Seguridad y Resiliencia del DNS - 29 de octubre de 2024

Claire C. van Zwieten - Internet Society Foundation: Así que, bienvenidos a todos.

Genial, muy bien, ahí vamos. Así que, bienvenidos a todos. Gracias por unirse a nosotros hoy para este importante seminario web sobre la seguridad y la resiliencia del DNS. Este evento es coorganizado por ICANN y la Internet Society, y todos nuestros panelistas son exalumnos mutuos, es decir, son exalumnos tanto de la Internet Society como de ICANN.

Apuesto a que muchos de nosotros conocemos el DNS, el Sistema de Nombres de Dominio, y que sirve como la columna vertebral de Internet, conectando a usuarios de todo el mundo con servicios de información, pero también son un objetivo de amenazas cibernéticas. Es importante que, como comunidad, entendamos cuáles son las amenazas en la seguridad del DNS y cómo podemos ser resilientes, y, sobre todo, el papel de las organizaciones multipartitas en asegurarse de que podamos frustrar las amenazas cuando aparezcan.

Antes de comenzar, me gustaría invitar a Jadiel, quien hablará un poco sobre nuestro programa Pulse y sobre sí mismo. Así que, Jadiel, si quieres venir y empezar.

Jadiel ADEFOULOU - Internet Society: Muy bien. Soy Jadiel Adefoulou, consultor de ingeniería de datos para Internet Society. Es un placer para mí estar aquí y hablar sobre la plataforma Pulse.

Entonces, en primer lugar, ¿qué es Internet Society Pulse? Es importante saber que Internet Society Pulse consolida datos de medición de Internet de terceros confiables de varias fuentes en una sola plataforma. Utilizamos los datos presentados para

examinar las tendencias de Internet y adaptar los datos a las necesidades de los usuarios.

Utilizamos los datos presentados para examinar las tendencias de Internet y contar historias basadas en datos, de modo que los responsables de políticas, analistas de investigación,

los operadores de red, los grupos de la sociedad civil y otros puedan comprender mejor la viabilidad, evolución y resiliencia de Internet.

Entonces, en Pulse, rastreamos los cortes de Internet, estimamos el impacto económico de un corte utilizando el Calculador de Pérdidas Netas de Pulse, medimos la resiliencia de Internet, y seguimos el número de puntos de intercambio de Internet en todo el mundo.

y ofrecemos un informe por país, una manera fácil de obtener una visión general del estado de Internet en cada país ISO del mundo.

Entonces, ¿qué pasa con el DNS?

¿Específicamente? Dos de cada tres dominios de códigos de país son seguros con DNSSEC. Uno de cada tres usuarios de Internet está protegido por un resolvedor que valida DNSSEC. Otra estadística sobre DNSSEC: se puede decir que algunos países, como Suecia, tienen incentivos para que los proveedores adopten DNSSEC. En consecuencia, vemos un nivel relativamente alto de cobertura de seguridad de nombres.

La mayoría de los dominios de Internet tienen un nivel muy bajo de adopción de DNSSEC. Por ejemplo, el dominio .com está firmado solo en un 4%.

Claire C. van Zwieten - Internet Society Foundation: Gracias, Jadier. Muchas gracias por educarnos sobre el programa Pulse y sobre DNSSEC.

Ahora me gustaría invitar a nuestros panelistas para este seminario web. Tenemos a Jackie Akello, Kanaan Ngutu, Lia Solis y Marko Paloski. Gracias a todos por acompañarnos hoy. Kanaan, sé que es muy temprano para ti. Probablemente sean alrededor de las 3 a. m. en Kiribati, así que muchas gracias.

Me gustaría dar a todos nuestros panelistas la oportunidad de presentarse y compartir un poco sobre su opinión acerca del estado actual del DNS. Lia, ¿te gustaría empezar?

Lia Solis Montaño: Buenos días a todos. Soy Lia Solis. Mi formación es técnica. Trabajo en un ISP. Muchos años. Trabajo con DNS para ISP, en resolutores de DNS. Me encanta este entorno de DNS, y soy ingeniera de sistemas. Gracias.

Claire C. van Zwieten - Internet Society Foundation: Genial. Gracias por compartir.

Marko, ¿te gustaría continuar?

Marko Paloski - Netcetera: Sí. Gracias. Hola a todos. Soy Marko Paloski, vengo de Skopje, Macedonia, y trabajo como ingeniero de sistemas en una empresa privada, más en la parte de infraestructura, pero además de eso, también soy coordinador del capítulo del Foro de Gobernanza de Internet de Macedonia del Norte, y he sido parte de la beca de la Sociedad de Internet, y también de la beca de la Próxima Generación de ICANN.

Entonces, diría que eso es más o menos para mí. Como persona técnica, estoy más interesado en la ciberseguridad, la privacidad, la seguridad en línea, la fragmentación de Internet y la regulación de plataformas, esos tipos de temas. Pero sí, muchas gracias.

Claire C. van Zwieten - Internet Society Foundation: Gracias, y me encanta que Marko una vez más destaque que todos en este panel son tanto exalumnos de ISOC como de ICANN. Todos son expertos en este campo y han tomado las mejores becas de la industria para demostrarlo.

Entonces, Jackie, ¿puedes presentarte y compartir tu opinión sobre el estado actual del DNS?

Jackie Akello - Research ICT Africa: Muchas gracias por eso, Claire.

Hola a todos. Es un placer unirme a esta llamada, son las seis en Nairobi. Ya casi es de noche aquí, o mejor dicho, ya es de noche.

