



We are
Ireland online

Policy Advisory Committee

10th November 2022

Meeting - PAC#33

Policy Advisory Committee Agenda PAC #33

1. Membership Matters
2. Minutes from the PAC #32 meeting
3. Matters arising
 - *Domain Alert System to protect CI products with geographical origin and reputation*
 - *Agorateka portal – [EUIPO](#)*
4. Handling of online abuse which uses the .ie namespace
 - *4.1 illegality online (GNCCB protocol)*
 - *4.2 tech abuse (Netcraft stats)*
 - *4.3 Anti Abuse policy proposal (parked ?)*
5. NIS 2 update
6. AOB
7. Next Meeting



1. Membership Matters

- Please keep **microphones muted** throughout the call
- Please **“raise a hand”** to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
 - Recording will be deleted once the Minutes are approved by PAC

2. Minutes of the PAC #32 Meeting

- Meeting minutes are circulated to the membership promptly after each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on [weare.ie](https://www.weare.ie) after the comment period has ended
- Published online at <https://www.weare.ie/policy-development-process/>

3. Matters arising

- Domain Alert System (DIAS) to protect products with geographical origin and reputation:-
 - craft and industrial products (e.g Donegal Tweed)
 - wine, spirit drinks & agricultural products

*CIGIs - regulation on geographical indication protection
for craft and industrial products*

4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

Recap

- Agreement reached with the Garda National Cyber Crime Bureau (GNCCB)
- Common ground & Goodwill is substantial
- Key engagement at meeting on 10 March 2022 (esp. mutual understanding & due process)
- Agreement confirmed by email 17 May 2022 (circulated with Minutes)



4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

Action Items

- Publicity & Communications
- Regular Forum for GNCCB engagement :- invitation to Registrar Day
- Single points of contact (SPOCs)



