ICANN70 | Virtual Community Forum - KINDNS Presentation and Workshop
Thursday, March 25, 2021 – 09:00 to 10:00 EST

STEVEN KIM: During this session, questions or comments will only be read out loud if submitted within the Q&A pod. I will read them out loud during the time set by the chair or moderator of the session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute ir microphone at this time to speak. All participants in this session may make comments in the chat. Please use the dropdown menu in the chat pod and select “respond to all panelists and attendees.” This will allow everyone to view your comment.

Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by panelists or a standard attendee to another standard attendee will also be seen by the session hosts, cohosts and other panelists.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcript, please click on the closed caption button at the Zoom button in the Zoom toolbar. With that, I hand the floor over to Adiel.

ADIAL AKPLOGAN Thank you very much, Steven, and welcome, everyone, to this session on this initiative by ICANN to promote DNS operational best practices. The session will be made of this presentation and followed by a Q&A

and interaction with you. Of course, this is a very new initiative at ICANN, and the goal mainly here is to present this to the community and get feedback which is part of the normal process for us deploying and implementing the initiative.

So as you know, the DNS is one of the very old protocols on the Internet. The first RFC that described the DNS is back 1983 by Paul Mockapetris. That RFC set the baseline, but over the 30 or so years after that, there has been a lot of evolution, a lot of new things that came in to strengthen the protocol to evolve it and add some extension to it. According to a project, an initiative by PowerDNS that's called the DNS Camel Viewer, there are 297 RFCs that are relevant to the DNS today, and that is about 2080 pages of text to read if you want to know everything about the DNS. We all agree that that's not something easy for anyone to do.

Some of those evolutions touch on the DNSSEC, some on new resource record types added to the DNS protocols, some touch on privacy. Recently, we heard about the DoT/DoH and many more. So it keeps evolving, it keeps [inaudible] itself, and operational practice are also evolving with that.

So it becomes complex by becoming more and more reliable, strong and resilient. And it offers a lot of choice depending on situation, how you're running your infrastructure. If you're a good engineer, you want to implement a service accurately, make it fast and effective, particularly the DNS for your user, but to do that, as we can see, you have to understand all the intricacy, you have to practice that, you have [to good almost] everywhere. That's not easy, particularly if you are running a small network or you are coming from an area of the world where you don't have enough resource, doing several things at the same time and spending quality time to the DNS is not very easy. So big companies have several engineers, specialists dedicated to that, follow all the evolution, attend IETF events, are very active in different mailing lists or working groups that talk about the DNS operation in general, but not everyone can afford that. But we all know that the DNS is a very distributed service where the weakest link can be a problem for the whole infrastructure. So it's important that everyone that runs the DNS, because of the interconnection, run it in a secure and safe manner.

So this initiative mainly is trying to set some common understanding on the key and most important best practices so that we have a level setting for everyone. Some of the challenge that comes in implementing or providing DNS service especially for a small ISP is what do we do with the evolution of the DNS protocol such as the DoH, DoT, [DoQ, DoH over TLS,] and many other new evolution of the DNS, how those medium-sized—and I'm surprised [inaudible] DNS infrastructure follow what is going on when they don't have direct connection with the technical community and in general, how community networks that are growing these past years know how to run their DNS, if they need to enable validation on their DNS infrastructure or their recursive server, how do they secure and manage their cryptography if they have a DNS on their network, and so on.

So it's not a simple thing, and in many cases, we have seen in small operation where the DNS is just a service, that's the setup, it runs, it allows resolution, and it's just forgotten in a corner somewhere, it runs, until one day there is a huge issue and people start looking at it. So it's not an active engineering thing in many small- and medium-size organizations.

So we established an initiative that we call knowledge sharing and instantiation norms for DNS and naming security, KINDNS. So the name, first question is the name. Obviously, it plays a little bit into something that some of you may already know, Internet Society's initiative that is the mutual agreed norms for routing security, which is pronounced MANRS. So KINDNS and MANRS will help us evolve the overall security of the Internet a little bit further.

So, what is KINDNS? The quality of being friendly, generous and considerate. So if we practice that in the way we run the DNS and implement those basic security measures for sure, we will all together contribute to a more secure and robust DNS infrastructure in general. So KINDNS is what we want to practice when operating DNS.

