FE1816 FE-DDIS.DK

Fra:	Peter van Erp <peterve@nl-ix.net>
Sendt:	18. april 2018 18:49
Til:	FE1816 FE-DDIS.DK; cfcs@cfcs.dk
Emne:	FW: Hearing of new regulation on the security of network and information systems for Internet Exchange Points
Vedhæftede filer:	Udkast til IXP-bekendtgørelse.docx; List of parties to be heard.docx; hearing note.docx
Prioritet:	Høj

Dear ms Pedersen,

Thank you for the call today, and as promised, herewith our comments on your draft regulation on the security of network and information systems for internet exchange points.

Introduction

NL-ix is a pan European Interconnect service provider providing a full portfolio of connectivity services. NL-ix primarily provides interconnect services between (carrier neutral) data centres. NL-ix in general does not provide services to customers at customer premises. The NL-ix interconnect services are provided in 13 EU countries and can range from interconnect between parties in a single metro area to interconnect between two metro areas in the same country or between data centres in different EU countries. As a result, NL-ix is subject to regulations with respect to network and information systems in various different jurisdictions.

The NL-ix interconnect portfolio comprises a whole range of services in the following 4 categories:

1. Peering services: These are primarily Internet Exchange Point services as provided by more traditional Internet Exchange Points, but can also comprise Remote-IX services where NL-ix connects a customer in one country to an Internet Exchange Point in another country rather than the NL-ix Internet Exchange Point.
2. Transport services: These comprise point to point or point to multipoint connectivity services such as MPLS services or DWDM wave services
3. Transit services: Involve a mix of full IP transit and partial IP transit services
4. Cloud services: Comprising direct connectivity to public cloud services such as Amazon AWS or Microsoft Azure.

Comments on draft regulation

NL-ix would like to request that you take the following issues into account in finalising your regulatory framework.

Scope of the regulation

As set out in the introduction, NL-ix is a pan European provider of various interconnect services. We believe that this regulation should not be applied to NL-ix as a whole, but should be targeted on the following scope

a. Internet Exchange Point services (Peering services delivered in the internet exchange point in Denmark). Transport, Transit and Cloud services are out of scope; AND
b. Only the Internet Exchange Point services that involve Danish consumers. The services NL-ix provides involving say Dutch consumers, fall under the jurisdiction of the Dutch implementation of the NIS. We believe that it does not make sense to have overlaps in the services being regulated. The following examples of peering relationships illustrate this point:
    a. Disruptions in the service for a Danish ISP in Copenhagen peering with a content provider (independent of the location) such as facebook in Amsterdam or Copenhagen obviously affects Danish consumers. The location of the content provider is not relevant

b. Disruptions in the service for a United States ISP in Copenhagen peering with a content provider in Copenhagen does not affect Danish consumers. US consumers are affected despite the fact that Danish content is involved.
c. Disruptions in the service for an Indonesian ISP in Marseille (or a Dutch ISP in Amsterdam) peering with a Danish content provider in Copenhagen does not affect Danish consumers

NL-ix feels that the assessment whether NL-ix falls under the Danish implementation of the NIS, or the reporting obligations should thus be based on the volume of traffic *pertinent to Danish consumers* and not on the total volume of traffic handled by NL-ix be it in Denmark or Europe wide.

Article 2.3.3 and 2.6.3 - Requirements

> ***2.3.3.*** *Based on the risk assessment pursuant to subsections 1 and 2, operators shall implement appropriate measures to ensure availability, authenticity, integrity and confidentiality of services and ensure that third parties maintain equivalent security in relation to operating deliveries to operators pursuant to paragraph 1. 2nd*
>
> ***2.6.3.*** *In determining the risk tolerance pursuant to subsection 2, account must be taken of the fact that operators should maintain the availability of their essential services in emergency situations and in other exceptional circumstances in order to secure the community's internet traffic.*

Firstly, we believe that the EU NIS directive does not mandate any guaranteed availability of Internet Exchange Point services. The service provider should be free to choose the level of service provided (SLA) and the associated and price point of the service. Consequently, we feel that the above requirements *to ensure availability* should be nuanced to reflect the availability according to the service level offered.