4.2 Handling of technical abuse

Netcraft monitoring service

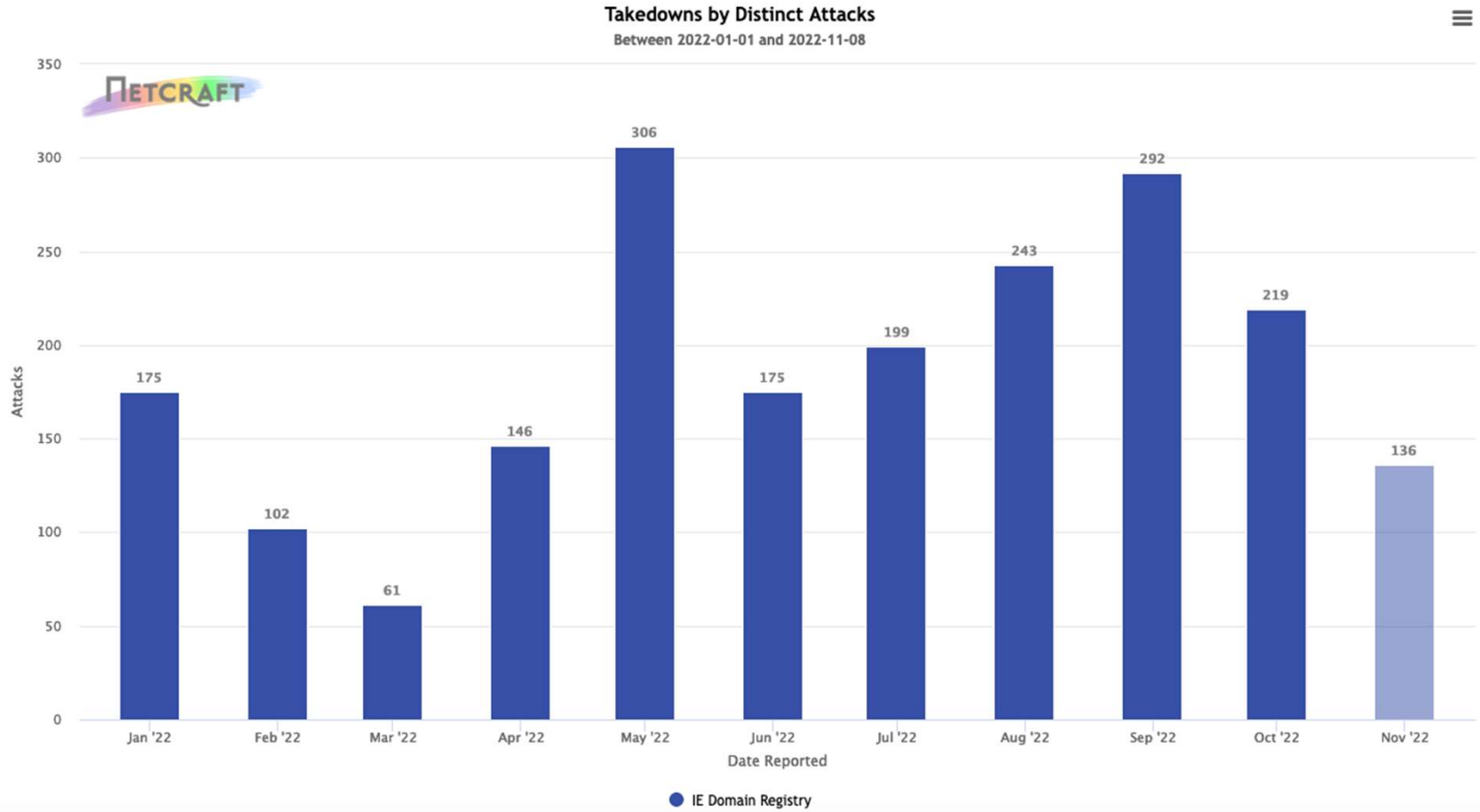
Recap

- Consensus from PAC members
- Service commenced March 2021
- Registrar's role
- Financed by .IE
- Benefits:
 - Proactively respond to technical abuse (e.g. malware, phishing or botnets)
 - Helps innocent victims (e.g. SMEs who might be unaware that they have experienced a cyber attack)
 - Notification allows them to take the required remediation action

4.2 Handling of technical abuse

Handling of online **Technical abuse:** use of Phishing, Malware, botnets etc...

