ICANN72 | Semana de preparación – Introducción de la Facilitación de Seguridad del DNS - Grupo de Análisis Técnico (DSFI-TSG)
Jueves, 14 de octubre de 2021 – 13:00 a 14:00 PDT

WENDY PROFIT: Hola, bienvenidos a la sesión sobre la presentación del grupo de análisis técnico para la iniciativa de facilitación de la seguridad en el DNS, soy Wendy Profit y coordinaré la participación remota durante esta sesión.

Tengan presente que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN. En esta sesión solo se leerán las preguntas y comentarios presentados en el espacio de preguntas y respuestas, Q&A en inglés, leeré las preguntas y comentarios en voz alta cuando quien preside o modere la sesión me lo indique.

Esta sesión tendrá interpretación simultánea en los cinco idiomas de Naciones Unidas, hagan clic en el ícono de interpretación en Zoom y elijan el idioma que desean escuchar durante la sesión. Si desean tomar la palabra levanten la mano en la sala de Zoom, esto es para los panelistas, y el coordinador de la sesión dirá su nombre.

Antes de tomar la palabra asegúrese de haber seleccionado el idioma en el que hablará en el menú de interpretación, si habla un idioma que no es inglés, también diga su nombre para los registros e indique el idioma en el que hablará.

Al hacer uso de la palabra asegúrese de silenciar todos los dispositivos y notificaciones, les pedimos que hablen en forma clara y a una velocidad adecuada para permitir una interpretación correcta, a todos los participantes de esta sesión les pedimos que utilicen el menú desplegable del chat si desean comunicarse a través del chat y asegúrense de seleccionar “responder a todos los panelistas y participantes” de esta manera todos verán sus comentarios.

Tengan presente que los chats privados solo son posibles entre panelistas en el formato de seminario de Zoom, todos los mensajes enviados por un panelista o participante a otro participante también serán vistos por los anfitriones, coanfitriones y demás panelistas de la sesión.

Para ver la transcripción en tiempo real hagan clic en el botón de subtitulado en la barra de herramientas de Zoom. Ahora le doy la palabra a John Crain.

JOHN CRAIN: Muchísimas gracias, Wendy. Buenos días, buenas tardes, buenas noches a todos, en primer lugar, quiero transmitirles las disculpas de Göran Marby que esperábamos que pudiera hablar en esta sesión, pero estaba ocupado con otros compromisos y me pidió que diga algunas palabras en su nombre.

Soy el director de seguridad, estabilidad y flexibilidad en la ICANN dentro de la oficina del director de tecnología de la ICANN, participo activamente en esta iniciativa. Como ustedes sabrán, la seguridad, la estabilidad y la flexibilidad del sistema de identificadores es central

para la misión de la ICANN, por lo tanto, esto está presente en nuestros estatutos y en todas las actividades que llevamos adelante.

Göran se acercó a mí hace dos años después de una serie de ataques que se habían perpetrado y me preguntó cómo podíamos mejorar la seguridad en el sistema de identificadores y decidimos establecer un grupo de análisis técnico conformado por expertos dentro de la comunidad de la ICANN y también fuera de este ámbito.

Ustedes van a saber que Göran recibió este informe de nuestro grupo a principios de esta semana y la próxima semana estará a disposición de ustedes. Le quiero agradecer al grupo en nombre de Göran por este trabajo tan arduo que han llevado adelante en forma voluntaria para trabajar en una serie de recomendaciones ya desde hace más de un año.

Personalmente participé y fui testigo del arduo trabajo que se llevó adelante y no tengo palabras para agradecer todo lo que se hizo, vamos a tomar todos estos aportes como organización, los aportes a los directivos, al director ejecutivo y vamos luego a proceder a determinar de qué manera podemos utilizar esta información para facilitar la seguridad del DNS.

Sin más, le quiero ahora dar la palabra a Merike Käo quien se ha ofrecido a coordinar amablemente estos esfuerzos, hace prácticamente un año y medio. Merike, le doy la palabra, adelante.

MERIKE KÄO: Muchísimas gracias, John. La sesión en el día de hoy tiene el siguiente temario que ven en pantalla, yo voy a hacer una presentación breve del

trabajo general que hemos realizado en los últimos 18 meses y voy a continuar luego con lo más sustancial del trabajo que tiene que ver con los vectores de ataque en el ecosistema del DNS, las mitigaciones, las recomendaciones y vamos a dejar un espacio para preguntas.

Cada una de estas secciones en el temario serán presentadas por un miembro de nuestro grupo. Como dijo John, este trabajo se inició en mayo del año pasado, fue una iniciativa conducida y dirigida por el director ejecutivo de la ICANN, nos pidió que ejecutáramos su compromiso, los materializáramos, trabajando con la comunidad sobre cuestiones de seguridad y estabilidad.

Principalmente nuestra labor tenía la función de ofrecer algunas recomendaciones con lo que la ICANN podría o debería hacer para mejorar el perfil de seguridad y también ver si había alguna función que la ICANN no debía desempeñar en este sentido.

Como mencionó John, entonces parte de esta iniciativa o gran parte de ella se llevó adelante debido a algunos ataques muy sofisticados que se produjeron hace unos años.

