PAC
#30

IE Domain Registry CLG

trading as .IE

Policy Advisory Committee – PAC #30

Minutes – 24 February 2022 Meeting

.ie We are Ireland online

Table of Contents

Minutes of the PAC #30 Meeting held on 24 February 2022

Meeting Location: Hybrid meeting. Spencer Hotel, Dublin 1 for in-person attendees.
Meeting Time: Called to order at 11:00 am by the PAC Chair.
Members and representatives present:

Chair
CyberSafeKids
Department of Environment, Climate & Communications (DECC)
Department of Enterprise, Trade and Employment (DETE)
HEAnet
.ie Accredited Registrar (Blacknight)
.ie Accredited Registrar (Register Group)
.ie Accredited Registrar (MarkMonitor)
Irish Computer Society (ICS)
Irish Reporting & Information Security Service (IRISS)
IE Domain Registry CLG t/a .IE
Small Firms Association

1. Memberships Matters

Apologies – Members not present:

- Association of Patent and Trade Mark Attorneys (APTMA) – pre-arranged
- Enterprise Ireland – pre-arranged
- Law Society of Ireland – pre-arranged
- Internet Service Providers Association Ireland (ISPAI) – pre-arranged
- .ie Accredited Registrar (FCR Media) – pre-arranged

Change of membership.
There will be a new representative from the Association of Patent and Trade Mark Attorneys at the next meeting.

2. Minutes from the PAC #29 meeting

As there were no requested edits from members, the Chair confirmed that the Minutes from the 11 November 2021 PAC #29 meeting will be published online following the meeting (available here http://www.iedr.ie/policy-development-process/). Accordingly, the minutes will be digitally signed by the Chair.

The Chair reminded the PAC that the draft Minutes of today's meeting will be circulated to the membership following the meeting.

3. Matters arising

3.1 Technical abuse – Netcraft experience so far

The Registry confirmed that the Netcraft service will be renewed on 1 March 2022, following the negotiation of contractual terms and conditions with Netcraft, and confirmed that costs will be paid by .IE.

The reason the service is in place is so that collectively we can help innocent victims of technical abuse, to find out if their websites were impacted, and do what we can to assist them in removing the harmful software. Registrars are the key success factors in this work.

The .IE Chief Information Officer (CIO) updated the PAC on the latest metrics and some of the positive feedback we have received about the service. Registrants have been happy to receive notifications relating to their customers' websites that have fake shopping sites, skimming and phishing URLs.

They explained that there was a spike in web shell attacks in Q1 last year but they are now averaging at 25 attacks per month.

The Registry concluded by saying that there have been 376 notifications since March 2021 with 1,617 attacks handled. This is not that many considering that there are over 330,000 domain names in the database, but it's not insignificant, either. Collectively, Registrars are acting on the service alerts from Netcraft and therefore have been able to help 376 potential victims, mainly small businesses, to identify potentially harmful issues that they may not have been aware of.

4. Handling of online abuse which uses the .ie namespace

4.1 Criminal abuse - illegality online.

The registry provided a brief recap of the discussions and deliberations to date on the issue. The main action item was to agree the text of a Suspension Request Protocol document with the Garda National Cyber Crime Bureau (GNCCB). Feedback from PAC members at PAC #29 was reflected in an updated draft. This was circulated on 29 November. There were no additional requested edits from members so it was shared with the GNCCB.

The Registry confirmed that there is a lot of common ground and goodwill with the GNCCB. To move things along, it was agreed that rather than trying to establish a single point of contact (SPOC) with all 5 Garda agencies, it would be better to proceed with developing a Suspension Request Protocol document template with the GNCCB which can be used in due course to engage with the other four agencies.

The next step is for the Registry, the Registrar PAC representatives, the Detective Sergeant and Superintendent to meet to work through the Suspension Request Protocol document. The Registry plans to meet in person next week with An Garda Síochána (AGS) with the option for others to meet in person or remotely.

