nic.at GmbH
Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria
T: +43 662 46 69 -0 · F -29
office@nic.at · www.nic.at

nic.at GmbH · Jakob-Haringer-Str. 8/V · 5020 Salzburg

Bundeskanzleramt
Büro für strategische Netz- und Informationssystemsicherheit
Ballhausplatz 2
1010 Wien
Österreich

Wien, am 25. Oktober 2018

Betreff: Stellungnahme zum NIS-Gesetz

Sehr geehrte Damen und Herren,

als Betreiber des österreichischen nationalen CERTs (CERT.at) ist für nic.at GmbH der vorliegende Entwurf eines Gesetzes zu der Umsetzung der EU NIS-Richtlinie von hohem Interesse. Wir nehmen daher gerne die Einladung wahr, unsere Kommentare und Verbesserungsvorschläge einzubringen.

Einleitend möchten wir festhalten, dass wir das Gesetz explizit begrüßen, da es

- die NIS-Richtlinie umsetzt,
- einiges, was durch die ÖSCS geschaffen wurde, rechtlich verankert
- und den Computer-Notfallteams und den meldenden Organisationen eine klare rechtliche Grundlage für ihre Tätigkeit im Rahmen des Informationsaustausches gibt.

Wir möchten in den folgenden Erläuterungen Verbesserungsvorschläge darstellen, die möglicherweise im Zuge des legistischen Prozesses von Seiten der Behörden nicht diskutiert wurden.

Im Weiteren wird das englische Akronym CSIRT gleichbedeutend mit „Computer-Notfallteam" verwendet.

§ 4 Aufgaben des Bundeskanzlers

Hier würden wir empfehlen, dass bei den Aufgaben des Bundeskanzlers auch der Betrieb des GovCERTs explizit angeführt wird.

§ 9 Befugnisse zur Vorbeugung von Sicherheitsvorfällen

Die in § 9 Abs. 1 beschriebene Sensorik ist ein Schritt in die richtige Richtung, und wird in den Erläuternden Bemerkungen auch hinreichend gut erklärt. Trotzdem hielten wir es für notwendig, einige der Eckpunkte auch im Gesetzestext festzuhalten. Das sind:

- die Sensorik wird bei dem zu schützenden Betreiber eines Dienstes (BwD, AdD, EdB) installiert, und nicht in den Backbones / ISPs / IXPs
- im Spezialfall, dass der BwD ein ISP ist, so geht es um den Schutz des ISPs selber (also dessen Corporate Network), und nicht um das Produktionsnetz, das die Kunden nutzen
- ein klares Verbot diese Sensorik für anderwärtige Zwecke zu nutzen.

Des Weiteren empfehlen wir § 9 Abs. 1 zweiter Satz wie folgt abzuändern, um die Freiwilligkeit der Teilnahme sicherzustellen und um zu garantieren, dass gewonnene Erkenntnisse auch an die Teilnehmer weitergegeben werden.

§ 9 Abs. 1 nic.at/CERT Vorschlag Gesetzestext:

> Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes können **freiwillig** an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen teilnehmen, **aber nicht dazu (per Bescheid) verpflichtet werden**. Sie können weiters **eigenständig** festlegen, welche Daten an den Bundesminister für Inneres übermittelt werden. **Freiwillig teilnehmende Organisationen haben jedenfalls das Recht, umfassend und zeitnahe über sie betreffende Erkenntnisse informiert zu werden.**

Honeypots und Sinkholes (§ 9 Abs. 2) sind unserer Meinung nach sehr sinnvoll. Es fehlt hier eine Einschränkung der möglichen Platzierung dieser Sensoren, damit diese möglichst keinen legitimen Internetverkehr mit aufzeichnen.

§ 9 Abs. 3 nic.at/CERT Vorschlag Gesetzestext:

> (3) Die technischen Einrichtungen laut Abs. 1 und 2 sind so zu installieren, dass sie möglichst nur den für die Erfüllung des Zweckes unbedingt nötigen Datenverkehr erfassen. Die gewonnenen personenbezogenen Daten dürfen ausschließlich für die Erfüllung der Aufgabe gemäß § 5 Z 4 verwendet werden.

Hier würden wir es als positives Zeichen und auch als Anreiz der Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes sehen, wenn die Kosten für die Teilnahme zur Gänze vom Bund getragen werden.