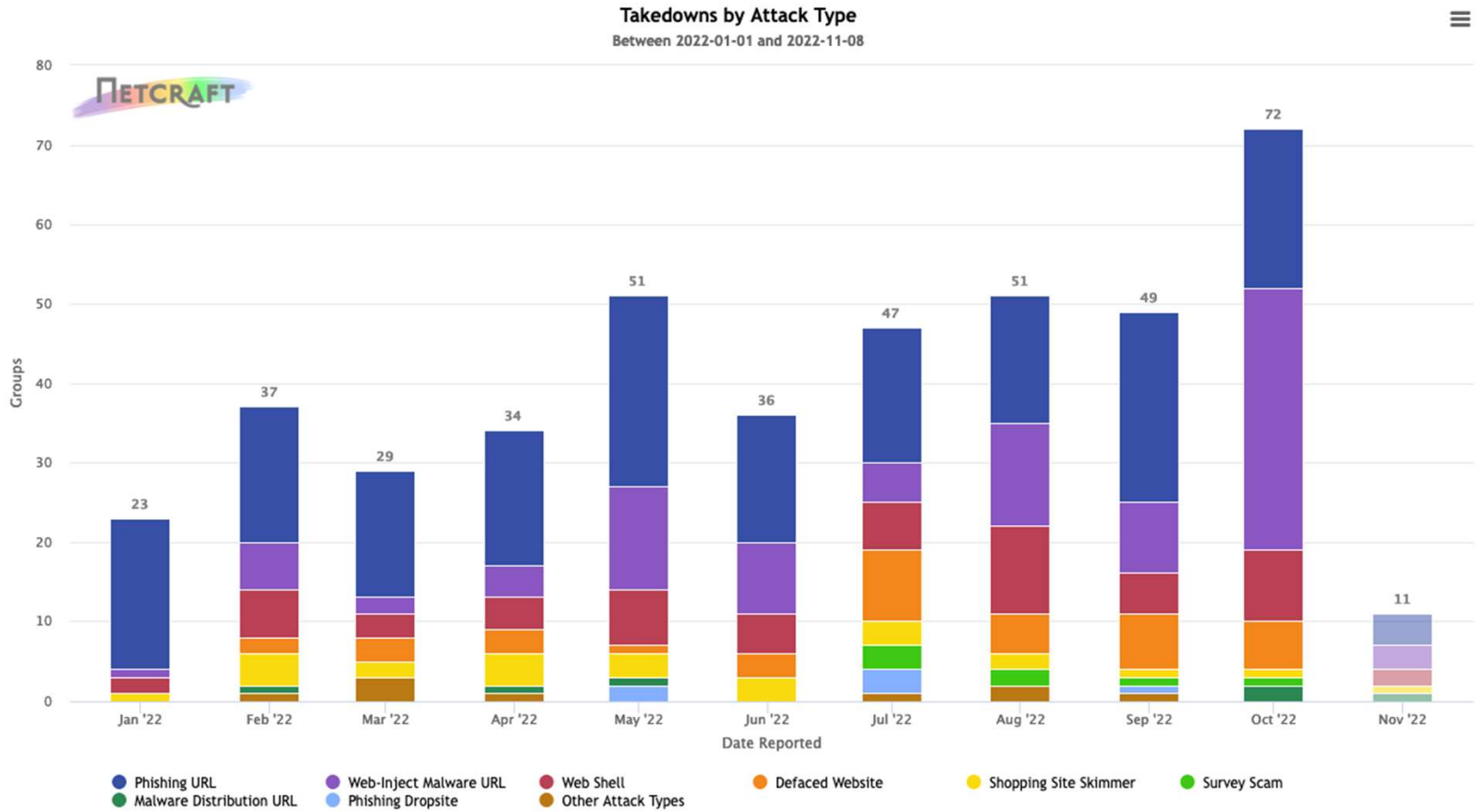
Netcraft service: 2,054 attacks Jan-'22 to Jul-'22



4.2 Handling of technical abuse

Handling of online **Technical abuse**:-
use of Phishing,
Malware, botnets etc

Netcraft service:-
440 takedowns
Jan-'22 to Jul-'22



4.2 Handling of technical abuse

Handling of online
Technical abuse:-
use of Phishing,
Malware, botnets etc

Netcraft service:-
2,054 attacks
Jan-'22 to Jul-'22

| Attack Type | ▼ Total Groups | Total Attacks | Total IP Addresses | Percentage of Attacks |
|----------------------------|----------------|---------------|--------------------|-----------------------|
| Phishing URL Q | 181 | 1120 | 107 | 43% |
| Web-Inject Malware URL Q | 96 | 172 | 62 | 22.8% |
| Web Shell Q | 59 | 446 | 47 | 14% |
| Defaced Website Q | 39 | 227 | 30 | 9.3% |
| Shopping Site Skimmer Q | 18 | 50 | 17 | 4.3% |
| Survey Scam Q | 7 | 10 | 5 | 1.7% |
| Phishing Dropsite Q | 6 | 11 | 4 | 1.4% |
| Malware Distribution URL Q | 6 | 6 | 6 | 1.4% |
| Other | 9 | 12 | 8 | 2.2% |

2,054

4.3 DNS Abuse – time for a formal .IE Policy ?

(more accurately ‘Abuse that uses the DNS’....)

