Belgisch Instituut voor
postdiensten en telecommunicatie

Mededeling van de Raad van het BIPT van 12 april 2023 over het platform SERIMA.be (risicoanalyses op het vlak van de beveiliging van netwerken en informatiesystemen)

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 bus 1 | 1030 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

1. Voorwerp

1. De elektronische-communicatiesector (waaronder ook de digitale infrastructuren vallen) omvat essentiële elementen voor de werking van de maatschappij en de openbare diensten. De beveiliging van al die elementen, zowel materieel als organisatorisch, moet een prioriteit zijn voor alle spelers in die sector. Door een toereikend beveiligingsniveau te bereiken, beschermt een sectorspeler niet alleen zijn eigen activiteiten, maar bovendien profiteren de diensten van de andere spelers van de sector daar ook van, gelet op de talrijke vervlechtingen tussen de verschillende spelers en diensten.

2. In deze context bepaalt artikel 107/2, § 1, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de "WEC") dat elke telecomoperator:

   2.1. de risico's voor de veiligheid van zijn netwerken en diensten moet analyseren, waarbij het BIPT de nadere bepalingen van deze risicoanalyse kan vastleggen;

   2.2. *"de passende en evenredige technische en organisatorische maatregelen* [moet nemen], *waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden."*

3. Wat de tweede verplichting betreft (verplichting met betrekking tot de maatregelen) omvat 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, 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".

4. Deze mededeling beoogt om de sector te informeren over de risicoanalysetool inzake veiligheid van de netwerken en informatiesystemen (hierna "het platform SERIMA.be[2]). Deze tool is bestemd om:

   - de uitwisseling van informatie tussen de operatoren en het BIPT te vergemakkelijken, met name in het kader van de controle op de naleving van artikel 107/2, § 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.

5. 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, na een analyse van de vervlechtingen en op basis van de feedback, zal het BIPT de opportuniteit bekijken om het aantal gebruikers van het platform uit te breiden.

[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".

6. Deze mededeling vervangt de mededeling van 5/07/2022. De wijziging die aan die mededeling wordt aangebracht, is de volgende (zie punt 35 van de huidige mededeling): na raadpleging van de operatoren wordt de vervaldatum voor het doorsturen van de risicoanalyse naar het BIPT vastgelegd op de maand juni (in plaats van december van elk jaar).

2. Juridisch kader

7. Krachtens artikel 6, 4°, van de WEC, "bevordert het Instituut de belangen van de burgers" "door de beveiliging van netwerken en diensten te handhaven".

8. Artikel 107/2, § 1, van de telecomwet bepaalt dat het BIPT de voorwaarden kan vastleggen voor de risicoanalyse op het stuk van beveiliging van de netwerken en diensten die de operatoren moeten uitvoeren.

9. Artikel 107/4, § 1, van de WEC preciseert dat, in het kader van deze controle, het BIPT de macht heeft om aan de telecomoperatoren bindende instructies te geven, ook met betrekking tot de termijnen voor de uitvoering.

10. Het BIPT kan ook, conform artikel 107/4, § 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).

11. 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).

12. Artikel 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (hierna de wet "kritieke infrastructuren") bepaalt vervolgens dat *"Voor de sector elektronische communicatie en digitale infrastructuren wordt het Belgisch Instituut voor postdiensten en telecommunicatie aangeduid als inspectiedienst belast met het controleren van de toepassing van de bepalingen van deze wet en haar uitvoeringsbesluiten."*

13. 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 ten slotte mee belast om de naleving van de bepalingen te controleren van onder meer:

13.1. de WEC;

13.2. de wet "kritieke infrastructuren", wat betreft de sectoren van de elektronische communicatie en van de digitale infrastructuren, en;

13.3. de NIS-wet, wat betreft de sectoren van de digitale infrastructuren.

3. Veiligheidsmaatregelen en risicoanalyse

14. Conform artikel 107/2, § 1, moeten de operatoren de risico's voor de veiligheid van hun netwerken en diensten analyseren. Een risicoanalyse in overeenstemming met deze bepaling houdt in dat ze wordt bijgewerkt wanneer dat nodig blijkt.