Soy investigador de IA en Research ICT Africa, y mi trabajo se centra en gran medida en la IA y la gobernanza de datos. Principalmente realizo investigaciones y análisis de políticas sobre temas de actualidad que surgen de la IA y la gobernanza de datos.

Además de eso, he tenido el privilegio de ser becario de ISOC, así que fui parte de la cohorte de 2020 y pude asistir al IGF a través de la beca. También he sido becario de ICANN en varias ocasiones, como en la reunión ICANN 73 y la reunión ICANN 77.

Es un placer unirme a todos ustedes en esta llamada, y estoy deseando escuchar sus opiniones e incluso comenzar la conversación sobre la seguridad del DNS. Gracias.

Claire C. van Zwieten - Internet Society Foundation: Gracias.

Kanaan, ¿te gustaría presentarte y compartir un poco sobre a qué te dedicas profesionalmente y cuál es tu opinión sobre el estado actual del DNS?

Kanaan Ngutu - Digital Kiribati: Sí, absolutamente.

En primer lugar, fue y es un placer para mí unirme a esta conversación, a pesar de que es muy temprano en la mañana en esta parte del mundo.

Mi nombre es Kanaan, y como ya mencionaste antes, todos somos parte de los exalumnos de ICANN e ISOC. Asistí a dos reuniones de ICANN y también a dos reuniones de ISOC en el pasado, y en este momento trabajo en varias cosas. Hago trabajos de consultoría en el ámbito de las TIC, también trabajo con la UIT en los proyectos de islas inteligentes en Kiribati, pero al mismo tiempo también dirijo una ONG llamada Digital Kiribati que se dedica a promover la ciberseguridad y la alfabetización digital dentro de la comunidad aquí en Kiribati.

Claire C. van Zwieten - Internet Society Foundation: Gracias.

Creo que algo que quiero compartir es que lo especial de este grupo es que todos provienen de grupos de interés muy variados. Todos tienen una opinión y una visión muy diferente sobre la seguridad y la resiliencia del DNS.

Me encantaría empezar contigo, Lia. ¿Cuál es el papel de la seguridad y la resiliencia del DNS en el trabajo que realizas, y cuál es tu opinión sobre nuestra situación en ese ámbito en octubre de 2024?

Lia Solis Montaño: De acuerdo. El DNS es un servicio con una función definida, que es traducir nombres de dominio en direcciones IP. Con estas direcciones, los paquetes pueden seguir el mejor camino definido por el equipo de enrutamiento. ¿Puedes imaginar un mundo donde todos los usuarios tengan que memorizar direcciones IP?

Precisamente, uno de los factores que ha promovido el crecimiento de Internet en general es la facilidad de uso, gracias al DNS. El DNS es un servicio crítico para la accesibilidad a Internet, por lo tanto, merece especial atención en contextos de seguridad. Por mencionar algunos, podemos hablar del envenenamiento de consultas donde se cambian los orígenes de las respuestas DNS y contienen información falsa para manipular el destino de los paquetes.

La comunidad técnica ha trabajado arduamente para evitar estas amenazas.

Claire C. van Zwieten - Internet Society Foundation: Gracias. Y mencionaste a la comunidad técnica, y eso me hace querer dirigirme a Marko. Basado en tu trabajo y lo que haces, ¿cómo sientes que el DNS ha cambiado tal vez en los últimos 10 años?

¿Cómo han cambiado los riesgos de seguridad y nuestros modelos de resiliencia y DNS?

Marko Paloski - Netcetera: Sí. Gracias por la pregunta. Diría que incluso en los últimos dos o tres años, lo que ha cambiado, no solo en 10 años, porque en el mundo de hoy, cada año tenemos muchos nuevos desafíos y oportunidades y nueva tecnología, nuevas versiones, todo está cambiando y yendo en una mejor dirección.

Pero sí, estoy de acuerdo, es una buena pregunta. También, como sociedad, somos un poco más conscientes de las cosas, porque ahora usamos la tecnología todos los días y cada vez más, pero por otro lado, debido al uso de algunas de nuestras habilidades, todavía nos falta el conocimiento o tal vez no el conocimiento, sino tal vez el enfoque en las cosas.

Por eso, en los últimos años, creo que tenemos cada vez más amenazas cibernéticas, especialmente en el lado del DNS. Diferentes tipos de ataques. Esto está aumentando porque ahora dependemos más de la tecnología que tenemos en cada dispositivo. Incluso ahora en los coches, tenemos tecnología y sistemas y una computadora, lo que nos convierte en un objetivo más para los ataques. Hace 10 años, tal vez los objetivos eran las instituciones, tal vez las empresas, los gobiernos. Ahora, siguen siendo objetivos, pero también el usuario final es un objetivo mucho.

Es un momento desafiante.

Ahora tenemos más conciencia, porque hay muchas iniciativas. Por supuesto, algunas provienen de la Internet Society. ICANN también está haciendo mucho trabajo en esto para la seguridad del DNS, pero aún creo que estamos lejos de estar siempre seguros. El DNS es un sistema crítico, pero diría que es uno de los más atacados, porque como mencionó Lia, es una de las cosas fundamentales de Internet.

No puedes imaginar Internet sin el DNS, especialmente la seguridad del DNS, que hoy en día es por defecto. En el pasado, tal vez no necesitabas tener extensiones de seguridad DNS o algún tipo de cosas, pero hoy no puedes prescindir de eso.

Entonces, diría que con el avance de la tecnología, también avanzan los ataques y las vulnerabilidades. Ahora tenemos inteligencia artificial, puedes pedirle a GPT que escriba o te dé alguna vulnerabilidad de algún sitio, o tal vez que te haga una herramienta.

