Programma RDO

Ministerie van Volksgezondheid, Welzijn en Sport

Standard Operating Procedures – Adhoc Secure File Transfer –

RDO, MinVWS

– 1.02– 18 juni 2021–

Document geschiedenis

Versie	Datum	Veranderingen
1.00	2020-12-31	Eerste concept - voor interne discussie en verificatie.
1.01	2021-01-02	Finale versie - voor productie.
1.02	2021-06-18	Made more generic for CIMS/RIVM/GGD-GHOR project

Hoofdstuk 1

Context

Tijdens outages of andere onvoorziene events kan het nodig zijn om AdHoc bestanden uit te wisselen welke gevoelige informatie bevatten. En waarbij er niet de tijd is dit te doen via een bestaande koppeling.

Dit document beschrijft de aanbevolen procedures voor dit soort noodgevallen alsmede de te gebruiken tools en technieken.

Hiernaast is onverkort, en voor het overige, het vigerende beveilingsbeleid en de Baseline Informatiebeveiliging Overheid (BIO) van de rijksoverheid van toepassing.

Ontwerp uitgangspunten en afwegingen

Deze standard operating procedure is bedoeld voor de uitzonderingen - éénmalige uitwisselingen waarbij er geen tijd is voor de bouw van een koppeling of het inrichten van een PKI. Daarom is deze procedure bewust simpel gehouden (enkel ZIP), maakt zij gebruik van processen (borging, 4-ogen principe), is zij zo min mogelijk digitaal (geen opslag password, password in persoon of per telefoon communiceren) en zo veel mogelijk éénmalig (wachtwoord maar één keer gebruiken; alle bestanden na overdracht wissen).

Uitwerking

Waar mogelijk is het process als hieronder beschreven. Eventuele afwijkingen dienen achteraf gedocumenteerd te worden in een kort document dat gedeeld wordt met alle betrokken partijen.

Borging Deze stappen zullen waar mogelijk voorzien worden van een ops-ticket nummer of andere interne tracking en borging.

Inpakken De stappen zullen uitgevoerd worden door twee personen (4-ogen principe):

- De te versturen bestanden zullen in één directory gezet worden.
- Deze directory zal ingepakt worden met ZIP (file format versie 5.2 of nieuwer) gebruikmakend van AES-256 encryptie.
- Er zal een sterk wachtwoord (Zie handreiking Wachtwoorden, BIO[1]; meer dan 20 cijfers en letters of meer dan 8 indien de regels van 'complex' gevolgd worden).
- Dit wachtwoord is éénmalig (emphemoral) en wordt niet digitaal opgeslagen (e.g. in een email, Notepad, etc).

overdracht Het ZIP bestand kan uitgewisseld worden via een onveilig kanaal. Hierbij heeft een intern kanaal de voorkeur, gevolgd door een kanaal via een beperkt toegankelijke file server waar mogelijk.

Dit wachtwoord wordt via een ander kanaal, niet digitaal, gecommuniceerd. Bijvoorbeeld in persoon of per telefoon.

Ontvangen De stappen zullen uitgevoerd worden door twee personen (4-ogen principe).

- Ontvangende partij stelt het versleutelde bestand direct veilig.
- Controleert of het bestand versleuteld is.
- Decodeert het bestand in een veilige omgeving

Na ontvangst, veiligstellen informeer de ontvangende partij de verzendende partij zo snel mogelijk.

Afronding *Beide* partijen nemen dan, waar nodig, actie om alle versies van het ZIP bestand te wissen.

Beide partijen zorgen voor eigen vastlegging en delen die. Eventuele afwijkingen worden gedocumenteerd.

Aanbevolen versies ZIP

Aanbevolen versies van ZIP zijn elke versie van WinZIP en PKZIP van na 2004 (het menu 'Conversion Settings' toont de default geselecteerde 256-bits AES). Voor Linux, *BSD en MacOSX zijn alle versie van '7za' of 'PkZip' afdoende.

Voor MacOSX is de meegeleverde 'zip' (command line utility) met de flaggen '-er' vanaf MacOSX 10.2 voldoende indien de procedure van `https://www.canr.msu.edu/news/encrypted-zip-mac` gebruikt wordt.

[1] `https://www.informatiebeveiligingsdienst.nl/product/wachtwoordbeleid-2/`