Belgisch Instituut voor
postdiensten en telecommunicatie

Raadpleging betreffende het ontwerp van mededeling over de risicoanalyses op het vlak van de beveiliging van netwerken en informatiesystemen

Hoe kunt u reageren op dit document?

Tot 15/09/2020
Enkel via e-mail naar consultation.sg@ibpt.be
Met de referentie CONSULT-2020-D1

Aanspreekpunt: Pierre-Francois Vandenhaute, Ingenieur-adviseur (+32 2 226 89 78)

Antwoorden dienen elektronisch te worden verzonden naar het opgegeven adres.

Voeg dit formulier als eerste blad bij uw antwoord a.u.b.

Uw opmerkingen zouden moeten verwijzen naar de paragrafen en/of tekstgedeelten waarop ze betrekking hebben en duidelijk aangeven wat vertrouwelijk is.

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 | 1030 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

Deel I. Inleiding

1. Het BIPT is van plan om de operatoren te vragen om jaarlijks een risicoanalyse voor te leggen aan het BIPT en om op basis daarvan de voornaamste risico-elementen op nationaal niveau te evalueren ten behoeve van de overheden en de operatoren. Daartoe stelt het BIPT het platform SERIMA.be ter beschikking.

2. De ontwerpmededeling die ter consultatie is voorgelegd, is weergegeven in deel 2.

3. Het BIPT wil alle relevante suggesties of opmerkingen over deze ontwerpmededeling verzamelen.

Deel II. Ontwerpmededeling

1. Voorwerp

4. De elektronische-communicatiesector (waaronder ook de digitale infrastructuren vallen) omvat essentiële elementen voor de werking van de maatschappij en de overheidsdiensten. De beveiliging van al die elementen, zowel materieel als organisatorisch, moet een prioriteit zijn voor alle spelers in die sector. De talrijke vervlechtingen tussen de verschillende spelers en diensten moeten elke speler aanzetten om een voldoende beveiligingsniveau te bereiken om zijn eigen activiteiten te beschermen maar ook de diensten van andere spelers in de sector.

5. In deze context bepaalt artikel 114, § 1, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de "WEC") dat elke telecomoperator de passende technische en organisatorische maatregelen moet treffen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen. Rekening houdend met de meest recente technische mogelijkheden, moeten deze maatregelen een veiligheidsniveau garanderen dat is afgestemd op de bestaande risico's.

6. Artikel 20 van de NIS-wet[1], dat van toepassing is op de aanbieders van essentiële diensten (AED's) van onder andere de sector van de digitale infrastructuren, bevat een gelijkaardige bepaling. Het BIPT werd aangeduid als sectoroverheid en inspectiedienst voor deze sector in het kader van de NIS-wet en is gestart met de aanwijzing van de AED's. De AED's en de telecomoperatoren worden hierna aangeduid als de "operatoren".

7. Deze mededeling beoogt om de sector te informeren over de invoering door het BIPT van een nieuwe risicoanalysetool inzake veiligheid van de netwerken en informatiesystemen, in de vorm van een onlineplatform (hierna "het platform SERIMA.be[2]). Deze tool is gewijd aan:

   - het vergemakkelijken van de uitwisseling van informatie tussen de operatoren en het BIPT, met name in het kader van de controle op de naleving van artikel 114, § 1, eerste lid, van de WEC en van artikel 20, § 1, van de NIS-wet, en;
   - om de operatoren in staat te stellen zichzelf te evalueren en hun veiligheidsniveau te verhogen.

8. In een eerste instantie zal het BIPT aan de AED's en bepaalde telecomoperatoren (gezien hun beduidende belang voor de Belgische maatschappij en economie) vragen om het platform SERIMA.be te gebruiken. De overige telecomoperatoren kunnen de tool gebruiken als ze daartoe een verzoek richten aan het BIPT en de voorwaarden beoogd in deze mededeling in acht nemen. In een tweede instantie en op basis van feedback, zal het BIPT de opportuniteit bekijken om het aantal gebruikers van het platform uit te breiden.