Por un lado, es bueno porque puedes ver y probar más sistemas, ya que puedes ver cómo funcionan las máquinas, pero también le da mucho poder a algunas personas con malas intenciones. Tal vez no tengan malas intenciones, pero cuando tienes la herramienta, puedes probarla.

Entonces, sí, es un desafío, pero nuestro trabajo es muy crucial, tanto para los técnicos como para los responsables de políticas y todas las demás personas, porque el tema es importante. El multistakeholderismo aquí es una de las cosas cruciales, porque creo que Internet se basa en el multistakeholderismo y debería continuar así. Cada parte

interesada, su trabajo es muy crucial, especialmente en estos tiempos que estamos enfrentando.

No sé si respondí directamente a toda la pregunta o me desvié un poco, pero quería intentar dar alguna respuesta.

Claire C. van Zwieten - Internet Society Foundation: Definitivamente has mencionado un punto muy importante, que es que cuanto más digitales se vuelven nuestras vidas, igualmente se vuelven vulnerables en la misma medida, porque así como nuestras vidas, como dijiste, en nuestros coches y todo, hoy en día tenemos una computadora, por lo que tiene sentido que a medida que aumenta nuestro uso de estas cosas, también aumente nuestra vulnerabilidad.

Y Kanaan, quiero dirigirme a ti, porque sé que trabajas mucho con la comunidad en tu área. Y, dado que también haces mucho en ciberseguridad, tengo curiosidad por saber cómo has podido hablar con la gente de tu comunidad sobre este tema, y si has encontrado formas de cerrar la brecha técnica para las personas que obviamente conocen Internet, pero no necesariamente saben sobre las infraestructuras que lo mantienen tan seguro como es.

Como dijo Marko, no puedes tener Internet sin DNS, pero mucha gente no lo sabe, en realidad. Entonces, cuando hablas con tu comunidad sobre ciberseguridad, ¿cómo logras incorporar esto?

Kanaan Ngutu - Digital Kiribati: Mi discusión sobre este tema girará en torno a la experiencia del Pacífico, viniendo del Pacífico Sur.

Conocemos el DNS tal como es y su papel en toda la infraestructura de Internet. Es uno de los elementos cruciales que necesita ser protegido. Sabemos la importancia del DNS, ya que puede determinar el destino de Internet, y para que los recursos sean accesibles en Internet, necesitamos este elemento crítico.

Esto es especialmente cierto en el contexto de las Islas del Pacífico. Hemos estado operando desde el otro lado del mundo, prácticamente desconocidos para la mayoría de las personas en el mundo occidental, pero dependemos completamente de Internet, y tenemos partes interesadas que participan en dar forma a Internet tal como es, y, de cara al futuro.

Pero, lamentablemente, la mayoría de las personas, especialmente aquellas que se supone deben tener un papel en el mantenimiento de este recurso, no necesariamente conocen este elemento crítico de Internet, ¿verdad? Creo que esto resalta la importancia de involucrar a más y más personas, y pienso que comprometer a la gente comenzaría por desarrollar la capacidad de estas personas.

Como mencionaste correctamente, aprendí muchas cosas, y una de ellas es que la mayoría de las personas carecen de conocimiento sobre el DNS. Ni siquiera saben cuáles son las vulnerabilidades, cuáles son las amenazas de seguridad que socavan las operaciones del DNS en el Pacífico, y cuando hablas de ciberseguridad, la gente de mi comunidad tiende a ser muy vulnerable en comparación con personas de otras partes del mundo. En parte porque Internet es relativamente nuevo en nuestro horizonte cuando lo comparamos con algunas personas que están ubicadas tal vez en los EE. UU. o en Europa.

Puedes imaginarte usar Internet por primera vez, con sus vastos recursos. La gente cree que Internet es algo realmente bueno, y eso es un hecho, pero no saben cuáles son las amenazas dentro de Internet. Hay cosas como el abuso infantil en línea, las estafas y los ataques que se realizan en las redes y también en los individuos.

Entonces, estas son las cosas sobre las que la gente en el Pacífico carece de conocimiento, y que los hace aún más vulnerables a este tipo de ataques. Es lo mismo cuando consideras DNSSEC, y creo que la gente se dará cuenta cuando sean atacados, ahí es cuando se darán cuenta de la necesidad de mejorar sus habilidades y mantenerse informados y comprometidos en este ámbito tan importante.

Claire C. van Zwieten - Internet Society Foundation: Gracias por esa respuesta. Me encanta lo que dijiste y creo que haces un gran punto cuando hablas sobre la capacidad, es que la gente no sabe lo que no sabe, y si tuvieran los recursos para aprender las mejores formas de protegerse, entonces podría ser más fácil para ellos.

Afortunadamente, ahora en 2024 tenemos la IA, y eso está proporcionando muchas nuevas oportunidades para desarrollar las capacidades de las personas en muchos ámbitos diferentes. Me encantaría pasar a Jackie y ver si podría brindarnos alguna información o perspectiva sobre el papel de la IA y el DNS, y si la gente está utilizando la inteligencia artificial para aprender por sí mismos o para mantenerse más seguros.

Jackie Akello - Research ICT Africa: Muchas gracias por esa pregunta, Claire. Mis colegas han compartido ideas muy importantes sobre la seguridad del DNS y también sobre el estado actual del DNS en el mundo, así que compartiré algunas ideas sobre el papel que juega la IA, particularmente en mantener el sistema DNS.

