PAC
#29

IE Domain Registry CLG

trading as .IE

Policy Advisory Committee – PAC #29

Minutes - 11 November 2021 Meeting

We are
Ireland online

Table of Contents

Minutes of the PAC #29 Meeting held on 11 November 2021

Meeting Location: Virtual meeting.
Meeting Time: Called to order at 11:00 am by the PAC Chair.
Members and representatives present:

Chair
CyberSafeKids
Department of Communications, Climate Action & Environment (DCCAE)
Department of Enterprise, Trade and Employment (DBEI)
HEAnet
.ie Accredited Registrar (Blacknight)
.ie Accredited Registrar (Register Group)
.ie Accredited Registrar (MarkMonitor)
.ie Accredited Registrar (FCR Media)
Irish Computer Society (ICS)
Irish Reporting & Information Security Service (IRISS)
IE Domain Registry CLG t/a .IE ("The Registry")

1. Memberships Matters

Apologies – Members not present:

- Small Firms Association – pre-arranged
- 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

2. Minutes from the 15 July 2021 PAC #28 meeting

As there were no requested edits from members, the Chair confirmed that the Minutes from the PAC #28 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 Policy change request – re compulsory VAT for business registrants

This was submitted by a member of the public, who requested a policy change to make sure that all companies registering .ie domains outside of Ireland had a VAT relationship with, or was VAT registered in, Ireland They want to address the perceived issue of International .ie websites appearing as if they're based in Ireland. They thought this was misleading people and asked for a policy change to make sure that every business registration had a VAT relationship with or was VAT registered in Ireland. Following a discussion, there was consensus that this request be rejected. The matter is now closed will not go any further.

3.2 Digital Services Act

The registry stated that there are no further updates since the last meeting, when Polina Malaja, a Policy Advisor at CENTR, brought the PAC up to date on European engagements on the matter. Since then it has continued to progress through European Parliament discussions. It is expected that the proposals will enter Trilogue in early 2022. This is where the Parliament, Commission and Council engage and negotiate through their respective positions in order to reach a consensus on the final text of the legislation.

The Registry explained that there is a liability limitation for intermediaries and infrastructure providers. A member commented that the ‘Know your Business Customer’ (KYBC) was also a major element of the proposals. At the moment, it’s implied that infrastructure providers don't have liability for content but it isn't specific in the draft. Industry insiders are concerned about that and are campaigning to have it stated explicitly so it's clear that we are ‘mere conduits’ and that we don't have liability for content transitioning through our networks or digital service platforms.

3.3 Technical abuse – Netcraft experience so far

The registry reminded members that the Netcraft service launched on 1st March, following the negotiation of contractual terms and conditions with Netcraft, and confirmed that costs for the initial period would 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 described some of the most common issues that have arisen, such as attacks on remote access servers. These attacks have increased on the back of people working from home. The important point is that Netcraft monitors are spotting red flags early and identifying fake shopping sites, skimming and web shells.

The Chair asked the .IE CIO to explain web shells in layman’s terms for the wider group. He explained that during a web shell attack, a cybercriminal injects a malicious file into a target web server's directory and then executes that file from their web browser. After launching a successful web shell attack, cybercriminals could gain access to sensitive resources, recruit the target system into a botnet, or create pathways for malware or ransomware injections The .IE CIO gave the example of the attack which targets Microsoft Exchange Servers. What made the web shell particularly venomous was that the backdoor it established into the infected system remained, even after the server vulnerability was patched.

A representative of the accredited Registrars asked what the feedback has been like from registrars/SMEs receiving the reports? The .IE CIO confirmed that after some initial confusion, manly in week 1 after launch, over the wording of some of the emails (which were subsequently fixed), the feedback has been positive. Registrars and web developers are happy to be made aware of issues impacting their customers.

Another PAC representative asked if there were any trends in the issues arising. For example, when a web developer uses a particular template, if one client gets compromised, are they all compromised? The registry agreed to ask Netcraft for additional insights and revert to members at the next meeting.

The Registry concluded by saying that there have been 309 attacks since March 2021. This is not that many considering that there are over 325,000 domain names in the database, but it's not insignificant, either. Collectively, registrars acting on the service alerts from Netcraft have been able to help 309 small businesses 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 develop a Suspension Request Protocol document with the Garda National Cyber Crime Bureau (GNCCB).

The Registry confirmed that there is a lot of common ground and goodwill with the GNCCB. Since the last meeting, there have been approx. 6 engagements between the Registry and the GNCCB and there have been 2/3 updates of the protocol. These edits have been circulated to PAC members. It has also been escalated to a superintendent in An Garda Síochána (AGS) for consideration and formal approval, which is not at all guaranteed.