So the goal here is to produce something simple, straightforward that we can refer DNS operators to, large or big, so that they can follow and ensure that they promote those best practices for a better, secure and more effective DNS operation. That's simple, very straightforward.

So a key element of the current phase of the project, first, we want to make sure that we identify in a very effective way and build a sort of soft consensus around the most critical security norms for the DNS operation. That means there are hundreds of them out there, but the objective is to replicate all of them and ask everyone to implement everything. The objective is to streamline to look at what are the most important, what are the baseline for secure operation of the DNS, highlight those, promote them and provide people as well the necessary guideline to do that.

So there will be an information website dedicated to those best practices and also guideline on how to implement them. There will be a need at some point to communicate and promote it [to enroll] more DNS operators who can [lift] the initiative, because the success of this initiative will depend critically from how the community, how operators embrace them. And we want big operators as well to join, because this will need leading by example. People have to show that they adhere to those minimum best practices and ensure that they make it known and advertise it in their region.

One other aspect of the project that is critical for us is to be able to measure the impact of the project globally, to be able to identify indicators that can help us measure the impact on the ground, how those best practices are being implemented, how many people are joining and how many are adhering, voluntarily of course, to those best practices.

The last element of this is to match those best practices to the policy functions that are defined within ICANN framework, which is, how can we extend that to registry, registrar, operation and even registrant, because as you know, a registrar or registry operation is beyond the core DNS operation itself. There are other elements that also contribute to the overall security of the ecosystem. So we will, at a certain level, match and connect those two so that we can bring the registry and registrar community into this.

So in short, first identify and document critical best practices for a secure DNS operation, encourage participation from the community to adhere and become a goodwill kind of ambassador for this initiative within the community, and have a more active campaign and outreach to bring more operators to the initiative and to contribute to a more robust and secure DNS ecosystem.

So we have started this. I'm working with an external consultant as well to help us streamline and document these best practices. We have identified a few components of this. Those in gray and italic here are elements that are important for the operation but won't be the core of the initiative at this point, because again, as I mentioned originally, our goal is not to overwhelm people with thousands of things to do. Some, they already know, some are very particular to their network. But we want to focus on the DNS operation itself to start with.

So, handling your operational environment, your service, your system, your networks is part of the day-to-day operation of any network, and that is important. But then we look more closely at the DNS component, authoritative server, if you're running for a TLD, you're running an SLD, if you make it run by a registry or an independent DNS operators, if you're running a recursive server, how to run it to make it secure with very few key elements, are you running a closed or open resolver, what are the things that you need to pay attention to? So those will constitute the key elements to start with.

Then there are other considerations, like DoH and DoT which are emerging now, and then potential impact on securing your DNS. Some run Anycast DNS. What is the implication? So those are part of the global ecosystem, infrastructure consideration, but we will again try to focus on the key elements that are more generally found on ISP or corporate network.

These are going to be, of course, documented, [reference to be given, and guideline will be] produced so that anyone that want a one-stop point to have access to the right information can get them.

We expect to roll the product out toward the end of this year. This is the timeline. We are still at the very early stage, which is the identification of the key operational best practices, and that is where our engagement with the community is key. This is the first time we are exposing this, and our goal is to get more input from the community of this. Then we will start developing the guideline, and as you can see, throughout the project, we'll make sure that we keep the community in the loop and get in feedback and contribution from different components of the community. And by the end of this calendar year, we hope to be able to launch the project itself through the normal website and all the different elements that come with it.

Right now, how can you engage with the KINDNS? We have a mailing list, KINDNS-disucss@icann.org, which we're going to use to inform those who are interested in the progress of this, but also, will be a vehicle to hear from those who are interested.

We have also set up a Wiki page that we're going to use to publish some of the work as we go. That is a temporary placeholder at the end, as I mention before, there will be a dedicated website where all the information will be published and where people can also interact.

There is one aspect of the initiative as well that I didn't mention, which is the toolsets. We plan as well to provide through the platform tool that can help operators to assess their DNS infrastructure against some of those key best practices so they can self-assess themselves, they can know where they're falling and they can see how to probably fix that, or go check for more information. All that will be part of the platform that we plan to develop and release.