Lo que hemos visto recientemente, particularmente en los últimos años, es que la IA ha crecido mucho y ahora tenemos IA generativa y ChatGPT. El papel que veo que juega la IA, especialmente en el contexto africano y también para las personas a nivel de base y en los sistemas educativos, es que ahora educa a la gente sobre los sistemas DNS. Las personas llegan a ver lo crucial que es el sistema DNS, cómo funciona como infraestructura y también a entender el papel fundamental que desempeña.

Otra cosa es que la IA también, a través de las herramientas educativas, expone a las personas a los daños que pueden afectar a los sistemas DNS. La gente sabe que,

aunque la infraestructura DNS es crítica, al comunicarse y conectarse entre sí, existen riesgos al usar otros sistemas, y también están equipados con información sobre cómo pueden protegerse.

Otra cosa es que la IA también se está utilizando para causar inseguridad en el sistema DNS, por lo que cuestiones relacionadas con la ciberseguridad, daños e incluso ataques, son creadas simplemente por el uso de sistemas de IA. Este es un riesgo crucial que realmente necesita ser abordado en términos de examinar los sistemas DNS y la IA.

La IA también desempeña un papel crucial en la formulación de políticas en torno a los sistemas DNS, porque involucra a partes interesadas clave en el desarrollo de estos sistemas de IA, y también en el intercambio de conocimientos sobre cómo se pueden prevenir y mitigar algunos de estos daños.

Entonces, la IA tiene un papel crucial en la seguridad del ADN y también en el avance de la formulación de políticas en torno al sistema de ADN.

Claire C. van Zwieten - Internet Society Foundation: Gracias. Esa fue una gran respuesta. Creo que es realmente importante que las personas comunes, el cajero del supermercado, tu mamá, tu papá, que todos, todos sepan cómo protegerse y las mejores prácticas para la seguridad del DNS.

Si pudieran decir, me encantaría que cada uno de nuestros panelistas respondiera a esta pregunta: si pudieran dar un consejo práctico a las personas que quieren protegerse y asegurarse de mantener un sistema resiliente con una seguridad DNS robusta, ¿qué les sugerirían?

Y podemos empezar con Lia.

Lia Solis Montaño: Podemos hablar sobre las mejores prácticas, por ejemplo. Es importante entender las recomendaciones para el despliegue y operación del servicio de resolución de nombres, pero también estar abiertos a que estas recomendaciones son dinámicas y se basan en cada amenaza identificada en Internet.

Podemos citar algunas mejores prácticas, por ejemplo, tener DNS autoritativo y resolutivo en diferentes herramientas de infraestructura, asegurar la redundancia de los servidores DNS de la manera más transparente para el usuario. Una de ellas puede ser el uso de nubes anycast, que nos permite tener el servidor con la misma IP identificando diferentes ubicaciones geográficas.

Además, llevar a cabo una buena dimensionamiento de la infraestructura basada en el tráfico generado por los usuarios de la red. Estas medidas restringen específicamente las consultas recursivas a las direcciones IP del usuario objetivo, ¿asegurando la veracidad de las respuestas a las consultas cargadas en DNSSEC?

La mejor guía para KIND DNS es consultar las plataformas de aprendizaje proporcionadas por ICANN y también la Internet Society sobre estos temas.

En este punto, me gustaría añadir que todas las partes deben entender que el DNS no es una herramienta para bloquear. Este es un tema muy amplio que podría abordarse en otro seminario web, pero considero importante mencionarlo para orientar el pensamiento de los múltiples actores.

Gracias.

Claire C. van Zwieten - Internet Society Foundation: Gracias, y gracias por compartir que tanto ICANN como la Internet Society tienen excelentes recursos sobre la seguridad del DNS, y las mejores guías que puedes obtener para protegerte. Gracias por compartir eso, creo que es importante que la audiencia lo sepa.

Y luego, Marko, me encantaría escuchar tu respuesta sobre cuáles son las mejores prácticas en la seguridad del DNS y qué puede hacer una persona común para protegerse.

Marko Paloski - Netcetera: Sí. Depende del sistema, por supuesto, pero hay muchas mejores prácticas. Como mencionaste, hay muchas de la Sociedad de Internet y de ICANN que te ayudan a elegir o encontrar lo que es relevante. Porque no siempre la organización, la empresa o el individuo tienen el conocimiento o los recursos, no necesariamente recursos monetarios, sino personas con conocimiento que saben qué hacer.

Desde el punto de vista técnico, la implementación de la seguridad DNS, DNS seguro, hace 10 años, tal vez era una característica avanzada o algo así, de alto nivel, pero hoy creo que es una de las cosas básicas que debes implementar de alguna manera, si quieres tener un DNS seguro o un sistema seguro, porque el DNS es una de las cosas fundamentales que, si un hacker accede a él, tu empresa u organización es vulnerable y está abierta a ataques, abierta a un hacker.

Hay muchas otras cosas que algunas tal vez existían en el pasado, otras tal vez no, pero durante este auge de la nueva tecnología, el uso diario, muchas de ellas se especifican y tal vez se avanzan, así que añadiría más sobre el monitoreo y registro del tráfico DNS. Especialmente con la IA hoy en día, hay muchos sistemas que pueden ver el comportamiento de la red, ver las solicitudes, ese tipo de cosas, pero también revisar manualmente y observar porque, así como las máquinas de defensa o la inteligencia artificial están avanzando, también lo están los atacantes. Ambos lados tienen sus pros y contras, y siempre, cuando un lado avanza, el otro también avanzará después de un tiempo.

