SAFE – Security Alliance For Europe

Developing Europe's Network and Information Security framework, without impediments to the Digital Single Market

As the European Commission prepares its strategy to achieve "A Connected Digital Single Market", the Security Alliance for Europe (SAFE) would like to provide some thoughts on the impact the upcoming Network and Information Security (NIS) Directive may have on this objective.

SAFE, a coalition representing the ICT sector, welcomes the increased policy focus on network and information security in Europe and the steps taken to improve pan-European coordination regarding cybersecurity incidents. **However, we are concerned that the proposed NIS Directive from the Commission, if adopted in its current form would create significant barriers to the Digital Single Market instead of dismantling them.**

Ensuring a high level of network and information security is important

In Europe today, citizens, governments and businesses rely on a wide range of services, systems and assets to function effectively. Some of these infrastructures have become so vital that their incapacitation or destruction could have a debilitating effect on a country's economic or national security, public health or safety. If they are not adequately secured, they may be exposed to cyber threats and attacks, increasing the vulnerability of the entire system.

Cybersecurity has been a matter of good business practice for our industry for decades. Today, most EU Member States also recognise that working toward cybersecurity and cyber resilience – with particular focus on the protection of critical infrastructure – must be an important national priority.

However, as demonstrated by a study conducted by BSA | The Software Alliance, member of the SAFE Coalition [EU Cybersecurity Dashboard], considerable discrepancies exist between Member States' approaches, policies, legal frameworks and operational capabilities, creating notable cybersecurity gaps across the EU.

It is therefore important to achieve a more coherent approach and a common baseline level of cybersecurity across the EU, and the NIS Directive has the potential to support this objective.

NIS: a threat to the Digital Single Market?

Given the significant cybersecurity gap that exists today in Europe, it is essential that the Directive remains focused on those services and infrastructures that are truly critical to the functioning of the society and economy.

This also means that we should not extend the scope, purely for political reasons, to an open-ended list of services with little or no relevance to protecting the cybersecurity of Europe's critical infrastructures. In fact, the inclusion of certain subsectors does not reflect the dynamic nature of the digital environment at all, and hence misses the opportunity to come up with a future-proof and technology-neutral legislation.

By including Internet enablers, as suggested by the Commission, we would not only divert limited resources from the public and private sector without any gain to Europe's cyber resilience; it would also create a serious impediment to the Digital Single Market.

Already today, Member States take wide-ranging and divergent views to cybersecurity and this problem will only be made worse by an NIS Directive which prescribes that Member States pick and choose those services that are "essential" to the functioning of their society as well as tailoring the actual requirements which are directed towards these service providers.

Indeed, Article 2 of the proposed Directive emphasise that the rules outlined in the legislation represent a "minimum harmonisation", and amendments put forward in the Council only reinforce this.

What would this mean in practice? As Member States will be able to define the scope and design the rules independently from each other, only limited by a very loose definition of "operators", Internet enablers **will face a patchwork of different obligations**, where parts of their services will be covered in some Member States, different parts in others, and all of them will be subject to diverging and potentially conflicting legal requirements. This situation means that the business environment becomes more complicated for companies providing business-to-business solutions, with regard to overlaps and conflicts between Member State requirements.

Nothing in the Directive, as it stands today, would address these problems.

The text being negotiated in Council further compounds the issue by calling for lists of standards implementing the security requirements of covered operators to be determined at national level.

It is good practice for a covered operator to rely on globally accepted international standards to achieve the security objectives of the Directive. From that perspective, Member States should indeed encourage the use of globally recognised standards, as noted by the Council document.

However, it is important to avoid that Member States take different approaches. Rather than referencing the range of appropriate and mature international standards, the text only calls for so-called "internationally recognised standards". This opens up a path to a de facto requirement to implement a wide range of potentially conflicting national requirements. This would defeat the purpose of the Digital Single Market, and significantly add to cost and tie up security resources that would be better deployed on managing truly critical services and infrastructures.

The Commission should promote a common approach taken by Member States, while engaging in a dialogue with industry to ensure a successful and vibrant Digital Single Market.

The practical implication of these provisions would lead to a situation that is contrary to the stated objectives of the Digital Single market, i.e. to ensure that businesses offer services in any EU country easily. If faced with such legal uncertainty, would European cloud providers be inclined to offer services to operators in another country? Would cross-border e-commerce really strive in Europe, when providers can easily be subject to conflicting security requirements and contradictory binding instructions from authorities?

Solution

As the first ever legislation in the field of cybersecurity, the Network and Information Security Directive should focus on ensuring that operators providing truly essential services have appropriate network and information security measures in place.

Using the NIS Directive by to regulate Internet enablers in order to create a level-playing field will neither advance cybersecurity, not Europe's digital single market. There are better suited policy options which could be considered.

Improving network and information security is not a novel concept for our industry. On the contrary, providers of ICT products and services have been committed to securing the cyber ecosystem for many years – in some

cases for over a decade. The ICT industry is keenly aware that it must continue to play its part, and as such we will endeavour to share best practices, engage in voluntary exchanges of cybersecurity information and continue to implement relevant security measures across digital products and services to protect our customers. These efforts will ensure increased cyber resilience and a higher level of cyber security in Europe.

Contact information

BSA | The Software Alliance
Thomas Boué
Director, Policy – EMEA
thomasb@bsa.org
Tel: +32 (0)2 274 13 15
www.bsa.org

DIGITALEUROPE
Jean-Marc Leclerc
Director
JeanMarc.Leclerc@digitaleurope.org
Tel: +32 (0)2 609 53 10
http://www.digitaleurope.org

EDiMA
Siada El Ramly
Director General
siada@edima-eu.org
Tel: +32 (0)2 626 1990
www.europeandigitalmedia.org

EuroISPA - European Internet Services Providers Association
Eszter Bakó
Policy Executive
eszter@political-intelligence.com
Tel: +32 (0)2 550.41.14
www.euroispa.org

TechAmerica Europe powered by CompTIA
Christian Wagner
Senior Manager, Digital Economy
christian.wagner@techamerica.org
Tel: +32 (0)491 741 888
www.techamerica.org