the European association of national internet domain registries

Brussels
20 February 2015

CENTR Board of Directors Statement
Directive on Network and Information Security (NIS) (COM (2013) 48)

CENTR understands that there are ongoing discussions about the draft NIS Directive at the level of the Council Working Party, which particularly focus on the definition of the scope of the NIS Directive. In this context, there seems to be considerations to explicitly include 'national domain name registries' and 'domain name system service providers', which had previously not been included in the European Commission's original proposal and the European Parliament's amendments. CENTR members are strongly committed to the principles of openness, resilience, stability and security of the internet and support the overarching objective of the NIS Directive to 'ensure a high common level of network and information security' as the basis of a secure and trustworthy digital environment.

With regards to the inclusion of additional market actors into the scope of the Directive, we would like to share the concerns of the CENTR community about including the domain name system in particular and call to take the following elements into account:

1. Maintain a level playing field among all the actors in the domain name system (DNS)
2. Sustain the diversity of the DNS ecosystem
3. Ensure that measures relating to risk management are appropriate and proportionate to the risk

1. Maintain a level playing field among all actors in the DNS

The domain name system (DNS) is organised hierarchically. The root servers contain information of the root zone, which contains both generic top-level domains (gTLDs, such as .com, .net) and country code top-level domains (ccTLDs, such as .be or .es). Registries run these TLDs and in most cases sell domains via agents (often referred to as registrars), which manage domains on behalf of their customers (registrants).

Current discussions seem to focus on the sole inclusion of ccTLD registries into the scope of the NIS Directive. It is important to take into consideration that this would lead to unfair competition among ccTLDs and gTLDs. As an example of a gTLD, .com comprises more than 100 million domain names worldwide and is operated by Verisign, a US-based company under US jurisdiction. In comparison, the largest European ccTLD is the German .de, which operates 15 million domain names, whereas Malta (.mt) operates just over 4,000.

In Europe, the market share of gTLDs, largely dominated by .com, often exceeds that of the national ccTLDs. This is the case, for instance, in Croatia, Cyprus, France, Ireland, Luxembourg and Spain. Despite their dominant market position, gTLDs would not need to comply with reporting obligations or security requirements. It should also be noted that geographic top-level domains, such as .berlin, .wales or .paris would not fall under the scope of such a Directive either.

Whereas the impact assessment accompanying the Directive did not include information on the costs related to the implementation of NIS requirements by DNS actors, it is rather unlikely that implementation will come without a cost. Such costs would possibly be reflected in the fee levels for domain name registrations and renewals of those actors covered by the Directive, while gTLDs would be able to avoid them and improve their market situation. The security risks, however, such as the inaccessibility or operational failure of websites, do not only apply to ccTLDs but also to gTLDs. This means that in some countries more than three quarters of all websites, which are not operated under a ccTLD, could still be subject to operational failure but the operator would not be required to report the incident.

On top of the DNS hierarchy is the root zone. Failure at this level would affect the whole DNS and not only one specific TLD zone. The root zone is managed by twelve organisations, out of which only two are based in the EU. Hence ten of them would not fall within the scope of the Directive.

2. Sustain the diversity of the DNS ecosystem

We understand that the Council Working Party is currently discussing the possibility of bringing 'name service providers' under the scope of the Directive. A clear explanation of who is meant by this should be provided. In most cases, this will be the registrar. However, it might as well be the registrant. There are thousands of registrars in Europe, of which only a few are large international companies and most are (micro-) SMEs that only manage a small client portfolio. Managing domain names on behalf of their customers is often only a small part of their activity next to other services, such as running name servers and providing hosting services. The number of registrars per ccTLD can vary considerably across countries: whereas some ccTLDs have only a few accredited registrars, others can have over 2,000 registrars. Including small registrars in particular within the scope of the Directive could have a considerable impact on the DNS ecosystem.

Heavy reporting and auditing requirements are likely to exceed the resources of many registrars and would push them out of the market. This could lead to market consolidation and less choice for consumers, but in order to diversify and control the risk, choice is essential. If, for example, a registrar is compromised, the consumer can easily transfer the same domain name to another registrar. There is no single point of failure and the risk of a security breach spreading to another registrar is practically inexistent. The risk of spreading to registry level is limited, as even if the system is hacked, the damage would only affect the domain name under management of the registrar and not the whole TLD zone.

3. Ensure that measures are appropriate and proportionate to the risk

The Directive remains vague about what type of incidents of 'critical impact' needs to be reported and what measures are considered 'appropriate'. The Directive refers to Member States ensuring that appropriate technical and organisational measures are taken and that binding instructions can be issued by the competent authorities. The Directive remains unclear as to the scope of so-called security audits.

The concerns of CENTR members with regards to excessive burden on *registrars* have been outlined above. In addition, however, it should be noted that within the European ccTLD landscape, some *registries* are very small and run by a small team. Excessive requirements on them both in terms of reporting and auditing will impose disproportionate pressure on their resources to the detriment not only of those using domains under their TLD and but also those providing and promoting local content and support to the local internet community.

CENTR members have long-standing experience and an exceptional track record in handling and reacting to incidents, as well as providing solutions and exchanging best practices with each other. Some European ccTLDs run a national Computer Emergency Response Team (CERT), others collaborate closely with them. Over the years, CENTR members have developed and refined systems and services to raise their security levels, which they promote across the community (such as DNSSEC or 'Anycast' services).

The success of mitigating incidents and cybersecurity threats lies in diversifying the response to risk and reducing the response time. This is the foundation of the highly resilient nature of the DNS. Therefore, CENTR members are advising against prescribing measures on risk and incident management, as this is likely to be linked to lengthy procedures and attempts to find a one-size-fits-all solution to incidents.

About ccTLDs

The ccTLD landscape in Europe is highly diverse, which is reflected in the different sizes of the organisations and their business models. The majority among ccTLDs is managed on a non-profit basis, others are in the private and public sector. They provide domain names to registrars or sometimes directly to registrants (end-consumer). They display a strong commitment to their local communities and the development of local content. Their success is highly related to the level of trust by their communities, including both registrars and registrants.

About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 52 full and 9 associate members – together, they are responsible for over 80% of all registered country code domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Notice of abstention
Please note that CENTR member Red.es (.es) abstains from supporting this Board of Directors statement.