NEDU
Nederlandse Energie Data Uitwisseling

Issue TC029 Beveiliging SFTP informatieoverdracht

Status	ter vaststelling ALV		
Versienummer	2.0	**Versiedatum**	13 december 2017
Documentnaam	TC029 Beveiliging SFTP informatieoverdracht v2.0		

Behandeld door de Technische Commissie

Raakt aan	Kleinverbruik	Grootverbruik	Wholesale
Elektriciteit	**X**	**X**	**X**
Gas	**X**	**X**	**X**

Impact op keten	Ja/Nee
Codewijziging	**Nee**
Berichten	**Nee**
Ketenprocessen	**Nee**

Mogelijke impact marktrollen en EDSN	Ja/Nee
LV	**Ja**
PV	**Ja**
MV	**Ja**
RNB	**Ja**
LNB	**Ja**
EDSN	**Ja**

V2.0 Vastgesteld door NEDU op 13 december 2017 Invoering in markt per direct	Contact	
	Technische Commissie	

Management samenvatting

De meeste informatie uitwisseling in de ketenprocessen gebeurt in het 'berichtenverkeer' via webservices, AS2, AS4 of CPS (AS1), waar beveiliging is geregeld middels beveiligingscertificaten (zie o.a.TC027). Daarnaast wordt voor het uitwisselen van grote datasets in de sector onder andere gebruik gemaakt van het zogenaamde Secure File Transfer Protocol (SFTP, op basis van SSH verbindingen), waarvoor de nodige beveiligingsrisico's bestaan, niet zozeer in de verbinding als wel op de omgeving die met de verbinding is verbonden. Verder blijkt dat het beveiligingsbeheer voor de SSH verbindingen bij veel organisaties zwak is ingericht. Het beleid in de sector zou er opgericht moeten zijn het gebruik van SFTP/SSH zo veel mogelijk te voorkomen. Als we het wel moeten/willen gebruiken dan dient er scherp bij elke partij op te worden toegezien dat de verbonden omgevingen goed worden beveiligd en dichtgezet en het SSH keybeheer goed is geregeld. Dit issue geeft een aantal richtlijnen voor de inrichting van de SFTP verbindingen.

Situatieschets:

Er zijn in de sector voor informatie overdracht van grote datasets verschillende kanalen in gebruik, waar onder het FTP protocol. Op dit moment wordt Secure File Transfer Protocol (SFTP) op basis van SSHv2 (Secure Shell (kortweg: SSH) een goed te beveiligen protocol voor verbindingen) voor bestandsuitwisseling tussen marktpartijen voor zowel het Portaal (Uitwisselen grote datasets) als TMR ingezet. De authenticatiewijze voor marktpartijen om toegang te verkrijgen op de SFTP servers verschilt per server.
Ter verduidelijking van de beschikbare authenticatie methoden worden in de bijlage de protocollen (SFTP en SSHv2) beschreven. Vervolgens wordt in de bijlage kort de huidige implementatie van de SFTP servers in het NEDU domein behandeld.
Er zijn tot op heden geen richtlijnen hoe het landschap, waar de SSH verbinding binnenkomt/uit gaat, zo veilig mogelijk in te richten.

Vraag:

Kunnen we richtlijnen afspreken in de sector voor een betere beveiliging van de informatieoverdracht via SFTP?

Aanbevelingen

1. Het gebruik van SSH zou beveiligingstechnisch gezien zoveel mogelijk moeten worden beperkt en in ieder geval dient men het sleutelbeheer en de kwetsbaarheden van alle betrokken verbindingen in de keten goed te laten bewaken.