§ 10 Datenverarbeitung

Zu Abs. 2 unterbreiten wir folgenden ergänzenden Vorschlag: Es ist zur Wahrnehmung der Aufgaben der Computer-Notfallteams wichtig, dass auch diese dazu explizit befugt sind und ermächtigt werden, sowohl Identifikations- und Erreichbarkeitsdaten als auch auch die Liste der wesentlichen Dienste erhalten und verarbeiten zu dürfen.

Es ist nachvollziehbar, dass NIS-Büros Zugriff auf Information bekommen, die für ihre Aufgabenerfüllung nötig sind. Eine „Freiwillige Meldung" (§ 20) stellt den Grundpfeiler zur Prävention von Angriffen auf die IKT Infrastruktur in Österreich dar. Daher ist bei der Formulierung des § 10 Abs. 3 dahingehend Vorsicht geboten, dass die Konstruktion der „freiwilligen Meldung" an die Computer-Notfallteams oder das Vertrauensverhältnis zwischen Betreibern und ihren sektorenspezifische Computer-Notfallteams nicht untergraben wird.

Die an die Computer-Notfallteams übermittelten Daten von Dritten unterliegen, sofern es sich nicht um Daten eines meldepflichtigen Vorfalls handelt, einer hohen Vertraulichkeit zwischen Meldern und dem CSIRT. Daher ist sicherzustellen, dass das CSIRT bei der Kontrolle seiner Aufgabenerfüllung (§§ 12, 13) durch die NIS-Büros keinen Zugriff auf die Inhalte der eingemeldeten Daten ermöglichen muss und dies auch nicht aus der Auskunftspflicht nach Abs. 3 abgeleitet werden darf.

§ 11 Gemeinsame Verarbeitung

Neben der Verarbeitung von Daten zu konkreten Vorfällen in Österreich ist es für die NIS-Büros und die Computer-Notfallteams wichtig, Information zu aktuellen Bedrohungen einzuholen, diese zu sammeln, zu bewerten und für den effektiven Schutz der IKT Infrastruktur Österreichs einzusetzen. Das kann entweder durch Weitergabe an die BwD/AdD/EdB (§ 12 Abs. 2(4)) oder durch Nutzung in der Sensorik laut § 9 Abs. 1 erfolgen.

Für eine effektive Gefahrenabwehr ist es sinnvoll, dass diese Datenbasis zu Computer Threat Information (CTI) übergreifend im BMLV, BMI und den CSIRTs gemeinsam geführt werden darf.

§12 Aufgaben der Computer-Notfallteams

Die Regelungen bezüglich der CSIRTs sind aus unserer Sicht sehr praktikabel. Zwei Punkte möchten wir jedoch noch anmerken:

Das CSIRT-Netzwerk definiert sich selbst eine Geschäftsordnung und kann einhergehend Treffen einberufen. Aktuell sind das 2-3 internationale Treffen im Jahr, zu denen maximal 2 Personen pro EU Mitgliedsstaat kommen können. Das ist zum aktuellen Entwurf des NIS-Gesetz kompatibel. Es wäre aber denkbar, dass sich im CSIRT-Netzwerk eine Arbeitsgruppe zum Thema „Sicherheit der Energieversorgung" bildet, zu deren Treffen dann die entsprechenden sektorspezifischen Teams eingeladen werden, um spezifische, sektorale Herausforderungen besser zu adressieren. Daher ist der Abs. 5 potentiell zu spezifisch, weil eben nicht alle Sitzungen des Netzwerkes sowohl für das nationale CERT wie auch das GovCERT gleich relevant sind. Wir sehen zwei Optionen, diese Unschärfe zu beheben:

a) den Nebensatz „und nehmen an dessen Sitzung teil." zu streichen (präferiert), oder
b) ihn genauer zu spezifizieren, etwa „und nehmen an dessen Vollversammlungen teil."

Es ergibt sich aus der NIS-Richtlinie auch, dass alle sektoralen Computer-Notfallteams Mitglieder im CSIRTs Network sind. Es kann daher zur Klarstellung sinnvoll sein, den Abs. 5 mit

„Das GovCERT, das nationale und alle sektorspezifischen Computer-Notfallteams sind Mitglieder des europäischen CSIRT-Netzwerks."

einzuleiten. Die aktuelle Geschäftsordnung des Netzwerkes sieht vor, dass genau ein CSIRT als primärer Ansprechpunkt für das Netzwerk nominiert werden sollte. Aktuell nimmt diese Rolle das nationale CERT (CERT.at) ein, es kann Sinn machen, diese Rolle für das nationale Computer-Notfallteam auch gesetzlich zu fixieren. Daher schlagen wir vor, § 12 Abs. 5 wie folgt zu ändern:

