Communicatiescenario's Justitiële ICT Organisatie intern

Door de Justitële ICT Organisatie is de afgelopen periode afstemming met alle opdrachtgevers geweest om mogelijke scenario's naar aanleiding van de problematie met de netscalers te bespreken.

In dit document brengen we de scenario's voor JIO zelf in kaart.

We onderkennen de volgende scenario's

1. Er zijn geen aanwijzingen dat aanvallers voorbij het voorportaal zijn gekomen
2. Er wordt wel een aanwijzing gevonden dat aanvallers voorbij het voorportaal zijn gekomen
    a. Het inkomende internetverkeer richting de Connect dienst wordt beperkt
    b. Het inkomende internetverkeer richting de Connect dienst wordt volledig afgesloten
    c. Uitgaand internetverkeer wordt beperkt
    d. Uitgaand internet wordt volledig afgesloten
    e. Volledige quarantaine

    Hierin zijn ook combinaties mogelijk

    In onderstaande uitwerking is sec gekeken naar de impact als we alléén de betreffende optie uitvoeren. Bij combinaties, moeten de diverse boodschappen samengevoegd worden.

Communicatievragen per scenario:

- Wat is er aan de hand, algemeen?
- Waarom maken we deze keuze en waarom nu?
- Wat is de impact?
    - Welke diensten zijn wel/niet beschikbaar?
    - Wat kunnen mensen nog wel/niet?
    - Wat betekent dit voor je werk?
    - Wat wordt er van jou verwacht?
- Welke maatregelen nemen we nu?
- Hoe lang gaat dit duren?
- Waar terecht voor meer informatie?

---

1. **Er zijn geen aanwijzingen dat aanvallers voorbij het voorportaal zijn gekomen**
   We zetten de communicatie op de huidige wijze voort."

2. **Er wordt wel een aanwijzing gevonden dat aanvallers voorbij het voorportaal zijn gekomen**

   a. **Het inkomende internetverkeer richting de Connect dienst wordt beperkt**

   Wat doen we: Specifieke IP-adressen worden toegestaan, de Connect dienst is beperkt bereikbaar, alleen via deze toegestane IP-adressen 5.1.2h 5.1.2h
   De rest wordt afgesloten. Zowel productieomgeving als acceptatieomgeving.

   Impact algemeen
   - Impact op inloggen op Connect! omgeving
   - Thuiswerken niet mogelijk
     - Webex en 5.1.2h (mail via tablet, telefoon) wel beschikbaar
   - Je kunt alleen werken op kantoor, via een thin client of Govroam en je mobiele device
     - Dit kan ook een rijkskantoor of rijkshub zijn
     - Alle diensten zijn op deze locaties gewoon beschikbaar

Doelgroep –	Impact	Wijze van communicatie + wie	Boodschap
Medewerkers		Leidinggevenden: • Afdelingshoofden bellen - • Teamleiders bellen – afdelingshoofden • Mail naar alle LG's • Mail en intranetbericht – • Bellen/signal (m.n. medewerkers op vakantie) – LG's	Specifiek: • Bij gebrek aan ruimte op kantoor: o Afstemmen wie wanneer op kantoor (LG's) o Eerst beheerteams, kritieke functies o Verdeling over JIO-locaties • Géén bestanden naar jezelf mailen, blijf werken in de beveiligde omgeving. Veilig gedrag benadrukken • *Let zelf ook op verdacht verkeer, verdacht gedrag (gebruikers verdacht, gekke bestanden) – optioneel, kan ook doorslaan* • Contactpunt medewerkers is eigen LG

Voor JIO wordt qua werkplekken het volgende voorgesteld:
Medewerkers met standplaats Gouda gaan naar kantoor Gouda met als uitwijk de Rijkshub in Leiden
Medewerkers met standplaats Soesterberg gaan naar kantoor Soesterberg met als uitwijk Rijkskantoor Herman Gorter in Utrecht;
Medewerkers met standplaats Veenhuizen gaan naar kantoor Veenhuizen met als uitwijk Rijkskantoor Assen.

b. Het inkomende internetverkeer richting de Connect dienst wordt volledig afgesloten

Wat doen we: Volledig afgesloten, de dienst Connect! is volledig onbereikbaar. Zowel productieomgeving als acceptatieomgeving.

Impact algemeen

- Impact op inloggen op Connect! omgeving
- Thuiswerken niet mogelijk
  - Webex en 5.1.2h (mail via tablet, telefoon) wel beschikbaar
- Je kunt alleen werken op kantoor, via een thin client
  - Alle diensten zijn op deze locaties gewoon beschikbaar
  - Niet via Govroam (dus Rijkskantoor/rijkshub kan niet)

  - Alle diensten zijn op deze locaties gewoon beschikbaar

Doelgroep –	Impact	Wijze van communicatie + wie	Boodschap
Medewerkers		Leidinggevenden: • Afdelingshoofden bellen - • Teamleiders bellen - afdelingshoofden • Mail naar alle LG's • Mail en intranetbericht – • Bellen/signal (m.n. medewerkers op vakantie) – LG's	Specifiek: • Bij gebrek aan ruimte op kantoor: o Afstemmen wie wanneer op kantoor (LG's) o Eerst beheerteams, kritieke functies o Verdeling over JIO-locaties • Géén bestanden naar jezelf mailen, blijf werken in de beveiligde omgeving. Veilig gedrag benadrukken • *Let zelf ook op verdacht verkeer, verdacht gedrag (gebruikers verdacht, gekke bestanden) – optioneel, kan ook doorslaan* • Contactpunt medewerkers is eigen LG