Some of the points raised at PAC #29 were covered:

- The Registrar is the intended first point of contact but the protocol document refers to hosting providers as the first point of contact, inferring that they are the same, which they are not. The default position is to contact the Registrar, then the Registry and if the Registrar isn't the Hoster, the protocol will accommodate getting the Hoster involved. There was an acknowledgement that if the Hoster is uncooperative or it's outside of the jurisdiction, the Registry can take action.
- The default position is that the registrant will be informed but a provision has been included for exceptional circumstances to allow AGS to ask for the registrant not to be informed. The basis for refusal and the basis for Registrar opt-out must be given.
- The domain cannot be left suspended indefinitely. There should be a time limit on how long a domain can be suspended. The protocol text should require a renewal of the request after a period of time. A suspension period of 90 days has now been included.

Some of the points raised by PAC members are outlined below:

- A Registrar representative noted that there needs to be engagement with other non-PAC Registrars on this topic.
- There wasn't a lot of notice given for the GNCCBmeeting which makes it difficult for Registrars to attend. The Chair acknowledged this but outlined that we have been waiting for some time for this level of engagement and we need to move forward with the meeting.

4.2 Potential for an Anti-Abuse Policy

The theme for this agenda item - is it time for the Registry to introduce a formal Anti-Abuse policy?

The rationale for an Anti-Abuse policy: is-

- The exponential increase in malware, phishing, scams in a digitally transformed post-Covid world
- The scams are a high-profile topic on popular radio talk shows and on social media.
- EU* regulators' attention

- Self-regulation provides confidence, builds trust through transparency
- Channel is mature & responsible & cares about Consumer Protection
- Formalises our position (we are in a good place; managed registry model; Netcraft service)
- ccTLDs will (eventually) follow gTLDs - obliged to have a policy

*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.

The Registry put forward the rationale and opened it for discussion, emphasising that the registry and channel partners are not legally responsible for content per se.

The Chair led the ensuing discussion where the following points were made:

- A Registrar representative noted that:
  - There are provisions made for this in the existing Registrar agreement and the Registry needs to ensure that they are implementing the existing clauses.
  - The Registry cannot make the policy too prescriptive as it may hamper their ability to do anything.
  - Other gTLDs have policies on this. Some feel they go too far and some feel they don't go far enough so perhaps we should avoid using those as a template.
  - The policy should focus on things like infrastructure, the DNS abuse framework and the Internet jurisdiction project rather than coming up with something formulaic.

- The Registry clarified that any policy change would follow the usual 10 step process (PDP).

- Another Registrar representative noted that:
  - It's a good time to explore if a policy is needed. If it is, what should it look like and when is the best time to implement it.
  - Legislation is expected. When it comes to legislation it will be black and white and any policy will need to be the same. It has to be narrow and explicit. If you start getting into nuances, it becomes difficult.
  - If we can get a first draft policy implemented it can evolve.

The Chair probed what other ccTLDs are doing on this topic - is there a pan-European effort? The Registry confirmed that other Registries, like Nominet in the UK, has a policy on engaging with law enforcement which is essentially their abuse policy. The European Commission has engaged consultants to write a document on DNS abuse based on comprehensive engagement with stakeholders. The study, which has just been published, assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures. It proposed a set of recommendations in the field of prevention, detection and mitigation of DNS abuse addressed to DNS operators (TLD registries, registrars, resellers and hosting providers, depending on their role in the DNS chain) but also to international, national and EU institutions and coordination bodies.

One Registrar representative noted that:

- The European Commission is driving a broader digital policy.
- A lot of the focus has been on IP interests. There hasn't been much engagement with civil society so they're seeing a lot of IP focused stuff like DNS abuse, counterfeiting, malicious marketing places and dealing with online terrorism.
- From a ccTLD perspective, CENTR is engaged with the Commission.
- .IE is an Irish company and subject to Irish law. The scope of the policy needs to be narrow and focus on technical aspects. They do not want the Registry to open themselves up to becoming the Internet police.