So that's it. As I mentioned, we are working right now with [Tim Rosinsky] that some of you know helping us in streamlining the best practices that will be part of the core of the initiative and also helping to document them, and of course, we will use either ICANN meeting or separate webinar regularly to update the community and get feedback from you on this.

That's it for now. I have originally planned to have a few words from Tim but he is not able to actually engage very actively today for some challenge he's having. But I'll be more than happy to get input, comment and questions that you may have related to this initiative. Thank you.

STEVEN KIM: There is one question. Lito Ibarra, “Do you expect KINDNS to be translated to other languages?”

ADIAL AKPLOGAN Yes. We will take the translation into consideration, of course, because if we want this to be available as widely as possible, the language barrier needs to be addressed. So yes, the translation aspect is going to be taken into consideration, and I would also like to add that KINDNS is one of the many other initiatives that ICANN is supporting and OCTO is working on to support a secure DNS ecosystem as the new strategic plan suggested. So there are a few other initiatives that are going to anchor to what KINDNS is doing, so to kind of have a 360-degree approach to this. But this specifically, as you can see, will focus on best practices and how to help operators, no matter which size they have, to have a reference point for secure operation of their infrastructure.

STEVEN KIM: I think this is more of a comment, from Hugo Salgado. “I applaud the initiative. it is long awaited in the community. I want to suggest involving NOGs from each region or country. I know that LACNOG from the Latin American region is working on a similar effort.”

ADIAL AKPLOGAN Thank you very much, Hugo. Sure. In our effort to engage the community as much as possible, we will work with NOGs and any other group that has an active involvement in operational aspects. And the

NOG, of course, are one of them, and definitely vehicle for us to promote those best practices.

STEVEN KIM: Another one. “I probably missed the beginning. What is your roadmap on this project in terms of participation, deliverables, and are there going to be renderings to the Board or the GNSO?”

ADIAL AKPLOGAN Well, our roadmap is first to work with the community, as I mentioned originally, to kind of identify those best practices that we can consider as the baseline for secure DNS operation. When we have them, we’ll get them published, but throughout the process, we will engage the community, the GNSO included, to share what we are finding and what we identify, so that what we finally have up there is something that has the buy-in from everyone so to be able to promote them. And that’s why we want to kind of [lower the bar] but focus on the most critical so that everybody can implement it.

Of course, some aspect of its implementation will probably need the involvement of the BTC and the Board. When we reach those points, we’ll get them involved. But right now, we are working on big content and the tooling side for this [inaudible].

STEVEN KIM: Here's one from Svitlana. “Do you invite end users to work in KINDNS, not only ISPs or TLDs?”

ADIAL AKPLOGAN Yes, there will be some aspect that will touch on registrants. That is going to be played on two fronts. One, of course, KINDNS is targeted towards DNS operators in general, but we have other program which will develop content that can help end users in, for instance, identifying what are the key elements they need to look for when they are registering their domain so that it's run securely. Many end users, registrars, will use a third party to run their DNS, but what exactly they have to expect from those are important as well, and that is going to be part of guideline that we will publish soon, can be part of the KINDNS, but the core element of KINDNS is DNS operators, but we have other program and other initiative, including capacity building programs that we are deploying right now that will touch on registrant and help them also understand what are the key elements they have to expect from their DNS vendor to run a secure DNS.

STEVEN KIM: Okay. THis one's from Yoshiro. "We should consider two guidelines from perspective of, A, DNS service provider, and B, DNS service consumer. DNS service provider includes both authoritative and full resolver, small, medium ISPs and enterprises should use DNS service provider as a consumer instead of operate by themselves."

ADIAL AKPLOGAN Yeah. That aspect is going to be taken int oconsdieration. Of course, if you are a corporate or you're small and you use your ISP or somebody else to provide you DNS service, that means you have to either select them through a mechanism or use those which are open out there and when you are doing that, you need as well to know what exactly you are expecting from your resolver provider in this case to run your network. And if you are using them to provide authoritative servers for you on domain names that you hold, you also need to know what to expect from them. And those are going to be part of the set of guidelines that are going to be developed. And thank you for highlighting that, because it's something that is not highlighted very often about the difference in the two aspects of running the DNS. Thank you.

