Betreft: Reactie op Internetconsultatie Conceptvoorstel Wet Beveiliging Netwerk- en Informatiesystemen

Namens het DIVD CSIRT hebben we de voorgenomen wijziging aan de WBNI doorgenomen. In de kern vinden wij het een goede zaak dat er nu wetgeving in de maak is die het NCSC (het Nationaal Cyber Security Centrum) in staat stelt informatie breder te delen dan nu het geval is.ge beperkingen waaronder het NCSC veel informatie niet mag delen komt de cyberveiligheid in Nederland niet ten goede.

De wetswijziging beoogt het NCSC meer vrijheid te geven m.b.t. twee soorten informatie:

a. “vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder” (Artikel 20 lid 2)
b. “verkregen gegevens over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen dan bedoeld in de aanhef van het eerste lid” (Artikel 3 lid 2)

Ad a. We vinden het een goede zaak dat het NCSC deze informatie ook mag gaan verstrekken aan OKTTs. Deze wijziging komt de cyberweerbaarheid te goede, zonder dat zij extra administratie of versnippering tot gevolgen heeft.

Ad b.
Hoewel wij het in de basis ook een goede zaak vinden dat het NCSC in staat wordt gesteld partijen rechtstreeks te benaderen, denk wij dat de bewoording van lid 2, te veel restricties en randvoorwaarden oplegt:

1. Ten eerste moet er sprake zijn van “het voorkomen van nadelige maatschappelijke gevolgen in en buiten Nederland”. Dit is een behoorlijk hoge drempel.
2. Lid 2e heeft het over aanbieders. Niet iedere partij in Nederland kan gezien worden als een “aanbieder”. Is een producent van auto’s een ”aanbieder” zoals bedoelt in deze tekst?
3. Lid 2e stelt als voorwaarde voor het informeren van een “aanbieder” dat: “een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening”. Is het NCSC in staat een accurate inschatting van de impact van een dreiging of incident en is de vertraging die het maken van deze inschatting oplevert wenselijk? Hoe zit het met incidenten waarbij data of persoonsgegevens gestolen worden zonder dat er een verstoring van diensten plaats vind?
4. Lid 2e stelt als voorwaarde dat “voor de verstrekking van gegevens een onder a tot en met d bedoelde organisatie ontbreekt.” Ook hier is weer onderzoek door het NCSC nodig alvorens er gewaarschuwd wordt.
5. Lid 2e stelt als voorwaarde dat “voor de verstrekking van gegevens een onder a tot en met d bedoelde organisatie ontbreekt.” Lid 2d stelt nadrukkelijk dat “aanbieders van internettoegangs- en internetcommunicatiediensten” (ISPs dus) voorrang moeten hebben op het rechtstreeks benaderen van “aanbieders”. Maar aangezien elk bedrijf in Nederland wel een ISP heeft, zullen deze dus altijd voor gaan.

Hieronder een paar voorbeelden:

Het NCSC wordt (bijvoorbeeld door DIVD) op de hoogte gesteld van een lijst van IP adressen met daarop kwetsbare Exchange email servers, de bijbehorende bedrijven door de maker van de lijst al geidentifieerd.

Vraag: Is er bij het overnemen van een mailserver en meelezen met alle email communicatie spraken van dusdanige “nadelige maatschappelijke gevolgen” dat deze bedrijven door het NCSC benaderd mogen worden?

Op de bovengenoemde lijst staat leverancier van zaden, deze leverancier heeft unieke kennis die belangrijk is voor de Nederlandse economie.

Is het benaderen van deze leverancier mogelijk gegeven dat lid 2e het over “aanbieders” heeft, maar een zaadveredelaar geen “aanbieder” is.

Op de lijst staat ook de grootste aanbieder van openbaar vervoer diensten van Nederland.

Vormt het feit dat de dienstverlening van deze aanbieder niet verstoort wordt als zijn email gelezen wordt een beletsel voor het benaderen van deze aanbieder.

Op de lijst staat een organisatie die aangesloten is bij twee OKTTs en een organisatie die dit niet is.

Andere voorbehouden daargelaten, is het zo dat het NCSC nu wel de tweede organisatie rechtstreeks mag benaderen, maar de eerste niet?

Aangezien de lijst IP adressen bevat, is het waarschijnlijk dat deze verzorgt worden door een aanbieder van internettoegangs- en internetcommunicatiediensten.

Betekent dit dat het NCSC de IS[moet benaderen en niet rechtstreeks de organisatie mag benaderen?