Another Registrar representative reiterated that we cannot cover every nuance and we should look at the simplest starting point with a view to it evolving.

The Chair and the Registry concluded that the starting point is defining the scope of the policy, possibly through a working group. There isn't any issue with the integrity and stability in the Registry or with adhering to laws and government rules but it needs to avoid liability, ensure compliance with the terms and conditions of the Registrar agreement and provide for timely correction of mistakes that are made.

So the next step is for the Registry to create and circulate a PDP New Policy Template to clarify the intention of the policy proposal, with a view to creating a working group at the next meeting.

5. NIS 2.0 – Role for the PAC?

In its recap, the registry noted that a quote from Dani Michaux, EMA Cyber Leader at KPMG Ireland captured where we currently are with NIS 2.0.

> *"All businesses are increasingly dependent on third-party services - from major cloud providers, through the ecosystem of software as a service (SaaS) providers and managed service providers, to a new world of data and analytics service providers.*
>
> *In the old days, our IT was on-premises, defended by firewalls and barriers, under our control and our management. This model is dead, and with it comes a raft of new digital infrastructure providers that we depend on for hosting, for platform and for service provision.*
>
> *NIS is being revised to reflect this reality."*

The Registry noted that there is a range of new digital infrastructure providers that businesses and individuals are now dependent upon for their outsourced platforms and services. NIS 2.0 has been revised to reflect this reality and reliance. While the overarching cyber security objectives of NIS 2.0 are positive and deserve to be supported, there are several problematic issues with the text, as currently drafted.

The current NIS 2.0 text contains specific proposals for data accuracy and completeness in the 'Databases of domain names and registration data', set out in Article 23. It became apparent that there is a need for clarification and additional information on matters such as:-

- what is the meaning of "accurate" and "complete" and "verification" in relation to domain name registration data,
- who are the proposed "legitimate access seekers" who need to be provided with access to specific domain name registration data,

So what has happened since the last PAC meeting in November? One of the issues that the channel has is around data "verification". The EC Council has as issued a response to the draft and is proposing to take out the word verified. Other suggested edits include reducing the perceived conflict with GDPR in proposals affecting WHOIS disclosures and data access – to legitimate access seekers and that Member States would have 24 months to transpose (not 18 months, per Commission's proposal). This shows that the Council is listening to Registrar representatives and industry bodies such as Centr. It has to go back to the European Parliament and there may be further dialogue during the negotiation phases. There may still be issues with the European Parliament as the three committees seem determined to have verification text included.

The Chair concluded that verification of domain holder ID is the main stumbling block at this point. The Registry confirmed that verification and the level of detail that needs to be disclosed are the main stumbling blocks. The level of detail that needs to be disclosed appears to conflict with GDPR. The level of data that's being asked to be accumulated and published, does appear to be at odds with many of the provisions of GDPR, particularly those around purpose limitation and personal identifiable information (PII). The detail includes email addresses, contact details and physical addresses.

The French Presidency of the Council of the European Union aims to achieve significant progress on important files many of which impact ccTLDs. It has announced that it intends to accelerate negotiations with the European Parliament and the European Commission ('trilogues') on the Digital Services Act (DSA) as well as on the NIS 2 and Critical Entities Directive (CER) Directives targeting a conclusion before the national elections in April 2022. It's proposing to link the DSA and the CER.

One Registrar representative noted that:

- .IE has never disclosed contact details in its WHOIS.
- Therefore, the impact of something like this would be greater for .IE than other Registries (including Verisign re .com domains) that do disclose this type of information.
- The language that has been removed may get put back in at a later date.
- The French view of digital is at odds with others – they are pushing an EU Digital Sovereignty concept.

