocollen worden dus enorm veel gebruikt, maar wat is het verschil tussen HTTP en HTTPS? Zowel HTTP als HTTPS zorgt ervoor dat een gebruiker data kan versturen en ontvangen op het internet. HTTP doet echter letterlijk dat, het opsturen en ontvangen van data, terwijl HTTPS het internetverkeer versleutelt. Een HTTP verbinding is dus een onveilige verbinding, omdat al het verkeer door iedereen die toevallig aan het luisteren is te lezen is. HTTPS daarentegen, versleutelt al het verkeer dus, en enkel de ontvanger en de verzender hebben de benodigde sleutel om het verkeer te ontsleutelen, waardoor het een stuk lastiger is om het verkeer af te lezen.

### TLS

TLS, oftewel Transport Security Layer, is een encryptie-protocol dat de communicatie tussen computers beveiligt. TLS maakt gebruik van asymmetrische encryptie om de identiteit van beide partijen te bevestigen. Vervolgens wordt de communicatie tussen beide partijen versleuteld door middel van symmetrische encryptie. TLS wordt dus voornamelijk gebruikt om de identiteit van een benaderde server te bevestigen.

### SSH

SSH staat voor Secure Shell, en wordt vooral gebruikt voor ‘remote login en command line’. SSH biedt dus de mogelijkheid om van afstand veilig een verbinding te kunnen maken met een SSH server. Er wordt gebruik gemaakt van Public Key-cryptografie, waarbij iedereen met een public key een bericht kan versleutelen, maar enkel degene die de bijbehorende private key hebben, kunnen het bericht weer ontsleutelen.

## VPN Setup

Om veilig te kunnen werken op het internet staat hieronder een beschrijving over het opzetten van een VPN via een PFSense router en OpenVPN:

Certificate Authority

Allereerst dient een “Certificate Authority aangemaakt te worden. Hiermee wordt de identiteit van de server gevalideerd. Ook is het mogelijk om met deze CA gebruikerscertificaten te valideren als dit nodig is. OpenVPN biedt een aantal opties voor de lengte van de key en het type key. Hierbij geldt natuurlijk dat een langere key, met complexere encryptie veiliger is. Vervolgens moet ingesteld worden hoe lang het certificaat geldig blijft. In dit geval hoeft dit niet heel lang te zijn, aangezien deze VPN niet langdurig gebruikt zal gaan worden.

Server Certificate

Een server certificate is een SSL-certificaat dat ervoor zorgt dat een host een naam krijgt. Deze naam kan een machine-naam zijn(bijv. XYZ-SERVER-01), of een domein naam, zoals [www.nu.nl](http://www.nu.nl). Als een client vervolgens een request verstuurt, wordt het certificaat van de server gecontroleerd om te achterhalen of de webserver wel legitiem is. Daarnaast verzorgt het certificaat een veilige verbinding met de client via Public Key Infrastructure(PKI).

Users en User Certificate

Het is natuurlijk niet de bedoeling dat de VPN voor iedereen toegankelijk is. Daarom worden een aantal gebruikers aangemaakt. Enkel deze gebruikers kunnen verbinding maken met de server. Hoe ziet de server nou wie er wel mag verbinden en wie niet? Aan de hand van een User Certificate. Dit certificaat wordt, net zoals een Server Certificate, gebruikt om de veiligheid van een gebruiker te waarborgen. Op basis hiervan wordt gevalideerd of de gebruiker legitiem is.

OpenVPN Server

Natuurlijk zal er een server opgezet moeten worden waarop de VPN gedraaid wordt. Clients kunnen een verbinding opzetten met deze server. Dit zorgt ervoor dat het internetverkeer van de client naar de server versleuteld is.

OpenVPN Firewall Rules

Om de VPN naar eigen wens in te stellen, is het mogelijk om bepaalde regels in te stellen, namelijk firewall rules. Met deze regels wordt gedefinieerd wat er wel en niet toegelaten wordt op de server. Zo wordt in dit geval een regel aangemaakt waarin gespecificeerd staat dat IPv4 gebruikt wordt, en IPv6 niet toegestaan is. Ook is het mogelijk om bijvoorbeeld in te stellen welk protocol gebruikt wordt. Ook is er de mogelijkheid om het IP-adres van de server en het subnet te specificeren. Er zijn enorm veel mogelijkheden qua regels. Hiermee hebben gebruikers aardig wat grip op wat ze wel of niet op hun netwerk willen hebben.