9. De ontwerpmededeling heeft ter openbare raadpleging voorgelegen van 22/07/2020 tot 15/09/2020.

[1] Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
[2] Kort voor "Security Risk Management".

2. Juridisch kader

10. Krachtens artikel 8, 6°, van de WEC, heeft het BIPT de taak om te waken over de integriteit en de veiligheid van de openbare elektronische-communicatienetwerken en over de veiligheid van de openbare elektronische-communicatiediensten.

11. Conform artikel 14, § 1, 3°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (statuutwet), is het BIPT er overigens mee belast om de naleving van de bepalingen van de WEC en de NIS-wet te controleren wat betreft de sector van de digitale infrastructuren.

12. Artikel 114/2, § 1, van de WEC preciseert dat, in het kader van deze controle, het BIPT de macht heeft om bindende instructies te geven, ook met betrekking tot de termijnen voor de uitvoering, aan de telecomoperatoren.

13. Het BIPT kan ook, conform artikel 114/2, § 2, van de WEC, van diezelfde telecomoperatoren alle informatie vragen die nodig is voor de evaluatie van de veiligheid of integriteit, of beide, van hun diensten en netwerken, met inbegrip van de stukken betreffende hun veiligheidsbeleid (eerste lid), alsook deze operatoren onderwerpen aan een veiligheidscontrole uitgevoerd door een gekwalificeerde onafhankelijke instantie of het Instituut zelf (tweede lid).

14. Verder is het BIPT aangewezen als inspectiedienst voor de sector van de digitale infrastructuren in het kader van de NIS-wet, die onder andere het volgende bepaalt:

- “De inspectiediensten kunnen op elk ogenblik controles uitvoeren op de naleving door de aanbieder van essentiële diensten van de beveiligingsmaatregelen en de regels voor het melden van incidenten.” (artikel 42, § 1);
- De inspectiedienst kan een verzoek om informatie of bewijsstukken formuleren (artikel 42, § 3);
- “De aanbieder van essentiële diensten verleent zijn volledige medewerking aan de leden van de inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.” (artikel 46, § 1).

3. Veiligheidsmaatregelen en risicoanalyse

15. De verplichting waarvan sprake in artikel 114, § 1, eerste lid, van de WEC, om de passende technische en organisatorische maatregelen te treffen om de risico's voor de veiligheid van de netwerken en diensten goed te beheersen en de verplichting die gelijkwaardig is aan artikel 20 van de NIS-wet, impliceren dat een systeem voor veiligheidsbeheer wordt opgezet en regelmatig wordt bijgewerkt dat van die aard is dat een gepaste risicoanalyse mogelijk is.

16. Een risicoanalyse omvat drie hoofdstappen[3]:

- de identificatie van de risico's;
- de evaluatie van de risico's;
- het risicobeheer.

17. Voor degelijke resultaten moet een risicoanalyse beantwoorden aan de volgende voorwaarden:

- worden uitgevoerd voor alle opgelijste assets van een onderneming[4];
- de assets tegenover de bedreigingen stellen;
- voor elk koppel asset-bedreiging, de kwetsbaarheden identificeren;
- op basis van de identificatie van de kwetsbaarheden, de veiligheidsmaatregelen treffen die de impact en/of de waarschijnlijkheid van misbruik van een kwetsbaarheid, en dus het risico, wegnemen, of bij gebrek daaraan beperken.

[3] Dit vloeit voort uit de normen inzake netwerkveiligheid: ISO/IEC 27005, NIST Special Publication 800-37, BS 7799-3 BSI.
[4] Per definitie vertegenwoordigen de assets van een maatschappij alle materiële, menselijke, administratieve of organisatorische middelen die betrokken zijn bij de verstrekking van zijn diensten of producten.