The list of remaining matters needing agreement from the Registry's point of view is as follows:

1. Single point of contact (SPOC)
2. Sequence of engagement
3. Informing the registrant, being the default comms principle
4. The basis for refusal to suspend
5. The basis for Registrar opt-out
6. Timing of requests – re stage of AGS investigation
7. Protocol – TBC – potential extension to MoU or Cooperation Agreement

A SPOC in AGS was suggested because the channel didn't want to have to engage with Garda members throughout the country. At the last PAC meeting it was suggested that multiple points of contact might ultimately be necessary. This was raised with GNCCB, who agreed, and suggested five:- Cybercrime Unit (GNCCB), the Economic Crime Unit (GNECB), the Criminal Assets Bureau (CAB) and the Organized Crime Unit (GNDOCB). If this could be achieved in the medium term, its not a bad outcome. If we can finalise the current protocol with the Cybercrime unit, we can use the template to engage with the other four agencies.

The next item is the sequence of engagement – who do AGS contact first? Substantial progress has been made in the current draft of the protocol, where it's the registrar first, and then the registry. (AGS has accepted that Registrars must be involved, so that content does not remain reachable from IP addresses, when a domain is suspended). AGS has intimated that, in some instances, they would prefer not to have to engage with certain Registrars. In addition, for operational reasons, in some instances they would prefer not to contact the registrant - organised crime investigations were referenced.

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

- A Registrar representative noted that:
  - 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. This needs to be clarified.
  - AGS need the cooperation of Registrars because the only email address available publicly for a domain name is the abuse contact for the Registrar.
  - Regarding AGS bypassing certain Registrars - if a domain name is removed from the DNS, a Registrar will see it and will most likely contact the registrant. So unless AGS do something to prevent Registrars from contacting registrants, Registrars could contact the registrant without knowing AGS has operational reasons for not doing so. Therefore, Registrars should not be by-passed.
  - If there's a problem with certain Registrars that AGS feel are somehow involved in criminal activity, then surely that's a matter that needs to be raised with the Registry as a matter of urgency, concerning their ongoing continuation as a Registrar.
- The representative from the ICS noted that:
  - We need to factor into the protocol that a national agreement may be extended to work internationally, or at least in Northern Ireland and the rest of the UK. Is this the intention ?
  - If AGS are to sidestep a Registrar, a formal process needs to be put in place. This cannot be done on a casual basis.
  - Concerning a SPOC – we need to tease out whether this will work. Does it mean that if another member of AGS (who isn't the SPOC) submits a request, it's rejected by Registrars/registry? In Romania, this is against the law. Any Law Enforcement Officer can submit a request whereas, in the UK, a SPOC works and is the most efficient way to coordinate.

  - It was noted that the SPOC can lead to higher quality submissions that are faster to process. The experience in the UK is that as a result of a SPOC having oversight of all the requests, they get to understand the size of requests, the types of requests, the complexity of the requests and they were able to weed out the ones that were not properly founded.
- The representative from HEAnet noted a concern about the feeling that we cannot say no to an AGS request. If a protocol is being put in place, it should be adhered to. If a request comes from outside of the SPOC, it should be directed to the SPOC. We should have the ability in the protocol to say no to requests that come from outside the SPOC.
- Training should be provided on the protocol for staff and for the SPOC.
- The domain cannot be left suspended indefinitely. There should be a time limit on how long a domain can be suspended for. The protocol text should require a renewal of the request after a period of time.
- A Registrar representative noted that in the UK, Registrars get suspension requests from the Registry and the Police. They are treated very differently. When they come to UK's Registrars from the Registry (mainly City of London Police requests to the registry) the registrant is informed and it works brilliantly. In cases where the registrant is not informed, they normally come from the Police directly to the Registrar. There is a process in place, so the Police must have the right documentation or it's rejected. For the .IE protocol, if an ongoing investigation relates to the content and not the domain, registry/Registrars should not get involved unless the Police can justify an immediate suspension.
- The issue of who pays for the domain if the suspension goes beyond the renewal date was raised. One of the Registrar representatives said they or their client should not have to pay for a domain that is suspended. On the .IE TITAN systems, the domain also needs to be associated with a Registrar, so how is that going to work?
- It was suggested by one of the Registrar representatives that if a Registrar spots an issue with a domain, that a facility should be put in place that allows them to suspend a domain without intervention from a Law Enforcement Agency. This would only be done on grounds where the issue is clear and obvious and they are confident that criminal activity has or will take place.
- Concerning the above, another Registrar representative noted that .IE's TITAN system allows a Registrar to put a domain in Client Hold – this removes the domain from the zone almost instantly.