STEVEN KIM: I think this is more of a comment. "A good initiative which contributes to more secure ecosystem and helps also in the field of DNS abuse." This one here is a question, Edmon, "Are universal acceptance considerations included in the initiative?"

ADIAL AKPLOGAN Sure. When we are talking about running a secure DNS, if aspects related to universal acceptance comes in the element that we [inaudible] we will highlight them. And again, as I mentioned, this initiative will try to focus really on some of the key elements that everyone can feel related to.

In parallel, ICANN and OCTO in particular in my department, the technical engagement department, have a few other initiatives that are going to touch on some other aspects of the DNS ecosystem security in general, because you could take it as ecosystem, there are elements elsewhere, and universal acceptance is one of them where we are working with our colleauges internally to develop more courses, more training for sysadmin, for network operators to take universal acceptance into consideration, and those will lead to guideline, will lead to also a referral.

If in the course of developing the key best practices, we see that there are some simple elements of universal acceptance that need to be implemented or taken into consideration more heavily in the core element that we mentioned, of course, we will take it into consideration. But again, that's where interaction with the communities will be key, because we will have the opportunity to discuss these with you and your input will help us also direct the outcome.

STEVEN KIM: Another one from Svitlana. "How do you join the KINDNS program?"

ADIAL AKPLOGAN Well, I didn't mention that, but the way we are designing it is that there will be different levels of joining. If you're DNS operators, joining means voluntary committing to implement some of the best practices elements that we will identify. This will be done through several steps, and that's why we are thinking of having tools that will allow you to self-assess yourself to see where you are in implementing those best practices, and there will be a process to fill a form to join the initiative and commit to implement those key best practices. And as soon as that is done, you will become kind of ambassadors of goodwill and help us promote those practices when and where needed. Those processes will be, of course, published on the website in detail when we [release there.]

STEVEN KIM: Brajesh, “If ISPs use DNS providers, would caching benefit be available, like Akamai?”

ADIAL AKPLOGAN Well, is the question related to KINDNS? Because the caching is something that is provided—either you decide to run your own cache, or if you're using a provider, if they provide it, you use it. But those nuances will be taken into consideration at some stage of KINDNS, because again, this is service-oriented, not core element, from my point of view, of the security aspect that we want to touch on. So if a DNS provider allow you to run a cache or you cache DNS internally, that is something more service-oriented and can be covered in guideline on how to purchase, request DNS services from your [operations] provider or any operators.

So, as I mentioned, right now we use the Wiki to publish news, evolution and documents related to the project as we go, and of course, the mailing list as well, so feel free to join the mailing list, and also, reach out to us. you can write to kindns-info@icann.org if you have a specific query beyond what was explained in this presentation. I would be more than happy to help you and provide you the answer [if you have it.]

STEVEN KIM: Yoshiro has another question. If some DNS best practice was developed in local community, do ICANN wish to translate it to English?

ADIAL AKPLOGAN Hi, Yoshiro. As I mentioned, if you have content, it will be good to point out to those content and see how we can use them or extract information from them. But of course, the objective here is not to translate or to kind of refer to all the documents that touch on DNS best practices. There are many out there. But if we have interesting elements covered by any, we'll be more than happy to integrate them in what we are producing.

So if there are a local community that already have some best practices, we'll be happy to consider them, but we are not systematically going to provide kind of translation to all those locally. But what we'll come up with as the key element of this project will definitely be translated.

Cool. I don't see any other question in the Q&A pod or the chat. Yeah, community.icann.org is  taking a long time to load. I think I too have noticed this morning and we will work with our IT team to see if there is anything specific happening there.

STEVEN KIM: A question just came in from Edmon. Will a mailing list be started, or we just check into the Wiki page?

ADIAL AKPLOGAN The mailing list will be started. It's kindns-discuss@icann.org. It's already set up, you can already join the mailing list for now. So it's already there. I mentioned it, and you can also see it from the Wiki page. Okay. Are you seeing anything else, Steven?

STEVEN KIM: I don't see any questions come in.

ADIAL AKPLOGAN Good. If there is no more question, thank you all for your attention and your contribution. We take notes of all of these, and of course, we'll use as much as possible to improve and extend the initiative as we [get them.] So watch this space, and thank you again.

**[END OF TRANSCRIPTION]**