The Chair concluded that we are currently in 'wait and see' mode with NIS2 and pondered what action the PAC can take to move things along. The Registry suggested that there are a lot of good things in NIS2. It's two years away but cyber threats are here today. Should we be waiting for it or should we start implementing some cyber defence elements of it now? PAC members have suggested that there is an awareness-building phase which the Registry agreed should start straight away. The audience for this is primarily smaller Registrars, SMEs in the ICT space, TDs and policymakers.

A newsletter is the first step. From a content perspective, the PAC Registrar representatives can support smaller Registrars in terms of guidance on best practices, good cyber etiquette and good security hygiene. The PAC lawyers can support on issues like GDPR. The Irish Reporting & Information Security Service (IRISS) might have some training materials for SMEs.

The NCSC has a big job to break down the NIS2 requirements into an easily digestible format for ordinary people.

One of the Registrar representatives brought up a point about engaging with the wider Registrar community. They feel that emails and newsletters may be forgotten and a member forum or portal could be more useful. This allows people to access the information at a time that is suitable to them. The DeskPro ticketing system that .IE use was suggested as a platform for hosting this forum. The Registry noted that it has relationships with the Small Firms Association and Retail Excellence and could give its members access to a forum to educate them.

The Chair queried what awareness of NIS2 currently exists in the wider community. The Registry, for the most part, doesn’t deal directly with the general public so feels Registrars are better equipped to answer this. One of the Registrar representatives suggested that awareness amongst the general public is close to zero. They also expressed concerns about very small Registrars being burdened with processing, storing, validating and verifying a lot of personal information. They concluded that the additional regulation in the current draft will make domains harder to register therefore driving businesses and people to platforms like Facebook, Instagram and YouTube.

The Chair queried where we go from here. The Registry agreed that awareness amongst the general public is low but the initial focus should be on educating Registrars and SMEs. We can use the likes of Black Friday, Cyber Monday, Cyber Security Day, Safer Internet Day etc. to push the message out to the general public. Further down the line, part of the awareness building will be reassuring citizens that this is not pushing back on GDPR. We also need to liaise with the security industry to see what we can do to help to improve the current cyber resilience, rather than waiting for two years for NIS2 to be in place.

The Chair suggested that the Registry has always been strong at creating and amplifying substantive content. This expertise can be used to help build awareness around NIS2.

To conclude, the Registry suggested doing an impact assessment and creating a formal document for the Irish audience. Other European countries will be more prepared for ID verification as they have electronic IDs and National Identity cards. A lobbying letter was also suggested - to ensure that local conditions are reflected during transposition of the Directive. This is something that can be created by the PAC so that concerned businesses can pass on to their local representatives around the time that the draft proposed legislation is passing through the legislative process.

6. Any Other Business

4.3 Registrar issue

Team.blue has a domain registration issue that has occurred 3 times recently. When a customer applies for a domain name, if the customer connection to Ireland does not auto-validate, they have 27 days to send in supporting documents. If they apply for a 2nd domain name while the other application is pending it is added to the same customer contact id. The timeframe for validation of the 2nd application is not extended and remains 27 days from the date of the 1st application. If validation hasn't occurred within 27 days from 1st application, all domain names associated with that un-validated contact in TITAN will be moved to PendingDelete status and deleted 5 days later. Team.blue's issue is that the 2nd domain isn't getting the full 27 days to validate. They feel that the 27-day timeframe within the .ie domain name life cycle refers to time allowed for validation of the domain name, not the contact ID.

The Registry confirmed that the system is designed to increase automation and ensure that the domain applications from returning customers are auto-validated. It accepts team.blue's point about validating the domain and has agreed to work with the software vendor to see if we can give the 2nd domain application the full 27 days.

Following discussion, the Chair concluded that this was an operational issue and should be resolved between the parties outside of the PAC.

4.4 Critical Entities resilience (CER) Directive

This was covered in earlier discussions.

7. Next Meeting

The provisional date for the next PAC #31 meeting has been set for Thursday 26th May 2022.