Recap

- Proposal for new, formal .ie policy
- Rationale for an Anti-Abuse policy
- Context :- digitally transformed post-Covid world (malware, phishing, scams)
- EU* regulators attention
- Self-regulation provides confidence, builds trust through transparency
- ccTLDs may (eventually) follow gTLDs - obliged to have a policy

Discussion deferred

*The European Commission has just published its study on DNS abuse. The study assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures. The study proposes a **set of recommendations** in the field of **prevention, detection and mitigation** of DNS abuse.

4.3 DNS Abuse – time for a formal .IE Policy ?

| Policy change proposal / New Policy proposal | |
|--|--|
| 1 | Proposal Originator (<i>name: email: telephone: organisation</i>) David Curtin, CEO, .IE dcurtin@weare.ie |
| 2 | Date 26 th May 2022 |
| 3 | Policy Proposal Name: "Anti-Abuse policy" to handle abusive use(s) of .ie domain names |
| 4 | Policy Proposal type: <i>new, modify, or delete</i> New policy |
| 5 | <p>Purpose and benefits of the proposal :</p> <p><i>Please state the purpose of your proposal</i></p> <ul style="list-style-type: none"> ➤ The purpose of the proposal is to formalise the policy and process for handling mis-use of the DNS. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general, noting that abusive use includes the wrongful or excessive use of power, position or ability. <p><i>Please state the benefits of your proposal</i></p> <ul style="list-style-type: none"> ➤ The benefits of the proposal include the formalisation and transparency of .IE's current policy, process and procedures for handling technical abuse using the DNS ➤ Improves the confidence and trust of consumers, policy makers and of business in the .ie namespace. ➤ Such a policy may empower industry participants to proactively handle instances of abuse using the DNS:- <ul style="list-style-type: none"> ○ to protect the integrity and stability of the registry; ○ to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; ○ to avoid any liability, civil or criminal, on the part of .IE, as well as its officers, directors, and employees; ○ to comply with the terms of the registration agreement or |

| | |
|---|--|
| 6 | <p>Please indicate any perceived problems (issues you envisage)</p> <ul style="list-style-type: none"> ➤ Legal Powers ? – no national legislation (yet). Registry currently empowered by its own T&Cs. ➤ Best practice alignment ? – internationally many ccTLDs have not (yet) adopted a formal anti-abuse policy. gTLDs have contractual obligations with ICANN. ➤ Efficacy ? purpose is 'handling of...' not 'prevention of...' ➤ Stakeholder objection ? .IE does not envisage objections from the domain industry to the change of the policy per se, particularly as most channel partners & Registrars already react promptly to technical abuse, when notified. ➤ Uncertainty ? Anticipate transposition of imminent EU cyber security regulations |
| 7 | <p>Policy proposal grounds: <i>please indicate the reasons for your proposal (what is wrong/missing/inadequate etc. with the status quo?)</i></p> <ul style="list-style-type: none"> ➤ Abusive use(s) of domain names is currently handled within the Dispute Resolution Policy and procedures, and in particular by protocols with national regulatory agencies and similar bodies with legislative responsibilities. These protocols generally deal with illegality of content, not technical abuse arising from mis-use of the DNS. ➤ Current responses are reactive in nature |
| 8 | <p>Policy term proposal: <i>temporary, permanent, or renewable</i> Permanent</p> |
| 9 | <p>Policy statement/text:</p> <p><i>New Policy Text</i> None proposed at this time.</p> <p><i>Note that Section 3 of the Terms and Conditions of Registration may require amendment if there is stakeholder consensus on this policy change request.</i></p> |

5. NIS 2 – Role for the PAC ?

Update on developments since PAC#32 :-

- Timing / Trilogues / and linking DSA & CER Directives.
- 12 May – Final stage of Trilogue negotiations
- 17 June - EU Council published latest version of NIS 2 text
- Known as the 4-column doc (472 pages)

- Some positive proposed edits from the **Council** draft.....
- Impact Assessment required
 - Article 23 – “accurate and complete information, including verification procedures”
 - KYC is costly, resource heavy, and introduces friction in automated online processes
 - GDPR in Whois proposals - identifying “legal person” in .com TLD world
 - Data Access – to legitimate access seekers – lawful and duly justified requests
 - Member States have 21 months to transpose
 - Scope – registries, registrar **and** resellers – “entities providing registration services”
 - Member States shall “require” Vs shall “ensure”

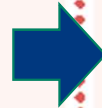
5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’



Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.



Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’

Action Items

- Action “**trigger**” is the publication in the EU Official Journal
- Legislation is c.21 month away, but **cyber threats** are here today
- **Awareness** building – “Just inform” via Newsletter, Blogs, Webinars, YouTube clips
 - *Audience* - RAR channel, SMEs in the Supply Chains, TDs & policy makers,
 - *Messaging* :- KYC is costly; Start now on cyber defences, think about ISO alignment 1st;
- Share **Impact Assessment** document – cyber benefits, regulatory cost burden, need for eID,
- **Lobby** letter - to those transposing into national legislation – do’s & dont’s; ask for early clarifications
- **Engagement** - Channel needs a clear legal framework (esp. re conflicts with GDPR provisions)
- Cyberthreats – how to improve **current** resilience and incident response capacities of critical service



5. NIS 2 – Role for the PAC ?

How can we make progress on ‘The Good’ Action Items



Cyber- Risk management

Regulatory Obligations: Risk management measures should include measures to identify, protect, detect, respond, recover.

FAQs

Q: My small Registrar business is ISO-aligned. Isn't that secure enough for the NIS2 register?
 A: No. Our impact assessment concludes that NIS2 is "high impact" on non-ISO aligned entities, because regulatory compliance is widely regarded as costly, resource intensive and administrative burdenome for SME companies (esp. providing audit evidence of controls).

Q: How do they expect NCSG, the "national competent authority" to regulate companies designated as "Essential Entities"?
 A: Not yet confirmed, but looking at NIS1 designated Operators of Essential Services (OES), we expect the NIS2 Framework will be used.

Q: What is the NIS2 cyber security framework (CSF) 7 to it like ISO certification?
 A: No, its benchmarking, not certification. The NIS2 CSF consists of the Framework Core, the Framework implementation Tier, and the Framework Profiles. The Core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover.

Q: I'm just a supplier. Why must my regulated customer take account of vulnerabilities specific to each supplier, per Article 18(3)?
 A: The rationale is helpfully provided in Recital 43 (see below, right).

Although voluntary and not intended to be an exhaustive checklist, the NIS2 framework covers five functions, being critical areas of cyberactivity:

- Identify: Identify looking at current data use and then evaluate and identify risk.
- Protect: Protect the elements that help protect a business.
- Detect: Detect being aware of problems as they happen.
- Respond: Respond the issues needing to be covered to make an adequate response to a problem.
- Recover: Recover the steps needed to make an effective recovery of lost data.

Here's an example of NIS2 in action.

Key Articles

- Article 18 (1) - Manage the risks - to prevent and minimise the IMPACT of incidents on recipients of their services. Take "appropriate" and "proportionate" measures.
- Article 18 (3) - must take an "all-hazards" approach to protect
- Article 18 (2) (a) - supply chain security - must take account of vulnerabilities specific to each supplier 18(3). The rationale is helpfully provided in Recital 43.
- Article 18 (4) - corrective measures required without undue delay - must be appropriate and proportionate.

Key Profiles (No. 43)

- Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security services and software vendors, is particularly important given the prevalence of incidents where entities have taken actions to attack against network and information systems and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services.
- Entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures.
- Entities should in particular be encouraged to incorporate cybersecurity measures into contractual arrangements with all their direct suppliers and service providers.
- Entities could consider cybersecurity risks stemming from other levels of suppliers and service providers.