Existen muchas listas negras que aplican limitación de tasa, cuántas solicitudes en un cierto tiempo pueden ser enviadas o recibidas, o tal vez procesadas. Dependiendo de los sistemas, podemos ver que, especialmente cuando ocurren ataques DDoS, muchas empresas y sitios están implementando limitaciones en el período de tiempo, cuántas solicitudes puedes hacer, lo cual creo que es algo muy inteligente y bueno de implementar, dependiendo del sistema y cuál es el propósito.

Luego, tener servidores DNS redundantes, ataques DDoS, la idea completa es apagar o eliminar la capacidad del servidor, así que si tienes redundancia, tal vez sea una mejor infraestructura en cierto sentido, o más resiliente.

Siempre, también para el usuario final, es importante tener todas las actualizaciones, o la aplicación actualizada, el sistema operativo, el BIOS, la red, los switches, depende del tamaño y de la empresa, pero todo debe estar al día. Esto es algo fácil y pequeño, pero muchas veces la gente olvida hacer esas cosas. Especialmente, solo con nuestros teléfonos cuando no los actualizamos o nos olvidamos de actualizar la aplicación, pero si miras en la historia de los ataques, o lo que sucede o algunos que obtuvieron publicidad, podemos ver que muchas de las cosas fueron, algún software no estaba actualizado, algo era una versión más antigua, y ese tipo de cosas.

Por supuesto, no siempre se puede estar al día debido a ciertas limitaciones o aplicaciones que estás usando, pero sigue siendo algo crucial. Si ves que algún software no se actualizó, aún lo rastrearé hasta una persona, un error, porque alguien necesita actualizarlo, no es como si la IA lo hiciera automáticamente. Así que, la mayoría de los ataques que han ocurrido son errores de los empleados, o de las personas que están manteniendo o trabajando en los servidores.

Hay algunas cosas más. Lista negra, también filtrado DNS. Eso también ocurre de vez en cuando, a veces con buen uso, pero a veces con mal uso, ya que algunos países o regiones están limitados para acceder o enviar. En un buen sentido, digo que puedes limitar si vienen solicitudes maliciosas o específicas, pero en malos tiempos, como mencionó alguien de los panelistas, el DNS no es una forma de bloquear Internet o de bloquear el acceso, sino de dar acceso. Podemos ver en algunos casos que a veces se usa el DNS para que los estados de algunos países lo utilicen para bloquear.

Y, sí, siempre la lista de control de acceso, y tal vez limitar zonas para la transferencia. Esto es más específicamente para las partes técnicas, donde se transfieren direcciones IP, o donde puedes tomar una nueva o algo así.

Esos son cinco, seis, siete que mencioné, pero esos son los básicos. Hay muchos más complicados, y sé que en el trabajo también tenemos algún tipo de software, que no sabía que se podían aplicar restricciones tan sofisticadas, pero tiene sentido después de ver qué tipo de ataques están llegando.

Entonces, siempre intentas protegerte de cualquier tipo de amenaza, incluso si no es una amenaza, solo para estar protegido, porque a veces, tal vez mañana, se convierta en una amenaza, aunque hoy no lo sea, así que daré esas como mejores prácticas.

Claire C. van Zwieten - Internet Society Foundation: Quiero aprovechar rápidamente, mientras te tenemos aquí, Marko, para compartir una pregunta que hizo Sana en el chat. Ella dice: Gracias a todos por compartir su importante conocimiento con nosotros. Mencionaste la importancia de la colaboración multilateral en la seguridad del DNS. Por favor, comparte tus pensamientos sobre pasos prácticos específicos que diferentes partes interesadas, como empresas privadas, agencias gubernamentales y expertos técnicos, pueden tomar para mejorar la colaboración en la seguridad de un sistema DNS. ¿Hay áreas particulares donde se pueda mejorar el trabajo en equipo tanto en amenazas existentes como emergentes?

De hecho, me gustaría que tantos de nuestros panelistas como se sientan cómodos compartan su opinión al respecto, porque es una gran pregunta. Entonces, Marko, ya que la pregunta fue dirigida a ti, ¿te gustaría responder?

Marko Paloski - Netcetera: Puedo decir que es una muy buena pregunta porque a veces, especialmente en la correlación del DNS, cuando preguntas sobre las empresas, ya que también trabajo en una empresa privada, no se entiende mucho. Porque si entendieran los beneficios que puede tener este enfoque multilateral, creo que todos lo querrían. Por supuesto, a veces es una falta de conocimiento sobre cómo funciona esto.

Creo que el enfoque multistakeholder es muy bueno, especialmente en este tema, porque Internet y la gobernanza de Internet se basan en eso, especialmente cuando, como mencionaste, las empresas privadas, las agencias gubernamentales y los expertos técnicos no siempre tienen los recursos y el conocimiento.

Tal vez algunas instituciones tienen muy buen conocimiento en ciberseguridad, otras tienen el software, pero no tienen los recursos, y es muy crucial tener cooperación y comunicación entre ellas. Además, vengo de un país pequeño, Macedonia. Tenemos un CERT, pero es muy pequeño y no está tan preparado para grandes ataques o algo así.

A menudo lo que veo es que a veces las empresas ayudan al gobierno o a alguna organización a mitigar ese tipo de ataques. Desafortunadamente, no existe una plataforma global a la que cada país o cada empresa pueda unirse, pero hay muchas iniciativas en las que tanto individuos como gobiernos o empresas privadas pueden participar.

Es muy agradable mencionar, aquí, porque somos parte de este seminario web, puedo señalar que hay algunas organizaciones que están haciendo diferentes tipos de cosas en el multilateralismo, para las mejores prácticas y también el establecimiento de estándares. ICANN está haciendo mucho, también el Grupo de Trabajo de Ingeniería de

Internet está desarrollando los estándares, están desarrollando mejores prácticas, que puedes encontrar en el sitio.