2. Daarnaast is het goed om een aantal richtlijnen in acht te nemen aan de kant van de marktpartijen, die dit gebruiken voor uitwisselen van datasets. Het gevaar is niet zozeer de dataoverdracht maar schuilt meer in de onvoldoende afscherming van de eigen omgevingen, waardoor via de SSH ingang makkelijk ongeoorloofde toegang tot data en systemen in het achterland is te verkrijgen. Goede richtlijnen hiervoor worden met enige regelmaat door het Amerikaanse NIST (National Institute of Standards and Technology) gepubliceerd, zie bijvoorbeeld **http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf**

3. Een complete lijst van mogelijke cipher suites voor SSH is te vinden op http://www.iana.org/assignments/ ssh-parameters/ssh-parameters.xml. Voor gebruik van veilige cipher suites in het opzetten van veilige SSH verbindingen wordt verwezen naar de lijst met cipher suites, die worden toegestaan (of anders afgeraden/verboden) voor de TLS verbindingen in de sector. De Technische Commissie en Security Commissie van de NEDU geven hier bijna jaarlijks nieuwe richtlijnen voor uit.

4. IP white listing is een goede manier om als eerste filter veel ongewenst verkeer af te vangen.

5. De data overdracht dient te worden beveiligd met een voldoende veilig certificaat. Omdat het SSH protocol geen controle tegen betrouwbare uitgevers doet is het inzetten van dure certificaten niet nodig en zal ieder zelf een validatie slag op de gebruikte certificaten moeten doen. Het protocol kijkt aan de 'overkant' van de lijn of er een publieke sleutel is te gebruiken. De certificaten zijn dan ook niet geschikt te gebruiken voor authenticatie.

6. Op het met de SSH connectie verbonden interne landschap dient voldoende zware hardening te worden toegepast:
   - Alleen file access verlenen en geen shell acces om te voorkomen dat van buiten eenvoudig commando's kunnen worden uitgevoerd en daardoor ongewenste toegang tot data wordt verkregen;
   - Het (externe) account, dat toegang is verleend, moet zoveel mogelijk worden 'dicht getimmerd', zoals het onmogelijk maken van tunneling;
   - De gebruiksmogelijkheden dienen strikt beperkt te worden tot hetgeen nodig is voor de overdracht van de datasets in een zeer beperkte omgeving (jailing).

Oplossing:

Partijen implementeren zo snel mogelijk de aanbevelingen, waaronder periodieke kwetsbaarheden scans.

Impact:

De SFTP/SSH omgeving is een statische configuratie die makkelijk is te controleren tegen deze aanbevelingen.

Invoeringsstrategie:

Elke partij gaat de bestaande SFTP omgevingen zo snel mogelijk controleren en aanscherpen conform de aanbevelingen.

Te vervallen issues:

Geen.

Versieoverzicht:

0.1 eerste aanzet door Gerrit Fokkema na bespreking in de TC op 2 oktober 2015;
0.2 na bespreking in de TC van 13 november 2015;
0.3 na akkoord in de TC van 18 december 2015;
0.4 na bespreking in de TC (van 5 februari 2016) van de reactie op het issue van de Security Commissie;
0.5 na bespreking in de TC (van 22 juli 2016) samen met vertegenwoordiging van de SC;
0.6 na finale bespreking in de TC van 6 januari 2017;
1.0 na vaststelling in de ALV van 18 januari 2017;
1.1 aanpassingen n.a.v. reacties, verwijzing naar NIST opgenomen en benoeming cipher suites verwijderd op 20 oktober 2017;
1.2 na bespreking en goedkeuring in de TC vergadering van 17 november 2017;
1.3 na review door de Sectorplanningscommissie op 30 november 2017.
2.0 na vaststelling in de ALV van 13 december 2017

Bijlage

Protocollen

SFTP

SFTP is een van de functionaliteiten van SSHv2. SSHv2 ondersteunt een FTP-achtig beveiligd bestandsuitwisseling systeem dat SFTP wordt genoemd.

[bron: https://www.enisa.europa.eu/activities/cert/support/chiht/tools/ssh-secure-shell]

SFTP dient niet verward te worden met FTPS. FTPS is een extensie van het FTP protocol voor beveiligde bestandsuitwisseling met behulp van SSL / TLS. FTPS maakt in tegenstelling tot SFTP gebruik van een TLS / SSL verbinding, middels de TLS/SSL verbinding wordt de FTP verbinding beveiligd voor het uitwisselen van bestanden. FTPS maakt voor de TLS/SSL en FTP verbindingen gebruik van verschillende poorten. Dit maakt implementatie van FTPS complex in combinatie met firewalls.