Definitions -

- "TLDs" = top level domain registries. This includes .com in addition to national country codes (like .ie, .uk, etc).
- "SPRS" = entities providing domain name registration services.
- "Appropriate" and "proportionate" security measures must take due account of severity of exposure, size, likelihood of occurrence, severity and societal/economic impact. Measures will be technical, operational and organisational. Article 18(1)
- "All hazards" approach includes theft, fire, flood, telecoms failures as well as unauthorised physical access/damage and malicious actors.
- "NIS2" = One of the main ways in which businesses measure their preparedness in managing cyber-related security risks is to benchmark themselves against the Cybersecurity Framework developed by the NIST (National Institute of Standards and Technology, U.S. Department of Commerce).
- "Essential Entities" = includes Digital infrastructure (DP; DNS; Top Level Domain (TLD) registries; cloud; data centre service providers; CDN; trust service providers; electronic communications)
- "Important Entities" = include digital providers such as online marketplaces; search engines; and social networks.

NATIONAL CYBER SECURITY CENTRE

Proposed New Cybersecurity Directive (NIS 2.0)

NIS2 Fact Sheet
 for: Company Directors, Legal, Policy

Who's in Scope for NIS2 – Sectors & Size

Entities may be in scope directly (due to sector, size) or indirectly (as a relevant supplier to an in-scope entity)

Who am I in or out of scope?

Deciding which sectors are "Essential" or "Important". EU directives give EU countries some level of discretion in national circumstances.

Is the Scope?

Entities providing domain name registration services ("SPRS") means registrars and agents acting on behalf of TLDs or PRSs.

Entities providing domain name registration services, publicly available recursive domain name resolution services and authoritative domain name resolution services ("DNS")

And preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of our society's continuous and stable operation, on which the digital economy and society depend" (Recital 15)

Level of compliance for small companies?

Small companies are not within the scope of the NIS2 Directive (NIS2 Annex).

Are there a few EU countries. Which country's rules will apply to my company?

Extend the scope even further for you... "taking account of their cross-border nature, the DNS service providers, and entities providing domain name registration services, cloud computing service providers, data centre service providers, network providers, managed service providers, and managed security service providers should be subject to harmonisation at Union level. The implementation of cybersecurity measures should therefore be facilitated by an implementing act."

NIS2 Fact Sheet
 for: Registration staff, DPOs, Legal

Domains - Data Accuracy & access to Data (Article 23)

Regulatory Obligations: TLDs and EPRS* are obliged to collect and maintain accurate and complete* domain name registration data in a dedicated database. It must contain sufficient information to contact domain holders. Information / data requests from legitimate access seekers** must be responded to within 72 hours.

FAQs

Q: Are they really suggesting that EVERY domain holder needs to be validated, like a bank's KYC and money laundering (AML) process??
 A: Yes, unfortunately, despite intense lobbying and awareness building exercises by CENTR and by TLD policy advocates. New domain creation will need to be validated (in advance or in-post), also, the validated database must also be "accurate". The workload to retrospectively apply KYC will be immense... imagine DENIC, the German ccTLD with over 17m .de domains!

Q: Who will be responsible for these new KYC processes?
 A: The Directive, Article 23, imposes the obligation on both TLDs and entities providing domain name registration services (EPRS). However, it also states that duplication of accurate processes should be avoided...

Q: Is there a GDPR conflict with the obligation about sharing a contact's email address and their telephone numbers?
 A: Avoiding a collision with GDPR is intended by Recital 42. It says "provided that it does not contain any personal data. This can be achieved through various technical means, including the use of email aliases, functional accounts or similar systems."

Q: Article 23(3) refers to "verification procedures" what are those?
 A: That's unclear currently. However, NIS2 recital 41 "The TLD registries and the EPRS should adopt and implement "proportionate processes" to verify such registration data (Recital 41). Verification processes may be performed en masse or post (Recital 41).