4. Het platform SERIMA.be

4.1. Algemene beschrijving

18. Via het platform SERIMA.be kan een volledige risicoanalyse worden gemaakt volgens de methode vastgelegd in de norm ISO/IEC 27005 met betrekking tot de informatietechnologie, beveiligingstechnieken en het risicobeheer in verband met informatiebeveiliging, die een relevante norm vormt voor de toepassing van verschillende reglementeringen die aspecten van risicobeheer omvatten zoals artikel 114, § 1, van de WEC en artikel 20 van de NIS-wet en de GDPR[5]. Het BIPT zal uiteraard enkel de inachtneming van de WEC en van de NIS-wet (voor de sector van de digitale infrastructuren) onderzoeken.

19. Rekening houdend met de talrijke contexten voor de toepassing van de norm ISO/IEC 27005, werd het platform SERIMA.be ontworpen om de ondernemingen in staat te stellen om de relevante risico's te selecteren om voor te leggen aan de bevoegde overheid voor een gegeven reglementering. Zodra deze data zijn ingevoerd op het platform, zullen ze deels of gedeeltelijk worden voorgelegd aan de relevante regulator(en), volgens de door de onderneming geselecteerde parameters.

20. Bovendien kan het platform SERIMA.be door elke operator die daar toegang toe heeft, worden gebruikt als systeem voor risicobeheer voor andere referentiesystemen[6], zoals de referentiesystemen die eigen zijn aan de onderneming.

21. Het platform SERIMA.be is bedoeld om te evolueren volgens de feedback van zijn gebruikers, met name wat betreft de update van de bibliotheken, de correctie van de bestaande functionaliteiten alsook de toevoeging van eventuele functionaliteiten.

22. Het platform SERIMA.be stelt elke telecomoperator in staat om een gepaste risicoanalyse uit te voeren en om de reeds intern ingevoerde veiligheidsmaatregelen te evalueren volgens de methode beschreven in de "Technical guidelines of security measures"[7] van ENISA. De relevante elementen voor het BIPT, in het kader van zijn wettelijke opdrachten, kunnen vervolgens geselecteerd worden per onderneming en worden doorgestuurd naar het BIPT.

4.2. Streefdoelen

23. Het platform SERIMA.be heeft als voornaamste doel om de uitwisseling van informatie tussen de operatoren en het BIPT te vergemakkelijken in het kader van de controle op de naleving van de WEC en de NIS-wet.

[5] Verordening nr. 2016/679, de algemene verordening voor gegevensbescherming.
[6] ISO27001, GDPR of een referentiesysteem gedefinieerd door de onderneming.
[7] https://resilience.enisa.europa.eu/article-13

24. De overdracht van informatie via het platform SERIMA.be zal in het bijzonder het BIPT in staat stellen om:

- over een duidelijker en preciezer overzicht te beschikken op het niveau van beveiliging van elke operator op het stuk van veiligheid van de netwerken en diensten;
- de evolutie van de situatie van een operator van jaar tot jaar te volgen;
- op een gemakkelijke en geautomatiseerde wijze de data te vergelijken tussen operatoren, dankzij het gebruik van eenzelfde werkwijze en de standaardisering van het dataformaat.

25. Bovendien zal het BIPT nuttige lessen kunnen trekken door de data doorgestuurd naar het platform SERIMA.be in geaggregeerde vorm te observeren, zoals de identificatie van de risico's die gemeenschappelijk zijn voor de meeste of alle operatoren, de goede praktijken wat betreft de veiligheidsmaatregelen enz. Deze vaststellingen zullen er met name toe bijdragen de niveaus van prioriteit vast te leggen voor zijn interventiedomeinen.

26. Overigens zal het BIPT aan de sector een bijdrage kunnen aanbieden op basis van deze lessen:

- door elke operator die gebruikmaakt van het platform, na onderzoek van de data doorgestuurd via dit platform, een generiek verslag en een individueel verslag van zijn risicobeheer te bezorgen om hem te ondersteunen bij zijn veiligheidsbeheer;
- door de publicatie van een algemeen verslag voor hulp bij het risicobeheer bestemd voor alle spelers van de sector.