In response .IE confirmed it will look at the terminology used around Registrars and hosting providers in the protocol. This discussion did raise an interesting point - what happens if the Registrar is based in Ireland and the hoster is based outside of Ireland, especially a hoster that isn't cooperating or is known not to cooperate? In this scenario, the website content will still be reachable at the IP address, even though the .ie domain is deleted. The Registry will raise this point with the GNCCB.

The Registry noted, in relation to GNCCB by-passing certain Registrars - it would be bad faith to do this in terms of disagreements, because that's not what the protocol text is intended to address. The bypass condition was definitely intended to be for criminal/legal reasons. It certainly wasn't anything to do with a Registrar being un-cooperative or cantankerous in the past.

The Registry noted the language needs to be tightened up in the protocol for specific issues related to the criminality in question. The Registry will also consider the question of its international application. The issue of who pays for a renewal arising during the suspension period will be factored into the protocol.

Regarding submissions from individual Gardaí, the Registry's objective is to point them in the direction of the SPOC. If refused, the Registry would nevertheless accept their submission and consider it on its merits.

The Registry noted that it has regulatory protocols in place with other regulators like the Central Bank and , HPRA and they work extremely well. The Central Bank will send a request concerning a website that they have an issue with, they specify the legislation, they tell us what action they want to take, indicate their powers under that legislation - then we can take action.
It's the same with HPRA, concerning medicines that are being sold online that are illegal. That protocol, for instance, provides for a scenario where maybe one medicine is illegal, out of maybe hundreds for sale. That protocol allows us to engage with the registrar and the registrant. Generally, the registrant removes the offending medicine from the website, and HPRA closes the case without the need for a suspension of the domain. These processes are streamlined now and that's what we want to work towards with this protocol with GNCCB.

Suggested next steps were that the Registry would update the protocol based on today's conversations. The updated version will be shared with the PAC to get their feedback and a follow-up call with interested parties can be arranged before the document is shared with the GNCCB. The ultimate objective is that we will have a protocol document that the Registry and Registrars can sign-up to (or opt-out of).

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 are 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 objectives of NIS 2.0 are positive and deserve to be supported, there are a number of problematic issues with the text, as currently drafted.

NIS 2.0 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" 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,

One of the issues that the channel has is around data verification. That brings to the fore issues around compliance costs, knowing your business customer (KYBC), the practicality of verification, handling of forgeries - who are the experts in saying whether a passport scan or photocopy is real or not. Certificate verification is an enormous issue as we don't have the e-ID in Ireland, in common with others in the EU 27.

Data Access is also problematic because, at the moment, we don't know who "legitimate access seekers" will be in Ireland, when the directive is transposed and effective in Ireland. A lot of proponents have a serious issue with WHOIS accuracy and say that that accuracy is required for security, stability and resilience.

The NIS 2.0 scope issue is dealt with, but not entirely. It excludes micro and small businesses, but it includes the providers of domain name services and Registrars etc. At the moment, there's no indication in Ireland if there will be a threshold number of domains to be considered as essential services. In the UK and Canada, thresholds are specified, so Registrars with less than that are not considered an essential entity and therefore not regulated by NIS 2.0.

There appear to be conflicting obligations 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).

There is a wider point that other European Registries are highlighting, which is how red tape will weaken the competitiveness of the European domain market. The fear is that this business will be driven offshore because European Registrars will be so burdened with this issue of accumulation of data and verification.

The final issue is supply chain responsibilities. While we could agree that the supply chain into an "essential service" is important, there is nevertheless a reluctance to take on responsibility for trying to regulate your supply chain, particularly in the context that KPMG identified - where the supply chain has global multinationals that you're dependent on for providing your service.

There was a significant and fruitful discussion on the wider implications of NIS 2.0:-

- A Registrar representative confirmed the UK has already amended the first draft. They do their threshold on DNS queries rather than the number of domains. The threshold is 250,000 DNS queries. This covers all the large players in the UK. It was noted that it's an EU directive but it needs to be ratified by Member Stats at a local level, so this is where you can influence thresholds and other elements that are specific to your market. In terms of GDPR, it works in the UK so it would be very surprising if NIS 2.0 doesn't follow the same model as GDPR.