Secondly, an Internet Exchange Point service provider is unable to independently maintain the availability of any consumer service (eg banking payment service or internet access service). While NL-ix internally always uses redundant connectivity between the nodes in the NL-ix network, if a customer purchases a single physical connection (port) on the NL-ix infrastructure, NL-ix cannot be held responsible for the consequences of this customer decision. All hardware can suffer failure and some failures take longer to solve than others. In such cases the services to the customer (and therefore banking payment service) can suffer disruption. While it is normal good practice to use multiple geo-redundant connections for essential services, NL-ix is not in a position to force any customer to implement such multiple geo-redundant connections through NL-ix or any other connectivity provider. Consequently, NL-ix is unable to independently ensure that essential services (such as banking payment services or internet access services) will be maintained

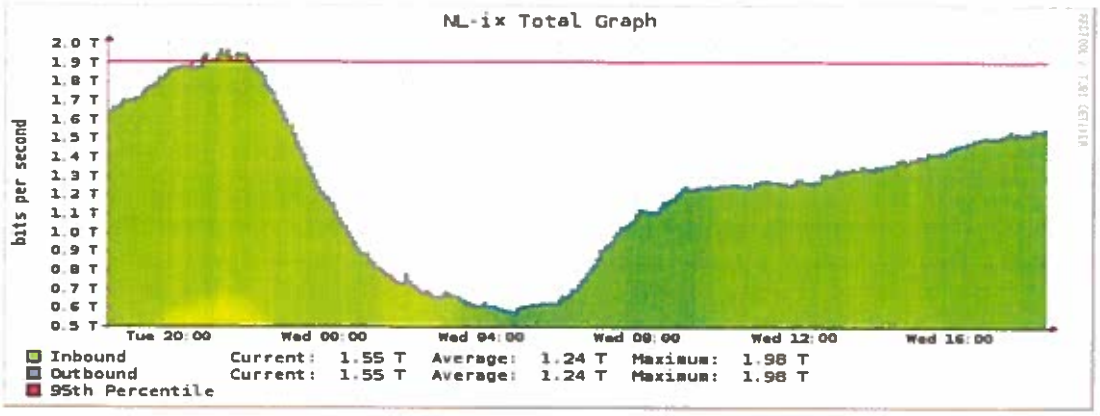
Article 3.8 – Notification obligation

> ***3.8.*** *An incident has significant consequences for the continuity of the essential services provided by an operator of a significant internet exchange point when the incident in the main service entails*
> *1) decrease in operator capacity compared to handling data of at least 50 percent for at least one hour, or*
> *2) Loss of authenticity, integrity or confidentiality.*

As shown in the attached graph, internet traffic typically shows a daily pattern whereby there is very little traffic at night. The traffic between midnight and 08:00 is typically at 50% or lower than the peak traffic being handled. ISPs typically have backup routes (via another Internet Exchange Point, or using IP transit) should the NL-ix Internet Exchange Point become unavailable. In addition, most operators, including NL-ix also implement service windows for network maintenance in the period 0:00 to 08:00. Any disturbances in the period 0:00 – 08:00 should easily be handled by existing backup arrangements.

We propose to add an extra qualification to the criterium for the notification obligation to reflect this and to avoid the sitation where a notification obligation would be caused by a planned maintenance by NL-ix at night.

> *1) decrease in operator capacity compared to handling data of at least 50 percent for at least one hour in the period 00:00 – 08:00, or*



Please feel free to contact me if you have any further questions.

Best regards,

Peter van Erp
CFO, Legal and Regulatory

NL-ix The Interconnect Exchange | Laan Copes van Cattenburch 73 | 2585 EW The Hague | The Netherlands
T: +31 70 3028820 | M: +31 6 53323952 | E: peterve@nl-ix.net | W: nl-ix.net

---

From: "FE1816 FE-DDIS.DK" <FE1816@FE-DDIS.DK>
Date: Tuesday, 3 April 2018 at 15:14
To: Sales <sales@nl-ix.net>
Subject: Hearing of new regulation on the security of network and information systems for Internet Exchange Points

To The Neutral Internet Exchange

Please find attached a draft for new regulation
on the security of network and information systems for Internet Exchange Points.

Center for Cybersecurity kindly asks that you forward any comments you may have no later than Friday the 20th of April 2018 to
cfcs@cfcs.dk
copy to fe1816@fe-ddis.dk.