La Internet Society también es una de ellas, junto con ICANN en la defensa de políticas y la concienciación. Hay muchas iniciativas de la Internet Society a las que la gente puede unirse, y también hay una red de expertos donde puedes compartir o preguntar en los foros. Estaba el Instituto de Abuso de DNS, pero ahora creo que cambiaron el nombre, se trata más de la respuesta a incidentes y la mitigación y colaboración en ese tipo de cosas.

Entonces, hay muchas plataformas o quizás foros que pueden ser útiles para empresas, organizaciones y ese tipo de cosas. Para organizaciones, no diría tanto, pero para empresas y gobiernos, veo que no se benefician mucho de unirse o usar tanto.

La empresa, a veces dicen que no, que no pueden pagarle a alguien, que pueden resolverlo ellos mismos, que no quieren colaborar, o a veces la empresa no quiere compartir lo que pasó, ni siquiera públicamente.

Y el gobierno, depende del gobierno, por supuesto, a veces quieren hacerlo ellos mismos. Tuvimos un caso en nuestro país donde se atacó el servidor, pero al final resultó que ellos fueron los que organizaron eso, para robar o lavar dinero.

Entonces, a veces es un problema, pero es algo muy crucial, porque si todos cooperan, será mucho más fácil mitigar los ataques y también estar más seguros.

Claire C. van Zwieten - Internet Society Foundation: Estoy de acuerdo contigo, lo que dices sobre cuando los gobiernos intentan hacerlo solo dentro del gobierno. Por supuesto, probablemente tengan una variedad de habilidades diferentes dentro de ese gobierno, pero realmente nada formativo, nada verdadero, ningún cambio robusto ocurre solo.

Entonces, realmente me gustaría invitar a Jackie y preguntarle cuál es su opinión sobre el enfoque de múltiples partes interesadas en la seguridad y resiliencia del DNS, y dónde hay mayores oportunidades de colaboración que probablemente deberían explorarse.

Jackie Akello - Research ICT Africa: Muchas gracias, Claire.

El enfoque multilateral en realidad juega un papel muy importante en la seguridad y también en la resiliencia de los sistemas de nombres de dominio. Estas organizaciones reúnen a diversos interesados, incluyendo gobiernos, entidades privadas, organizaciones de la sociedad y también expertos técnicos.

Cuando estas organizaciones se reúnen, lo que hacen es asegurar que se compartan diversas perspectivas e intereses que realmente dan forma a las políticas, estándares técnicos y marcos. Esto permite gobernar Internet de una manera muy significativa y fructífera, lo que fortalece la seguridad de nuestro DNS.

La importancia radica en mantener un Internet abierto, inclusivo y resiliente que refleje las necesidades de todos los usuarios, mientras se abordan las complejidades de una red global interconectada.

Creo que el enfoque multistakeholder desempeña un papel clave en la seguridad del DNS debido a los valores únicos que aporta en la formulación de políticas. Por ejemplo, permite la inclusión y la representación. Lo que sucede es que las organizaciones multistakeholder realmente reúnen diferentes voces de gobiernos, el sector privado y entidades técnicas. Al final del día, la inclusión asegura que la gobernanza de Internet refleje realmente las diversas necesidades y prioridades, en lugar de favorecer a un grupo particular en el ecosistema del DNS.

Otra ventaja que tiene el enfoque multistakeholder es que permite la transparencia y la rendición de cuentas. Las decisiones sobre el DNS tomadas a través de procesos multistakeholder son generalmente más transparentes y responsables cuando diversas entidades han estado involucradas en la formulación de esas decisiones.

Organizaciones como el IGF crean foros abiertos donde se pueden debatir políticas y prácticas. Pueden ser discutidas y revisadas por personas con diferentes conocimientos en los sistemas DNS. Lo que sucede al final del día es que las personas comparten las mejores prácticas que pueden gobernar los sistemas DNS de la mejor manera en el futuro.

Otra ventaja del enfoque multiactor es la innovación y la capacidad de respuesta. Como todos sabemos, la tecnología avanza a un ritmo muy rápido. Entonces, cuando involucras a personas de diferentes sectores, por ejemplo, organizaciones de la sociedad civil, lo que sucede es que las personas comparten su experiencia e incluso su conocimiento sobre las tecnologías actuales que tenemos, lo que garantiza que las leyes actuales también estén en sintonía con el avance de las tecnologías.

Las personas pueden compartir lo que está sucediendo en el ámbito tecnológico, qué nuevas tecnologías se están lanzando y qué consideraciones y medidas políticas deben implementarse para garantizar la seguridad del DNS.

Otra ventaja de esto es que, al final del día, se han considerado todos los intereses, lo que asegura que haya un equilibrio en cuanto a los intereses presentados en el debate sobre los problemas del DNS. Involucramos a diferentes sectores, a la sociedad civil, al gobierno y a los responsables de políticas. Cuando todos se sientan a la mesa, discuten y acuerdan sobre temas clave, lo que obtenemos al final del día es que sus intereses

están equilibrados y se ha tenido en cuenta la opinión de todos en cuanto a la seguridad del DNS.

Una última cosa que puedo decir sobre el multilateralismo es que también genera confianza y legitimidad en el sistema porque se han considerado todas las voces. Todos han podido compartir sus opiniones en cuanto a la formulación de políticas sobre el DNS e incluso la seguridad del DNS.

Lo que sucede es que, independientemente de las reglas y políticas que se aprueben al final del día, pueden ser consideradas legítimas porque se tuvo en cuenta la voz de todos en el desarrollo de estas políticas, y también se consideró la opinión de todos.