4.3. Praktische inlichtingen

4.3.1. Toegang tot het platform

27. Het platform voor risicobeheer SERIMA.be is toegankelijk via het volgende adres: https://serima.be.

28. De toegang moet gevraagd worden via e-mail aan net.sec@bipt.be.

29. Het BIPT verstrekt één toegang per operator. Verschillende gebruikers van eenzelfde operator mogen die toegang gebruiken.

4.3.2. Informatie waarmee rekening moet worden gehouden

30. Opdat de risicoanalyse via SERIMA.be doeltreffend zou zijn, moet een aantal elementen worden beantwoord.

31. De volgende diensten worden standaard meegenomen in de analyse:

- dark fiber of glasvezelnetwerk: uitbating, beschikbaarstelling en/of onderhoud van deze glasvezel;

- data: mobiel, vast, transit, interconnectie, VPN;
- spraak: mobiel, vast, interconnectie;
- video (met uitzondering van tv en radio): mobiel, vast, interconnectie;
- berichten: instant messaging, sms, e-mail.

32. Zowel de elektronische diensten op retailniveau (“retail”) als de diensten voor ondernemingen (“business”) en andere operatoren (“wholesale”) moeten in beschouwing worden genomen bij het gebruik van het platform aangezien elk van deze types van diensten een beduidende impact kan hebben op de goede werking van de maatschappij en de economie.

33. Opdat een nieuwe invoer geldig zou zijn, moet de als “verplicht” aangeduide informatie op het platform SERIMA.be exact en naar eer en geweten worden ingevuld. Het gaat om:

- algemene projectgegevens;
- data die de context van de risicoanalyse definiëren;
- data betreffende de risicoanalyse voor het geheel van aangeboden diensten, assets ter ondersteuning, in verband te brengen met ten minste de bedreigingen die als “verplicht” zijn opgenomen;
- data die de reeds ingevoerde maatregelen beschrijven en de evaluatie van het veiligheidsniveau.

34. Voor de jaren 2021 en volgende, worden de operatoren verzocht om dit formulier minstens één keer per jaar voor te leggen aan het BIPT, tussen 1 april en 30 juni ten laatste, via het platform SERIMA.be dat hen ter beschikking wordt gesteld of door aan het BIPT een export van hun eigen SERIMA.be-platform te bezorgen.

35. Indien het BIPT op gemotiveerde wijze de indiening van het formulier verwerpt wegens ongeldigheid van dat laatste, heeft de operator de mogelijkheid om een gecorrigeerd formulier voor te leggen binnen de door het BIPT vastgelegde termijn.

4.3.3. Opleidingen

36. Er zullen periodiek via het BIPT opleidingen voor het gebruik van het SERIMA.be-platform worden aangeboden.

37. Er zullen ook tutorials in de vorm van video’s beschikbaar gesteld worden.

5. Conclusies

38. In een eerste instantie zal het BIPT aan de AED's en bepaalde telecomoperatoren (gezien hun beduidende belang voor de Belgische maatschappij en economie) vragen om het platform SERIMA.be te gebruiken. De overige telecomoperatoren kunnen de tool gebruiken als ze daartoe een verzoek richten aan het BIPT en de voorwaarden beoogd in deze mededeling in acht nemen. In een tweede instantie en op basis van feedback, zal het BIPT de opportuniteit bekijken om het aantal gebruikers van het platform uit te breiden.

39. Na onderzoek van de data doorgestuurd via het platform SERIMA.be, zal het BIPT aan elke operator een generiek verslag en een individueel verslag van zijn risicobeheer bezorgen om hem te ondersteunen bij zijn veiligheidsbeheer.

Axel Desmedt
lid van de Raad

Jack Hamande
lid van de Raad

Luc Vanfleteren
lid van de Raad

Michel Van Bellinghen
voorzitter van de Raad