Kind Regards

Jane Pedersen
Special Legal Advisor

DANISH DEFENCE INTELLIGENCE
SERVICE
Legal Department
Kastellet 30, DK-2100 Copenhagen
Phone: +45 7959 5204
E-mail:
fe1816@fe-ddis.dk
www.fe-ddis.dk/eng <http://www.fe-ddis.dk/eng>

INSTITUT FOR
MENNESKE
RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL +45 9132 5775
LGH@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 18/00963-2

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø
Danmark

cfcs@cfcs.dk,
kopi til fe1816@fe-ddis.dk

17. APRIL 2018

HØRING OVER BEKENDTGØRELSE OM SIKKERHED I NET- OG INFORMATIONSSYSTEMER FOR OPERATØRER AF VÆSENTLIGE INTERNETUDVEKSLINGSPUNKTER

Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har ved e-mail af 23. marts 2018 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

Instituttet har ingen bemærkninger til udkastet, idet Instituttet blot henviser til sine principielle betragtninger om Center for Cybersikkerheds rolle som national "CSIRT" (Computer Security Incident Response Team) i instituttets høringssvar af 23. november 2017 over et udkast til forslag til lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v. under Forsvarsministeriets sagsnr. 2017/006372.

Der henvises til centrets sagsnr. 2018/000609.

Med venlig hilsen

Lise Garkier Hendriksen
CHEFKONSULENT

Vestre Landsret
Præsidenten

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Sendt pr. mail til cfcs@cfcs.dk og fe1816@fe-ddis.dk

J.nr. 40A-VL-28-18
Den 09/04-2018

Forsvarets Efterretningstjeneste har ved brev af 3. april 2018 (sagsnr. 84073) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Den 05 APR. 2018
J.nr. 40A-ØL-26-18
Init: sdy

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Sendt pr. mail til. cfcs@cfcs.dk og fe1816@fe-ddis.dk

Forsvarets Efterretningstjeneste har ved brev af 23. marts 2018 (Sagsnr. 2018/000609) anmodet om eventuelle bemærkninger til høring over udkast til bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Bent Carlsen

Elleg Busck Porsbo

FE1816 FE-DDIS.DK

Fra: Maiken Michelsen <MIMI@domstolsstyrelsen.dk>
Sendt: 18. april 2018 16:23
Til: FE1816 FE-DDIS.DK
Emne: SV: Høring over bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter

Til Forsvarets Efterretningstjeneste

Domstolsstyrelsen har ikke bemærkninger til udkast til ny bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter.

Venlig hilsen

Maiken Michelsen
Direkte: +45 99 68 43 07
mimi@domstolsstyrelsen.dk

Domstolsstyrelsen
Jura
St. Kongensgade 1-3
1264 København K
Tlf. (hovednr.): + 45 70 10 33 22
www.domstol.dk

Fra: FE1816 FE-DDIS.DK [mailto:FE1816@FE-DDIS.DK]
Sendt: 3. april 2018 14:17
Til: 'Domstolsstyrelsen' <post@domstolsstyrelsen.dk>
Emne: Høring over bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter

Til Domstolsstyrelsen

Vedhæftet fremsendes udkast til ny bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter med tilhørende høringsbrev og høringsliste i høring.

Center for Cybersikkerhed skal anmode om at modtage eventuelle høringssvar til det fremsendte udkast til bekendtgørelse **senest fredag den 20. april 2018**. Høringssvarene bedes sendt på e-mail til cfcs@cfcs.dk med kopi til fe1816@fe-ddis.dk og henvisning til sagsnummer 2018/000609.

Med venlig hilsen

Jane Pedersen
Specialkonsulent

FORSVARETS EFTERRETNINGSTJENESTE
Juridisk Afdeling
Kastellet 30, 2100 København Ø

Telefon: 7959 5204
E-mail: fe1816@fe-ddis.dk
www.fe-ddis.dk

Fra: Mikkel Brandenborg Stenalt <ms@datatilsynet.dk>
Sendt: 11. april 2018 10:14
Til: Center for Cybersikkerhed
Cc: FE1816 FE-DDIS.DK
Emne: Vedrørende høring over udkast til bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter - sagsnummer 2018/000609

Til Forsvarets Efterretningstjeneste

Ved brev af 23. marts 2018 har Forsvarets Efterretningstjeneste anmodet om Datatilsynets eventuelle bemærkninger til udkast ti bekendtgørelse om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter. Der henvises til sagsnummer 2018/000609.

Udkastet giver umiddelbart ikke Datatilsynet anledning til bemærkninger.

Med venlig hilsen

Mikkel B. Stenalt
Fuldmægtig, cand.jur.

Tlf.: (+45) 33 19 32 16
E-mail: ms@datatilsynet.dk

DATATILSYNET
Borgergade 28, 5. sal, 1300 København K
Tlf.: +45 3319 3200, Fax: +45 3319 3218
E-mail: dt@datatilsynet.dk, Internet: www.datatilsynet.dk