Entonces, lo que obtenemos al final del día es que se asegura la legitimidad en comparación con tener solo un grupo aislado tomando decisiones sobre cuestiones de DNS y aprobando políticas. Cuando eso sucede, hay mucha desconfianza y la gente no considera esas políticas ni esas decisiones como legítimas.

Entonces, en resumen, puedo decir que esas son algunas de las ventajas que tenemos con el enfoque de múltiples partes interesadas en el sistema.

Gracias,

Claire C. van Zwieten - Internet Society Foundation: y gracias por mencionar el importante aspecto de la confianza por diseño. Cuando desarrollamos políticas y sistemas con la seguridad y la confianza en mente, eso tiene un efecto dominó, a través de los usuarios, a través de la comunidad que utiliza estos sistemas. Así que, gracias por mencionarlo y también por destacar el lado de las políticas.

Es una transición perfecta para volver a incluir a Kanaan. Él es un consultor de políticas, y me encantaría escuchar cuál es tu experiencia en la creación de políticas y la consultoría en políticas como DNS, y qué tipo de desafíos y también oportunidades has visto en ese proceso.

Kanaan Ngutu - Digital Kiribati: Nuevamente, hablando desde las Islas del Pacífico, quiero hablar dentro de mi propio contexto, y creo que la experiencia es similar con el DNS y en todas las demás áreas de la política en otros ámbitos.

Comenzó con la idea de que los interesados, que se supone deben estar involucrados, comprendieran mejor la naturaleza del trabajo, y eso es para asegurar que pudieran contribuir de manera significativa a la discusión y a dar forma a los aspectos de la política con DNS en el Pacífico. Como mencioné antes, no muchas personas entienden esto.

Entiendo que hay varias plataformas creadas en el ámbito internacional que fomentan la participación en esta área, pero uno de los principales desafíos que tenemos en Kiribati y en las Islas del Pacífico es que tenemos una zona horaria muy diferente a la de otros países.

Entonces, está claro que necesitamos crear nuestro propio espacio, como un subespacio, que fomente la participación de los actores locales a nivel personal. Lo que quiero decir con esto es que, en Kiribati, lo que hacemos es tratar de identificar campeones, campeones que animen a los artistas a unirse y discutir estas cosas. Aquí es donde el apoyo de ICANN e ISOC en la producción de recursos que podamos usar localmente, y podamos traducir esas cosas, es crucial para asegurar que las personas interesadas tengan una comprensión integral, porque es ahí donde comenzaremos a construir la capacidad desde el nivel local.

A medida que maduren o se familiaricen con el conocimiento necesario, podrán llevar esto y elevar los compromisos al nivel regional y al nivel global o internacional, en términos de discutir asuntos relacionados con la política.

Creo que así es como deberíamos empezar en el Pacífico, y también se aplica a otras partes del mundo que se consideran aisladas de la comunidad global. Necesitas comenzar dentro de tu propia sociedad e involucrar a las partes interesadas y desarrollar sus capacidades, porque desde ahí puedes asegurarte de que, una vez que quieran llevar sus compromisos al siguiente nivel, podrán ser más significativos y eficientes en ese aspecto.

Esto se aplica al DNS, y también a todos los campos donde necesitas desarrollar políticas e implementar un modelo de múltiples partes interesadas.

Claire C. van Zwieten - Internet Society Foundation: El papel de los campeones en la creación de sistemas y políticas robustas que protegen y defienden Internet es crucial. Un pequeño autopromoción aquí, eso es algo realmente grandioso de ICANN y la Internet Society, es que podemos tener estos programas por los que todos en esta llamada han pasado, y a través de eso, han podido convertirse en campeones por derecho propio, y campeones de Internet.

Ya sea técnico o de políticas, o lo que sea, han podido tomar estas habilidades y regresar a su comunidad para implementarlas para el bien. Es importante que sigamos creando y desarrollando campeones como ustedes cuatro, para que realmente puedan hacer, honestamente, el trabajo pesado de la defensa de Internet. Son ustedes, en sus posiciones, en sus trabajos y en su vida, quienes realmente protegen Internet y hacen todo lo que necesitamos hacer.

Así que, muchas gracias a todos por todo lo que hacen, y muchas gracias por todo lo que han aportado a esta conversación.

Antes de que tengamos que cerrar por falta de tiempo, me encantaría llegar a las tres preguntas que tenemos en la sesión de preguntas y respuestas, y comenzaré con la primera de Ryan Uddin. ¿Qué vulnerabilidades en DNS lo hacen susceptible a ataques de suplantación? ¿Te gustaría responder a esa, Lia?

Lia Solis Montaño: De acuerdo. Cuando tenemos que verificar la dirección IP, debemos implementar estos métodos de suplantación en nuestra infraestructura, y el principio para hacerlo es DNSSEC.

Claire C. van Zwieten - Internet Society Foundation: Gracias.

Luego tenemos otra pregunta de Nicolas, quien es uno de los exalumnos de la Sociedad de Internet. Él dice: ¿Cómo se puede optimizar el marco KinDNS para soportar algoritmos criptográficos resistentes a la computación cuántica, qué colección de palabras, wow! y DNSSEC, ya que los avances en la computación cuántica, como el recocido cuántico, amenazan los métodos de encriptación tradicionales como RSA 2048?

Nicolás, estás poniendo a prueba mi capacidad de hablar hoy. ¡Vaya!

Entonces, Marko, ¿te gustaría responder a esa?