# Identity & Access Management

Identity & Access Management(IAM) gaat over het voeren van een beleid waarbij de juiste gebruikers de juiste rechten en toegangen hebben tot specifieke IT-resources met behulp van authenticatie en autorisatie. Authenticatie is een proces waarbij gecontroleerd wordt of een gebruiker daadwerkelijk is wie hij beweert te zijn. Autorisatie is het verlenen van toestemming aan een geauthentiseerde gebruiker om toegang te krijgen tot een bepaalde dienst. IAM bestaat uit een aantal verschillende onderdelen:

Registratie betreft het plaatsen van de juiste identiteitsinformatie van bronsysteem naar doelsysteem. Binnen een bedrijf kan dit op verschillende manieren aangepakt worden. Zo kunnen bijvoorbeeld gegevens van een HRM systeem naar een Active Directory worden gezet. Vanaf deze centrale directory is het eenvoudig om accountgegevens te koppelen aan andere services binnen een organisatie, zoals mailservers, portalen of HR systemen.

Autorisatie is dus het toekennen van de rechten om gebruik te mogen maken van een bepaalde dienst. Het autorisatieproces is enorm belangrijk binnen IAM, aangezien het bepaalt welke gebruikers wel of geen toegang hebben tot een dienst. Zo is het bijvoorbeeld belangrijk dat werknemers in het portal van het bedrijf kunnen, en er dus rechten toegekend moeten worden voor alle werknemers om gebruik te maken van deze dienst. Echter is het niet de bedoeling dat alle werknemers toegang krijgen tot bijvoorbeeld een management portaal.

Om te weten of iemand wel echt is wie hij zegt te zijn, wordt gebruik gemaakt van authenticatie. Tijdens het authenticatieproces wordt gebruik gemaakt van authentication credentials. Dit kunnen wachtwoorden zijn, maar ook asymmetrische of symmetrische encryptie, biometrische scans, of nog een hoop andere vormen. Om de veiligheid van een systeem te vergroten, is het aan te raden om meerdere credentials te combineren. Een extra slot op de deur is natuurlijk lastiger te kraken. Wat deze authentication credentials precies zijn en hoe ze werken wordt hieronder beschreven.

**Wachtwoorden**

Wachtwoorden worden nagenoeg altijd gebruikt als menselijke interactie vereist is voor authenticatie, zoals bij het inloggen op een mailserver. Vaak wordt gebruik gemaakt van statische wachtwoorden. Statische wachtwoorden veranderen nauwelijks, wat voor kwetsbaarheden zorgt. Uiteraard is het enorm praktisch voor gebruikers om altijd hetzelfde wachtwoord te gebruiken, aangezien het makkelijk te onthouden is. Echter zijn statische wachtwoorden relatief eenvoudig te achterhalen, omdat ze niet vaak veranderen en een hacker dus uitgebreid de tijd heeft om het te kraken.

Als een wachtwoord constant verandert, is er minder tijd om deze te achterhalen. Daarom zijn one-time passwords, oftewel OTP, moeilijker te achterhalen. Een OTP is een wachtwoord dat bij elk gebruik wijzigt. Doordat het wachtwoord snel verandert, wordt het een stuk lastiger om ongeautoriseerd toegang te krijgen tot vertrouwelijke digitale bronnen, zoals gebruikersaccounts. OTP wordt bijvoorbeeld gebruikt door de meeste Nederlandse banken. Zij maken gebruik van een kaartlezer(bijvoorbeeld een Rabo-scanner) die, samen met een bankpas, ter plekke een OTP genereert. Met dit OTP wordt vervolgens toegang tot een bankaccount verstrekt.

**Asymmetrische en symmetrische cryptografie**

Symmetrische encryptie is een vorm van cryptografie waarbij zowel voor het versleutelen als het ontsleutelen van een bericht dezelfde sleutel gebruikt wordt. Omdat de ontvanger dezelfde sleutel moet gebruiken om het bericht te ontsleutelen als de sleutel waarmee de verzender het bericht versleuteld heeft, ontstaat een probleem. Hoe komt de sleutel veilig van verzender tot aan ontvanger? Deze zal via het internet verstuurd moeten worden naar de ontvanger, waardoor de kans aanwezig is dat een derde partij de sleutel kan onderscheppen, en dus al het verkeer tussen ontvanger en verzender af kan lezen.

Om dit probleem op te lossen, wordt gebruik gemaakt van asymmetrische encryptie. Bij asymmetrische cryptografie wordt gebruik gemaakt van twee verschillende sleutels. De ene sleutel versleutelt het te versturen bericht, terwijl de andere sleutel, de private key van de ontvanger van het bericht, het bericht weer kan ontsleutelen. Deze private key is dus de sleutel om berichten te ontsleutelen, en is enkel voor de ontvanger bekend. Niemand anders mag weten wat de private key van de ontvanger is. Als iemand bijvoorbeeld de sleutel van je brievenbus heeft, kan die persoon al je post lezen. Een populaire methode om asymmetrische encryptie toe te passen is het RSA-algoritme. Dit algoritme genereert verwante private en public keys, maar het is niet mogelijk om de private key te herleiden op basis van de public key.

