the European association of
centr national internet domain registries

Brussels, 5 November 2013

SUBJECT: CENTR Opinion on the EU Network & Information Security Directive

Summary

CENTR members consider security as their top priority. As such, we welcome those parts of the Directive that focus on enabling a culture of security and trust: national strategies, national competent authorities, national CERTs and the cooperation network.

However**,** we would like to express our concern that the directive moves away from *enabling* the development of a security framework, in favour of a prescriptive, regulatory environment.

- The scope of the Directive is unduly broad and the lack of focus could place disproportionate demands on smaller market operators: Most EU ccTLDs are SMEs or not-for profit organisations. The approach should be defined by the nature of the incident.
- We would welcome more focus on capacity building and developing trust. We are concerned that the regulatory and compliance-based approach could undermine this.
- Mandatory reports should not be required until the incident has been resolved. More thought needs to be given to how to use reports to improve network and information security in the EU.
- Consideration should be given to auditing or certification against standards, bearing in mind the size of some of the market operators and the specialist support networks in place in the domain name sector.
- Delegated acts could lead to unforeseen consequences and should not be introduced without extensive consultation and proper assessment.

CENTR's Opinion on the Draft EU Network & Information Security Directive

a. CENTR Members' commitment to security

CENTR and its members **consider security being the top priority and essential for the trust their stakeholders – both** their sales network **and** the domain name holders – put in them. They all dedicate significant resources to maintain the security, stability and resilience of the domain name system (the DNS). As such, CENTR members support the objective of increasing the culture of security in the EU and, in particular, welcome the Directive's requirements for

- National network and information security strategies;
- The designation of national competent authorities;
- The development of CERTs; and
- The introduction of a cooperation network to facilitate best practice.

We believe that these initiatives will help promote the correct enabling environment for cyber-security in the EU.

Much of the work of CENTR is focused on developing trust to enable information sharing. There are three key functions at the heart of CENTR's approach:

i. Alerts: early warning of incidents: information is shared among peers.
ii. Support: help from community experts in addressing the problems.
iii. Analysis and sharing experience with the community following an incident.

CENTR has a Security Working group and its members share information and reporting between security & technical staff through CENTR mailing lists. A significant part of the main (CEO-level) meetings is spent on analysis of security issues: we recognise that security, stability and resilience have to be at the heart of the business.

Many CENTR members are active in other forums that allow sharing of information between peers and provide mutual support in the case of incidents: the domain name system is a unique environment and has maintained a strong sense of cooperation on a national and global scale. Forums with significant CENTR member engagement include:

- DNS-OARC (the DNS Operations, Analysis, and Research Center) brings key operators, suppliers of DNS technology, security system providers and researchers together on a trusted platform to coordinate responses to attacks and share information. Work includes measurement of traffic loads, performance and attack analysis and development of publicly available tools and services.
- The Internet Corporation for Assigned Names and Numbers, ICANN, (the private-sector organisation set up to coordinate the DNS) has a Security and Stability Advisory Committee that advises the wider DNS community on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational, administra-tive and registration matters. It engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services.
- Many EU registries either run or have close links to their national CERT or other critical national infrastructure coordination bodies.
- Many CENTR members are active contributors within RIPE (Réseaux IP Européens). RIPE and RIPE-NCC (the European registry for Internet Protocol addresses) also represent a strong community of EU infrastructure operators. This also has a strong community of mutual support, including working groups on abuse, DNS-related issues in technology and operations, and measurement analysis and tools. RIPE-NCC and other technical cooperation networks were able to provide support for the decision-making process during the cyber- attacks on Estonia in 2007.

b. Development of trust

It is not possible to regulate trust. Trust is based on mutual confidence and comes from cooperation between the government agencies and market operators, basing each organisation's assessment on the reliability of the other. CENTR members recognise the importance of developing trusted relationships: we need to demonstrate that we are credible partners. This is at the heart of achieving a national security culture to ensure effective and coordinated responses to security incidents.

Robust national environments to promote cyber-security depend on strong relationships between the national agencies and CERTs and the active engagement of market operators. Cooperation, both nationally and in the EU, needs to be based on two way engagement and information sharing between the national agencies and market operators. CENTR members are willing to engage in such cooperation.