15. Een risicoanalyse omvat drie hoofdstappen[3]:

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

16. Om bruikbaar te zijn moet een risicoanalyse beantwoorden aan de volgende voorwaarden:

- worden uitgevoerd voor alle assets die onontbeerlijk zijn voor de goede werking van de netwerken[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 haar diensten of producten.

4. Het platform SERIMA.be

4.1. Algemene beschrijving

17. 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 107/2, § 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 onderzoeken (voor de sector van de digitale infrastructuren).

18. Het platform SERIMA.be is gebaseerd op de tool MONARC[6] ten uitvoer gebracht door SecurityMadeIn.LU[7]. Het gaat om een "Open Source"-tool die beschikbaar is op https://monarc.lu.

19. Rekening houdend met de talrijke contexten van toepassing van de norm ISO/IEC 27005, werd het platform SERIMA.be ontworpen om de ondernemingen in staat te stellen om de analyse uit te voeren, rekening houdend met verschillende reglementeringen.

20. Bovendien kan het platform SERIMA.be door elke operator die daar toegang toe heeft, worden gebruikt als systeem voor risicobeheer voor andere referentiesystemen[8], 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"[9] 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] GEOPTIMALISEERDE METHODE VOOR RISICOANALYSES, https://monarc.lu
[7] https://securitymadein.lu/
[8] ISO27001, GDPR of een referentiesysteem gedefinieerd door de onderneming.
[9] 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 de sector kunnen laten profiteren van deze lessen:

- door elke operator die gebruikmaakt van het platform, na onderzoek van de data doorgestuurd via dit platform, 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;
- door een gebruikersgemeenschap te cultiveren rond het platform. Via deze gemeenschap zal informatie betreffende de risicoanalyses en de veiligheidsmaatregelen kunnen worden uitgewisseld.

4.3. Praktische inlichtingen

4.3.1. Toegang tot het platform

27. De toegang moet gevraagd worden via e-mail aan sec_netsec@bipt.be. De dienst NetSec zal de aanvraag valideren bij de contactpersoon bedoeld in artikel 9, § 1, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie voor de telecomoperatoren of bij het contactpunt bedoeld in artikel 23, § 1, van de NIS-wet. Bij de aanvraag moet een e-mailadres alsook een telefoonnummer worden verstrekt. De dienst NetSec zal dan de documentatie over het platform alsook de nodige gegevens om daarop in te loggen meedelen.

28. De operator heeft ook de mogelijkheid om de risicoanalysetool rechtstreeks in zijn eigen IT-omgeving te installeren. Deze tool is beschikbaar op de website van SecurityMadeIn.LU[10]. Al deze kosten in verband met zijn eigen *instance* van de risicoanalysetool zijn op eigen kosten. Het is belangrijk eraan te herinneren dat het gaat om een "Open Source"-tool waarvoor geen enkele licentie vereist is. In dat geval moet de operator de bibliotheken gebruiken die het BIPT aanbiedt voor de analyses die aan het

[10] https://www.monarc.lu/download/

BIPT zullen worden voorgelegd. De toegang tot de bibliotheken moet gevraagd worden via e-mail aan sec_netsec@bipt.be.

29. De algemene documentatie over de risicoanalysetool MONARC is beschikbaar op https://www.monarc.lu/documentation/.

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;
- sms'en.

32. De volgende diensten kunnen in de analyse worden beschouwd: e-mail, instant messaging.

33. 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.

34. 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[11] beschrijven en de evaluatie van het veiligheidsniveau.

35. Voor de jaren 2023 en volgende, worden de operatoren verzocht om dit formulier minstens één keer per jaar voor te leggen aan het BIPT, tussen 1 juni 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 instance te bezorgen volgens het sjabloon dat door het BIPT samen met de entiteiten van de sector werd vastgesteld.

[11] Het is voldoende dat de tool een geaggregeerde vorm van de ingestelde maatregelen of de verwijzing naar de relevante documentatie bevat.

36. 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

37. Er zullen periodiek via het BIPT of via SecurityMadeIn.LU[12] opleidingen voor het gebruik van het SERIMA.be-platform worden aangeboden.

[12] https://www.monarc.lu/trainings/

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

Bernardo Herman
Lid van de Raad

Luc Vanfleteren
Lid van de Raad

Michel Van Bellinghen
Voorzitter van de Raad