Marko Paloski - Netcetera: Intentaría porque no estoy muy metido en la computación cuántica y ese tipo de criptografía, pero sé que Nicolás sí lo está, porque también el año pasado en el IGF en Kioto, él también estaba discutiendo y haciendo preguntas sobre esto.

No estoy seguro, pero sé que este marco KinDNS, que es de ICANN, es toda la idea de la que hablé anteriormente, el multistakeholderismo y un lugar para las mejores prácticas. Este es un ejemplo de lo que ICANN está haciendo con este marco.

Pero, ¿cómo optimizar los algoritmos criptográficos resistentes a la computación cuántica? Esa es una buena pregunta.

Claire C. van Zwieten - Internet Society Foundation: Lo dijiste con tanta facilidad. Haces que suene tan fácil.

Marko Paloski - Netcetera: Sí, él habla como en una charla de café normal, pero creo que la criptografía, especialmente ahora con la computación cuántica, todavía estamos lejos de ese tipo de procesamiento masivo, pero algún día eventualmente llegaremos allí. La computación cuántica juega un papel importante ahora, especialmente en la criptografía para aquellos que son menos seguros, porque será mucho más fácil, con la computación cuántica, descifrar o encontrar la clave de encriptación.

Esto es relativamente nuevo. Está en investigación, hay pocos proyectos comerciales que lo estén haciendo activamente, pero creo que más sistemas se volverán más avanzados y será más fácil de implementar u optimizar.

Como mencioné, no estoy muy seguro porque no estoy tan involucrado en la computación cuántica, y especialmente en la encriptación con computación cuántica, pero mi idea es que, con el tiempo, los sistemas serán más avanzados, más fáciles de optimizar o configurar con ambas cosas, porque habrá más espacio para eso.

No estoy seguro si respondí. Conociendo a Nikolas, sé que no es la respuesta completa.

Claire C. van Zwieten - Internet Society Foundation: Desafortunadamente, Jackie tiene que retirarse, pero muchas gracias, Jackie, por todos tus aportes hoy, y gracias por prestar tu excelente conocimiento en DNS y legal a esta charla.

Ahora tenemos otra pregunta: ¿Qué medidas se pueden tomar para fomentar la adopción generalizada de prácticas de seguridad?

Me gustaría ir a Canaán para eso.

Kanaan Ngutu - Digital Kiribati: La respuesta es obvia, tenemos que concienciar más a la gente, especialmente a las organizaciones. Necesitan estar más al tanto de cuáles son las amenazas, y también guiarlos y enseñarles qué medidas tomar para empezar a implementar las seguridades en torno a la infraestructura DNS.

Eso es muy importante para mí, porque, hasta donde sé, en muchas organizaciones con las que he trabajado, la mayoría de las personas, incluso en el departamento de TIC, ni siquiera saben cómo tomar medidas para proteger su infraestructura DNS, especialmente en el contexto específico.

De nuevo, su red es tan simple, no hay sofisticación en ella, entonces, ¿cómo pueden implementar DNS cuando no tienen una infraestructura de red adecuada?

Entonces, para alentar a las personas a adoptar e implementar las mejores prácticas, necesitamos educarlas y mostrarles cómo se hace.

Creo que a partir de ahí pueden construir su conocimiento hacia adelante.

Claire C. van Zwieten - Internet Society Foundation: Es una gran pregunta y una gran respuesta. Me encantaría que Lia también abordara esta cuestión, y creo que esta será la última pregunta que responderemos antes de tener que cerrar el seminario web. Pero Lia, me encantaría escuchar tu opinión sobre lo que podemos hacer para aumentar las tasas de adopción de DNS.

¿Y cuál era el otro acrónimo divertido? El KinDNS.

Lia Solis Montaño: KinDNS nos ofrece una guía estándar para tener DNS. Es con lo que podemos trabajar inicialmente para aquellos de nosotros que queremos encontrar una guía. Las buenas prácticas son dinámicas y se ajustan a las necesidades del tiempo. Sin duda, podemos hacer contribuciones en cada escenario que pueda surgir. Recuerden que tenemos comunidades preocupadas por este uso.

Claire C. van Zwieten - Internet Society Foundation: Muchas gracias. Y creo que lo que esta persona también preguntó es qué podemos hacer para asegurarnos de que estamos estableciendo estándares de seguridad adecuados para este tipo de sistemas.

¿Alguno de ustedes tiene alguna idea sobre la importancia o la capacidad de establecer estándares?

Marko Paloski - Netcetera: Consulta las mejores prácticas, revisa cuáles son algunas cosas conocidas a nivel internacional y de organizaciones como ICANN o Internet Society.

Consulta también con tu país o comunidad local, qué están haciendo otras instituciones o gobiernos, o si hay alguna ley. No sé sobre eso, pero igual revísalo. Incluso si no hay nada, intenta proponer algo y ver si funciona. Si no, cámbialo.

Ese tipo de cosas no son algo que haces una vez y ya está para siempre; necesitas revisarlas y actualizarlas constantemente porque la tecnología cambia, los ataques cambian, así que debe estar al día.

Eso es todo.

Claire C. van Zwieten - Internet Society Foundation: Genial. Y, en esa nota perfecta, tenemos que terminar este seminario web. Muchas gracias a nuestros ponentes. Gracias por tomarse el tiempo de su día y de la mañana temprano para compartir su experiencia y su tiempo con nosotros.

Gracias a toda nuestra audiencia. Gracias por venir. Espero que hayan podido aprender un poco, y espero verlos a todos en nuestro próximo evento. Nos aseguraremos de compartirlo cuando podamos. Espero que todos tengan un excelente día.