Voor JIO wordt qua werkplekken het volgende voorgesteld:
Medewerkers met standplaats Gouda gaan naar kantoor Gouda met als uitwijk de Rijkshub in Leiden
Medewerkers met standplaats Soesterberg gaan naar kantoor Soesterberg met als uitwijk Rijkskantoor Herman Gorter in Utrecht;
Medewerkers met standplaats Veenhuizen gaan naar kantoor Veenhuizen met als uitwijk Rijkskantoor Assen.

c. Uitgaand internetverkeer wordt beperkt

Wat doen we: het internetverkeer wordt standaard geblokkeerd, alleen opgegeven domeinen/FQDN's zullen toegestaan zijn. Bij het aanpassen van de proxy naar alleen toestaan van bekende en vertrouwde resources verwachten wij dat de diensten blijven functioneren.

Impact algemeen

Waarschijnlijk in combinatie met A of B. In onderstaande uitwerking is sec gekeken naar de impact als we alléén de betreffende optie uitvoeren. Bij combinaties, moeten de diverse boodschappen samengevoegd worden.

- Impact op beschikbaarheid diensten/applicaties
  Primaire applicaties van JIO worden niet getroffen omdat deze on premis draaien.
  Het gaat hierbij om de volgende applicaties?
  -
  - 5.1.2h 5.1.2h
  - 5.1.2h
  -

  Secundaire applicaties die internet nodig hebben, kunnen niet worden gebruikt
  Dit betekent voor JIO dat de 5.1.2h applicatie moet worden gewhitelist of dat deze niet gebruikt kan worden.

Medewerkers		Leidinggevenden: • Afdelingshoofden bellen - directieleden • Teamleiders bellen - afdelingshoofden • Mail naar alle LG's Medewerkers: • Mail en intranetbericht – 5.1.2e • Bellen/signal (m.n. medewerkers op vakantie) – LG's	Antwoord geven op communicatievragen p.1 Specifiek: • Welke systemen zijn niet meer beschikbaar? • Wat betekent dit voor je werk (bijv. indien geen P-Direkt, dan kun je ook geen nieuwe mdw aanmaken) • Géén bestanden naar jezelf mailen, blijf werken in de beveiligde omgeving. Veilig gedrag benadrukken • *Let zelf ook op verdacht verkeer, verdacht gedrag (gebruikers verdacht, gekke bestanden) – optioneel, kan ook doorslaan* • Contactpunt medewerkers is eigen LG

d. Uitgaand internet wordt volledig afgesloten

Wat doen we: het internetverkeer wordt geblokkeerd. Diensten die gebruik maken van resources op internet, kunnen niet worden gebruikt.

Waarschijnlijk in combinatie met A of B. In onderstaande uitwerking is sec gekeken naar de impact als we alléén de betreffende optie uitvoeren. Bij combinaties, moeten de diverse boodschappen samengevoegd worden.

- Impact op beschikbaarheid diensten/applicaties
- Alle applicaties die internet nodig hebben, kunnen niet worden gebruikt
    - Primaire (kritieke) systemen die internet nodig hebben ook niet beschikbaar (geen whitelisting)
    - Let op: sommige on premise diensten hebben toch een verbinding naar buiten, en zijn dan niet beschikbaar.

Medewerkers		Leidinggevenden: • Afdelingshoofden bellen - directieleden • Teamleiders bellen - afdelingshoofden • Mail naar alle LG's Medewerkers: • Mail en intranetbericht – 5.1.2e • Bellen/signal (m.n. medewerkers op vakantie) – LG's	Antwoord geven op communicatievragen p.1 Specifiek: • Welke systemen zijn niet meer beschikbaar? • Wat betekent dit voor je werk (bijv. indien geen P-Direkt, dan kun je ook geen nieuwe mdw aanmaken) • Géén bestanden naar jezelf mailen, blijf werken in de beveiligde omgeving. Veilig gedrag benadrukken • *Let zelf ook op verdacht verkeer, verdacht gedrag (gebruikers verdacht, gekke bestanden) – optioneel, kan ook doorslaan* • Contactpunt medewerkers is eigen LG

e. Volledige quarantaine

Als onderzoek uitwijst dat de DWO gecompromitteerd is, dan is niet uit te sluiten dat een aanvaller nog aanwezig is en via JustitieNet mogelijk ook naar andere organisaties (in JustitieNet termen: sectoren) kan proberen door te dringen. Om te zorgen dat een compromitatie niet als een cascade van de ene naar de andere omgeving kan uitbreiden is er in JustiteNet daarvoor een quarantaine dienst.
Het is mogelijk om in de quarantainedienst specifieke verkeersstromen uit te zonderen (die kunnen dan dus wel doorlopen).