§ 12 Abs. 5 NEU nic.at/CERT Vorschlag Gesetzestext:

Das GovCERT, das nationale und alle sektorspezifischen Computer-Notfallteams sind Mitglieder des europäischen CSIRT-Netzwerks. Das GovCERT und das nationale Computer-Notfallteam informieren ohne unnötigen Aufschub die NIS-Büros über Aktivitäten des CSIRT-Netzwerks, die zur jeweiligen Aufgabenerfüllung erforderlich sind. Das nationale Computer-Notfallteam ist der österreichische Ansprechpartner des CSIRT-Netzwerks.

In Absatz 7 wäre eine klare Vorgabe hilfreich, wie lange (potentiell personenbezogene) Informationen zu Betroffenen, die im Rahmen von Abs. 6 (d.h. ohne direkten Kontakt/Auftrag des Betroffenen) gesammelt werden, gespeichert werden dürfen.

§ 20 Freiwillige Meldungen

Wir halten diesen Paragraphen zur Aufgabenerfüllung als essenziell, da wir über diesen Weg mehr Informationen für ein Lagebild erwarten als über die Pflichtmeldungen. Dieses Melderecht neben Störungen auch auf Risiken zu erweitern, würde den Prozess der „responsible disclosure" von Schwachstellen über die Computer-Notfallteams explizit erlauben. Weiteres ist eine genauere Angabe des zuständigen CSIRTs hilfreich und es sollte klarer erwähnt werden, dass diese Meldungen auch personenbezogenen Daten enthalten können.
:

§ 20 erster Teilsatz nic.at/CERT Vorschlag Gesetzestext:
Risiken und Störungen, die kein Sicherheitsvorfall (§ 3 Z 6) sind oder die Betreiber von nicht wesentlichen Diensten betreffen, können an das **jeweils zuständige sektorenspezifische oder an das nationale** Computer-Notfallteam gemeldet werden, das die Meldungen **anonymisiert und** zusammengefasst an den Bundesminister für Inneres weiterleitet; die Nennung der meldenden Einrichtung kann dabei auf ihr Verlangen entfallen. Die freiwillige Meldung kann Angaben zur Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zum Sektor des Betreibers sowie personenbezogene Daten enthalten. § 16 Abs. 3 letzter Satz gilt.

Fehlende Punkte

Die NIS-Richtlinie fordert in Artikel 9 (2):

> (2) Die Mitgliedstaaten gewährleisten, dass die CSIRTs mit angemessenen Ressourcen ausgestattet sind, damit sie ihre in Anhang I Nummer 2 aufgeführten Aufgaben wirksam erfüllen können.

Der vorliegende Text und die WFA sind hierzu nicht sehr aufschlussreich.

Die sektoralen Computer-Notfallteams werden aus dem Sektor selber finanziert, da dies aber nicht verpflichtend ist, liefert die WFA kein vollständiges Bild der wahren Kosten für die Wirtschaft.

Die Kosten für die erweiterten Aufgaben, die das GovCERT mit Inkrafttreten dieses Gesetzes übernehmen soll, sind in der WFA nicht ausreichend berücksichtigt. Im Vergleich mit den Anstrengungen anderer EU Mitgliedsstaaten ist die aktuelle Finanzierung des GovCERTs bei weitem nicht ausreichend, um dem steigenden Gefahrenpotential und den formalen Anforderungen durch die NIS-Richtlinie gerecht zu werden.

Für die Einrichtung und den Betrieb des nationalen Computer-Notfallteams (§ 12 Abs 1), bzw. den Ausbau des aktuell bestehenden nationalen CERTs sind in der WFA keinerlei Vorkehrungen getroffen worden. Dies gilt insbesondere für den Fall, dass neben dem bestehenden Austrian Energy CERT keine weiteren sektorspezifischen Computer-Notfallteams entstehen und folglich die Aufgaben vom nationalen Computer-Notfallteam übernommen werden müssen.

Die nic.at GmbH steht für etwaige Rückfragen natürlich zur Verfügung. Dem baldigen Erlass dieses Bundesgesetzes und einer Begutachtung der mit dem Gesetz in Verbindung stehenden Verordnungen blicken wir positiv entgegen.

Mit freundlichen Grüßen,

Robert Schischka
nic.at GmbH *Geschäftsführer*