- Another Registrar representative noted that:
    - o The additional regulation in the current draft will make domains harder to register therefore driving businesses and people to platforms like Facebook.
    - o It is a backwards step in terms of validation and verification.
    - o They are concerned that it will put them and EU businesses at a competitive disadvantage.
- The representative from the Department of Communications, Climate Action & Environment (DCCAE) noted that:
    - o the directive is still under discussion at the Council so it's not anticipated that it will be it'll be adopted until late in 2022. This means there is time to have discussions about items like thresholds.
    - o Currently, the directive does not provide for thresholds. What the Commission is proposing is that the determining factor is the size of the business and not the number of domains.
    - o In relation to the query about legitimate access seekers, they're not set out in the Directive. It is understood at a minimum to include law enforcement interests, and also National Cybersecurity authorities. They may also include academia and private sector interests. For example, people that would be would be conducting cybersecurity research.
    - o DCCAE would be interested to see what the PAC would see as a list of legitimate access seekers.
- One of the Registrar representatives expressed concerns about how the size of a business is determined. They worry that a very small Registrar will be burdened with processing, storing, validating and verifying a lot of personal information. They also noted that they would have issues with academia and researchers being legitimate access seekers.

The Chair invited the registry to assimilate the discussion and suggests next steps. The Registry noted that the combined influence of the PAC can help Ireland Inc. to transition to NIS 2.0. The next step is to explore what are the things that the PAC can do?

- First and foremost, it is important to build awareness of the positive aspects of NIS 2.0. The point has been made regularly that we as service providers should have these security and resilience controls and procedures anyway. We need to make businesses and representative bodies such as the SFA etc. aware of what is coming and how their members need to prepare. There may be blowback but the objective is to ensure that it doesn't arrive like GDPR where everyone is scrambling at the last minute to assess their obligations.

- The next issue is the burden of regulatory costs. We need to make our views known to the national legislatures and the drafters of the legislation. We know that in Europe, there are some requests for a budget to be set aside to help small businesses to finance the transition.

- Some variables need early clarification from the NCSC and those involved in influencing the legislators. For example, we need to define legitimate access seekers. Is it just law enforcement? Is it a firm of solicitors or attorneys? Is it a national body, like the Data Protection Commission, or some other regulators?

- Is the access process going to be automated or manual? There are requests from some European organisations for a portal for legitimate access seekers. In the portal, they would be able to access parts of the databases of the Operators of Essential Services to get the information they need. Or will it be a manual process where they request the information directly from the service provider?

- Which party will have the obligation to keep the data up to date into perpetuity - will the legislation impose that obligation on the registrant, registrar or the registry? (Bearing in mind that governments' information on its citizens is always out of date, except possibly after a census).

- A very important point, which has emerged in discussions from the Registrar representatives is the need for a clear legal framework. There are clear conflicts with some of the provisions of GDPR that need to be resolved. We need to know promptly how they will be resolved as a lot of time, effort and money went into putting systems in place for GDPR.

- The more engagement we have with policymakers and decision-makers in Ireland, the better, and there is a role for the PAC to carve out. We have a forum which we can use to engage with local politicians, for instance, as the legislation drafting process emerges, so that the responsible

Ministers are aware that there are really serious issues affecting this sector and businesses.

Our UK based Registrar representative stated that they have regular touchpoints with Ofcom about the draft Directive and what has changed and they have open and transparent engagement. Ofcom acted very quickly and provided an assessment of the differences with NIS 1.0 and give guidance to sectors on what is changing and how they should prepare.

There was some consensus among PAC members that an appropriate conduit for raising our concerns and addressing the issues is the Department of Communications, Climate Action & Environment (DCCAE) and the NCSC.

The Chair thanked members for their engagement and summarised that there was an emerging consensus that PAC could play an important role in relation to NIS 2.0 and should get involved. He asked the Registry to provide some clearly defined timelines, goals of what we want to do and to prepare an output document from the PAC, with consideration of the audience for the document.

The Registry confirmed that it is motivated to prepare an output document, potentially to be sent to the NCSC, or to the Minister as the designated competent authority under NIS 1.0. It was noted that the document would hold more weight if it came from the PAC collectively rather than just the Registry. It was accepted that not all members would be able to put their names to the document as their organisations may not be ready to do so, but the more that sign up to it, the more powerful it becomes.

The representative from the Department of Communications, Climate Action & Environment (DCCAE) stated that they have noted our concerns and will raise them internally on behalf of the PAC.

6. Any Other Business

No other business was raised.

7. Next Meeting

The provisional date for the next PAC meeting has been set for Thursday 17 February 2022.

____

Fergal O’Byrne
Chair of the .IE Policy Advisory Committee