Therefore, we are disappointed that the Directive does not focus on promoting risk-based cyber-security strategies and cooperation: developing capacity is the key to earning trust. A framework based on regulation and compliance with standards can undermine the culture of trust and cooperation that already exists.

c. Reporting requirements

We are concerned that mandatory reporting requirements could divert time and resources away from responding to any incident. The priority has to be to work with those parties most directly affected or who can assist in resolving the issue and/or in mitigating its effects. Formal reporting should be deferred until the incident is under control and remedial action has been implemented.

More thought should be given to how the reports can be used: collecting data for the sake of it is not useful and we should look more towards identifying lessons from incidents and at the evolution of attacks.

Systematic and continuous reporting after elaboration and analysis is a major part of the decision process for preventive actions. CENTR members share information about incidents (both successes and failures in responding to attacks) to learn from each other: reporting then has more tangible benefits for the community and helps lead to improving network and information security. It should be clear to the reporting organisation and to the rest of the community that they all benefit from the reporting process, and that it is not simply a naming-and-shaming exercise.

d. Standards and auditing

Security auditing against recognised standard such as the ISO 27000 family is an onerous process. The certification itself is only the part of a longer working process of the deployment of an information security management system. The standard is a tool to guide users through good practice. Some of the larger registries have obtained an ISO/IEC 27001 certification, or are well on the way to achieve it.

Certification provides evidence that security is embedded in the organisation's processes. However, most domain name registries are small organisations and the formal certification process itself is a substantial overhead on limited resources.

That is not to say that those smallest registries are less secure or less well prepared than the larger ones. They draw on expertise from their local community (many are based in universities or are well connected with main centres of expertise) and from CENTR and other networks. We strongly recommend appropriate consideration be given to other ways of verifying security capability than submitting to mandatory certification and auditing, which could impact the financial structure of the smallest registries.

In addition to the domain name registry, the domain name supply chain works through “registrars” – the domain-name sales channel. These registrars usually provide the DNS hosting, and are an integral part of the domain name routing system. There are several thousand registrars involved in the EU domain name market and the vast majority of these are small or even micro-businesses: requiring security auditing for all of these companies is disproportionate, especially as most of them do not provide services to critical applications.

Quite a number of the registries are working together with the registrars to raise the information security awareness through self-regulation and self-declaration, sometimes based on legally binding agreements.

e. Scope

The scope of the proposal is very broad. As previously noted, the lack of focus leads to a disproportionate impact on infrastructure operators, and in particular on the ccTLD registries and registrars. We would welcome an approach that is more clearly defined by the nature of the incident and of the network and information under attack. For example, we would expect critical infrastructure, networks supporting financial transactions and databases of personal data to be implemented with an all-round level of security, including using verified suppliers. Most of the smaller registrars and hosting companies would not be involved in these cases and could be excluded or subject to more balanced requirements.

f. Predictability

We are concerned that the draft Directive makes frequent reference to delegated acts. The domain name system in Europe is quite specialised. Delegated acts aimed at particular applications or sectors are not necessarily transferable. Delegated acts could have unintended consequences on other market operators (on the operation of the domain name system, for example) and such measures should be subject to careful analysis and proper consultation.

CENTR: the cooperation forum for European Internet domain name registries

CENTR is the European organisation of country-code Internet domain name registries (country-code top-level domain - ccTLD). A ccTLD registry is responsible for the administration of its country's country code on the Internet, such as .de for Germany, .es for Spain. The main task of a registry is twofold, providing the necessary platform to register the domain name – so that a domain name is unique in the world – and resolving the name – linking the domain name to an Internet Protocol address (IP address).

CENTR is the only association in Europe of this kind. Amongst our members we count all the 29 ccTLD registries in the European Union, those from Member States and the registry of the .eu top-level domain. The EU ccTLDs that are not agencies under the government or the national regulator all fit within the EU definition of SME.

EU ccTLD registries are generally not-for-profit organisations strongly rooted in their national community. They range in size from Germany (.de with over 15.5 million domain names) and the UK (.uk, with over 10 million) to Cyprus and Malta with fewer than twenty thousand registered domain names. Over half (16) of all the EU's ccTLDs each have under a million domain names. A similar range exists in terms of the number of registry staff with some registries employing over 100 FTE's working in a wide range of activities in the local Internet community, while in most countries the registry function is carried out by only few people.

The total of all EU ccTLD registrations is roughly half of the total sales of the major global player, .com, based in the US, which has a sizeable turnover in all EU Member States.

Further Information

If you would like further information about this CENTR's opinion or would like to discuss issues raised in this paper, please contact Peter van Roste, General Manager of CENTR on +32 2 627 55 50 or peter@centr.org