SSHv2

SSHv2 is een communicatie protocol dat zorgt voor veilige toegang tot een server, bestandsuitwisseling en TCP/IP verbinding in een niet-vertrouwd netwerk. SSHv2 ondersteunt cryptografische authenticatie van client en server, automatische sessie encryptie en integriteitsbeveiliging voor bestandsuitwisseling. In SSHv2 worden vijf afzonderlijke en opvolgende fasen onderscheiden die zorgdragen voor het opzetten van een SSH sessie:

1. Fase 1: Versie onderhandeling
   Server en client onderhandelen over de te gebruiken SSH versie (informatie wordt verzonden in platte tekst).
2. Fase 2: Sleutel en algoritme onderhandeling
   Server en client versturen lijsten met beschikbare sleutel, encryptie, MAC en compressie algoritmes. Server en client kiezen de te gebruiken algoritmes. Server en client gebruiken het Diffie-Hellman sleuteluitwisselingsalgoritme en parameters (zoals publieke host sleutel) voor het genereren van de sessie sleutel.
   De server en client hebben nu dezelfde sessie sleutel die gebruikt wordt voor het opzetten van:
   - beveiligd SSH kanaal;
   - betrouwbaarheid van het kanaal;
   - bescherming van integriteit en server authenticatie;
   - het versleutelen van de uit te wisselen data.
3. Fase 3: Authenticatie
   Na het opzetten van het SSH kanaal kan de client authenticatie plaatsvinden.
   De client authenticatie kan op meerdere manieren uitgevoerd worden:
   - Wachtwoord uitwisseling;
   - Publieke sleutel uitwisseling met challenge-response model (optioneel gebruikmakend van DSA en RSA algoritmes, X.509 PKI-standaard)
   - "interactief-toetsenbord" challenge/response methode (voor meerdere authenticatie challenges);

- GSSAPI (Generic Security Service Application Program Interface), een interface voor authenticatie protocols zoals Kerberos

4. Fase 4: Sessie aanvraag
   Na authenticatie vraagt de client een sessie aan bij de server. Indien de server de client heeft geauthentiseerd wordt een success - bericht naar de client gestuurd en wordt de interactieve fase gestart.
5. Fase 5: Interactieve sessie
   In deze fase kan de versleutelde data in het SSH kanaal tussen server en client data worden uitgewisseld.

Huidige inrichting van de beschikbare SFTP servers voor de marktpartijen

De marktpartijen kunnen met behulp van de SFTP servers van het Portaal en TMR bestanden uitwisselen met de CMF systemen of met elkaar.

Vanuit de documentatie van beide servers (Servicebeschrijving SFTP v1.1 en TM-Dienstbeschrijving_v1.0) kan vastgesteld worden dat de beide SFTP servers volgens het juiste SSH protocol, SFTP met SSHv2, zorgdragen voor de bestandsuitwisseling. Tevens kan worden geconcludeerd dat de authenticatiewijze voor de client (SSHv2 – fase 3) deels afwijkend van elkaar is.

Implementatie in Portaal

Een marktpartij kan gebruik maken van de SFTP functionaliteit door:

- Het aanleveren van een ip-adres voor whitelisting op de firewall;
- Gebruik te maken van het door EDSN beschikbaar gestelde SFTP account;
- Tevens is het mogelijk om middels een decentraal gegenereerde sleutelpaar o.b.v. RSA (4096 bits) middels de publieke sleutel toegang te krijgen op de SFTP server, indien deze bij de SFTP server bekend is en de private sleutel in bezit is van de marktpartij.

Implementatie in TMR

Een marktpartij kan gebruik maken van de SFTP functionaliteit door:

- Het aanleveren van een ip-adres voor whitelisting op de firewall;
- Decentraal genereren van een sleutelpaar (publieke en private sleutel) o.b.v. RSA (4096 bits) en de private sleutel additioneel te beveiligen met een “pass phrase”
- De publieke sleutel beschikbaar te stellen aan EDSN beheer voor creatie van een SFTP account;
- Indien account is aangemaakt kan het sleutelpaar gebruikt worden voor toegang tot de server de encryptie tijdens data overdracht.