Om asymmetrische encryptie toe te passen, moeten allereerst public keys uitgewisseld worden. Vervolgens gebruikt de verzender de public key van de ontvanger om het te verzenden bericht te versleutelen. Het verzonden bericht is enkel te ontsleutelen met de private key van de ontvanger. Zelfs de verzender kan dus het bericht niet meer ontsleutelen nadat het verstuurd is. Asymmetrische encryptie wordt bijvoorbeeld gebruikt door HTTPS websites en crypto wallets.

# IT System Hardening

System hardening is het proces van het zo moeilijk mogelijk maken om ongeautoriseerd toegang te krijgen tot een systeem door zoveel mogelijk veiligheidsrisico’s te elimineren. Door het aantal aanvalsvectoren te verkleinen, wordt gestreefd naar een veiligere applicatie. Om het aantal aanvalsvectoren te verminderen, is aan te raden om een systeem zo klein en compact mogelijk te houden. Dit houdt in dat overbodige functionaliteiten verwijderd dienen te worden. Hieronder staan een aantal potentiële aanvalsvectoren beschreven. Ook wordt beschreven hoe deze(gedeeltelijk) af te dekken zijn.

* **Default passwords.** Met geautomatiseerde password crackers zijn veel simpele wachtwoorden relatief snel te achterhalen. Wanneer een malafide gebruiker een wachtwoord achterhaalt, is de integriteit van het systeem in gevaar. Om dit te voorkomen, worden strengere eisen gesteld aan een wachtwoord. Zo moet een wachtwoord bijvoorbeeld minsten x aantal karakters bevatten, waarvan minstens één hoofdletter, één nummer en één ander teken. Zelfs met deze complexe wachtwoorden is het mogelijk om de wachtwoorden te kraken, het duurt alleen enorm lang.
* **Hardcoded passwords en andere credentials opgeslagen in plain text files.** Wanneer wachtwoorden en andere credentials in plain text, oftewel niet-versleuteld opgeslagen staan in een database, ontstaat er natuurlijk een enorm risico. Als iemand toegang tot de database weet te krijgen, liggen alle credentials van je systeem op straat, en zijn dus al je gebruikersaccount onveilig. Ook wachtwoorden en dergelijken in code zijn een risico. Wanneer bijvoorbeeld het wachtwoord van de database in de code te vinden is, en in de database alle wachtwoorden in plain text staan, is het heel eenvoudig om gevoelige data te achterhalen, want inbreken is niet moeilijk als de deur openstaat. Om dit te voorkomen, is aan te raden om alle credentials, overal in een systeem versleuteld op te slaan. Daarnaast is het aan te raden om zo min mogelijk wachtwoorden op te slaan buiten de centrale directory. Als een wachtwoord op meerdere plekken te vinden is, wordt de kans natuurlijk groter dat deze gevonden wordt.
* **Kwetsbaarheden door verouderde software.** Zorg er altijd voor dat alle services binnen je netwerk up-to-date zijn. Door middel van een update kunnen kwetsbaarheden gemitigeerd worden. Desondanks worden niet alle kwetsbaarheden verholpen met patches en updates. Bijvoorbeeld zero day kwetsbaarheden zullen niet gelijk gepacht kunnen worden.
* **Gebrek aan privileged acces control.** Wanneer acces control niet goed opgezet is, bestaat de kans dat gebruikers toegang hebben tot data of services die helemaal niet voor deze gebruiker bedoeld zijn. Een goede manier om met acces control om te gaan is “principle of least privilege”. Dit houdt in dat iedere gebruiker in principe geen enkel recht heeft, afgezien van eventuele publieke resources die voor iedereen toegankelijk zouden moeten zijn. Wanneer een gebruiker dan toch toegang moet krijgen tot bepaalde services of resources, kan alsnog toegang verleend worden. Op deze manier wordt voorkomen dat overbodige rechten toegekend worden.
* **Niet-versleuteld netwerkverkeer.** Als al het verkeer binnen je netwerk niet versleuteld is, geef je malafide gebruikers de mogelijkheid om alles af te lezen. Om dit te voorkomen, is het aan te raden om netwerkverkeer te versleutelen met behulp van een VPN. Een VPN, oftewel virtual private network, verbergt je daadwerkelijke IP-adres en versleutelt al het internetverkeer. Hierdoor is het een stuk lastiger om verkeer af te luisteren.