Key Provisions

- Article 23 (1) - TLDs and EPRS are obliged to collect and maintain accurate and complete domain name registration data in a dedicated database.
- Recital 42 - "It must contain sufficient information to contact domain holders when there are allegations of illegal or other fraudulent activity or to help police and other law enforcement authorities to investigate and prosecute criminal offences, including verification procedures."
- Recital 43 - "It should provide specific domain name access seekers, within 72 hours of a request in compliance with Union data protection law."

Perspectives of IT PAC Register representatives -

- "Cost increases associated with NIS2 'accuracy' & transparency could be burdensome for many Registrars".
- "Make Register, Register Labels".
- "NIS2 will raise the standard of cyber security risk management for all Registrars. This is a fundamentally good thing - we should be doing this already".
- "It's important that Law Enforcement and IP lawyers can contact domain name holders when there are allegations of illegal or other fraudulent activity or to help police and other law enforcement authorities".
- "There is a need for more information. We will need to use the national legislation quickly, in order to prepare properly for NIS2 regulatory compliance".
- "Clear MTRs, ICR Media".

Accuracy

The topic is within the data accuracy remit of the PAC Register.

No definitions provided. The intention to ensure that domain holders & EPRSs* are contactable is register. This includes .com in addition to national country codes (like .ie, .uk, etc).

Domain Name Registration Services: includes Digital infrastructure (DP; DNS; Top Level Domain (TLD) registries; cloud; data centre service providers; CDNs; trust service providers; electronic communications); search engines; and social networks.

Entities in any legal or natural person making a request based on Union or national law. They include but are not limited to competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, national CERTs, or CSIRTs, (Recital 40).

Legitimate access seekers - any legal or natural person making a request based on the pre-registration checks built into the .IE Managed protocols in place to tackle DNS abuse (specifically criminality or harmful abuse which uses the DNS) of an EU act that let out the reasons for its operative provisions.

NIS 1 Extending the Scope as NIS1 is repealed ->-> NIS 2

Who is in the Scope of regulations?

- Digital infrastructure includes DP; DNS; Top Level Domain (TLD) registries; cloud; data centre service providers; CDNs; trust service providers; electronic communications; search engines; and social networks.
- Directive does not apply to root name servers (Recital 15)
- Entities sectors may be in scope because they are defined as "essential" or "important" entities.

with thanks to ggg for the image (left):
 https://www.dns-uk.com/2022/05/06/nis2-impact-on-dns-uk/

| | Financial | Operational | Reputational | Legal | Governance | Human Resources / Staffing |
|-----------------------------------|-----------|-------------|---------------|--------|------------|----------------------------|
| Data Accuracy Controls | Medium | Critical | Low | Low | Medium | Null |
| Data Access requests | Medium | Critical | High/Critical | High | High | Null |
| Cyber Risk | Medium | Critical | Medium | Medium | High | Medium |
| Digital Supply Chain Risk | Medium | Critical | Medium | High | High | Low |
| Know your customer controls (KYC) | High | Critical | Medium | Low | Low | Medium |

Definitions -

- "TLDs" = top level domain registries. This includes .com in addition to national country codes (like .ie, .uk, etc).
- "SPRS" = entities providing domain name registration services.
- "Essential Entities" = includes Digital infrastructure (DP; DNS; Top Level Domain (TLD) registries; cloud; data centre service providers; CDNs; trust service providers; electronic communications)
- "Important Entities" = include digital providers such as online marketplaces; search engines; and social networks.
- "Legitimate access seekers" = any legal or natural person making a request based on Union or national law. They include but are not limited to competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, national CERTs, or CSIRTs, (Recital 40).
- "Domain name registration data" = should include: the domain name, the date of registration, the registrant's name, email address, telephone number, as well as the email address and phone number of "the point of contact administering the domain name in case it is different from the registrant's".



6. AOB

7. Next Meeting

Proposed date:

February 2023