Todos nos dimos cuenta en la ICANN de que la respuesta a estos ataques sofisticados había sido algo del momento y que tenía que haber una manera más estructurada de responder a este tipo de ataques en el ecosistema de internet y que era necesario también ver si se necesitaba un nuevo nivel de colaboración y de compresión para ello.

En esta diapositiva vemos todo el cronograma de trabajo de nuestro grupo, el TSG. El grupo comenzó en mayo, formulamos toda la composición del grupo y el 16 de junio del año pasado tuvimos nuestra

primera reunión, la mayor parte del trabajo en nuestro verano se concentró en responder e identificar algunas preguntas que queríamos abordar.

Luego comenzamos a principio de otoño a avanzar y parte de las deliberaciones se centraban en las causas raíz y en los vectores de ataques, creamos también una lista de prioridades sobre estos registros de ataques para ver cuáles eran estos vectores de ataques que eran más serios y que requerían de nuestra atención.

También observamos las medidas de mitigación que ya estaban vigentes o que estaban vigentes, pero no se habían puesto en práctica, o aquellas que tal vez estaban faltando y creamos un documento preliminar que luego fue finalizado con una serie de recomendaciones, hicimos consultas con expertos de la industria y, por último, elaboramos el informe final que se lo enviamos a Göran a principios de esta semana.

Estos son los miembros del TSG, nueve miembros y como pueden ver, es un grupo interfuncional con distintos expertos con experiencia y conocimiento especializado en la infraestructura de operación del DNS, conocimientos sobre la seguridad, las operaciones de los registradores y los registros, también operaciones de códigos de país, experiencia en todo lo que tiene que ver con los ISP y las redes de distribución de contenidos.

Entonces toda esta combinación de conocimientos nos llevó a un nivel muy profundo. Y como mencioné, también llevamos adelante consultas e hicimos una revisión con consultores técnicos del documento,

quienes nos ofrecieron comentarios muy específicos y el TSG está sumamente agradecido por la revisión en profundidad y minuciosa que se hizo porque nos permitió tener un documento final mucho más rico de recomendaciones.

Tuvimos apoyo de la ICANN en distintos niveles, con un comité directivo de DSFI TSG con cuatro miembros de la Junta Directiva y dos ejecutivos, también tuvimos un apoyo muy amplio de parte de la ICANN con la gestión de programas de comunicaciones, con conocimientos específicos en determinadas materias y también un escritor técnico excelente que, en este caso, fue una mujer que con sus conocimientos nos permitió realmente tener un texto que es muy fácil de leer a pesar del alto nivel técnico que tiene.

Esto es un diagrama que muestra la amplitud y la profundidad del ecosistema del DNS integral, se esperaba que el trabajo insumiera un año y en realidad insumió un año y medio, se hizo 100% en forma virtual, lo cual también presentó sus propias dificultades.

Personalmente quiero agradecer a cada miembro del TSG y al equipo de apoyo de la ICANN porque mantuvimos muchísimas reuniones, también talleres que duraban dos o tres horas semanales o cada dos semanas, que realmente nos permitió llegar a estos resultados, fue un tema sumamente complejo, pero realmente estamos muy complacidos y orgullosos del trabajo que hicimos.

Entonces ahora vamos a empezar a hablar de los temas sustanciales, vamos a comenzar con los ataques, entonces para ello pasemos a Gavin con la siguiente diapositiva.

GAVIN BROWN: Gracias, Merike. En esta parte de la presentación vamos a hablar de algunos de los vectores de ataques que podemos encontrar y las metodologías también que utilizamos nosotros para analizar estos vectores. Siguiente, por favor.

En esta imagen nosotros tratamos de ilustrar, como mostró Merike también, la profundidad, la amplitud y el alcance de los sistemas que estábamos analizando desde el punto de vista de las amenazas y vamos a ver que aquí se incluye tanto todo lo que tiene que ver con el DNS, como los usuarios y los registros. Aquí podemos ver toda la vía de resolución a través de los resolutores mínimos y también qué pasa del lado de la provisión con los usuarios finales, los registratarios, los sistemas que interactúan con los protocolos entre registros, registradores y personas individuales como nosotros.

Entonces aquí tratábamos de cubrir todos los sistemas de punta a punta y aquellos que se veían bajo mayor amenaza. El proceso que seguimos fue muy parecido, según mi experiencia, a un análisis de riesgo donde tratamos de analizar los distintos vectores de ataques, categorizarlos y establecer los puntos en común entre ellos.

Hablamos con cada uno de los vectores de ataques y también tomamos experiencias reales que habíamos tenido con distintos ataques, cuando vemos estos vectores de ataques consideramos distintas preguntas, por ejemplo, ¿qué medidas de mitigación podrían estar disponibles? Luego hablaremos más en detalle de eso, si había alguna cuestión que tenía que ver con un entendimiento o no ha acabado el riesgo, si la

infraestructura del sistema del DNS en sí misma era vulnerable a determinadas clases de ataques que podían sufrir otras partes del ecosistema del DNS.

Entonces a nivel muy general establecimos una gran cantidad de vectores que se redujo luego a lo que ustedes ven aquí en la pantalla, son bastante amplios, pero verán que algunos de ellos son genéricos también porque los participantes en el ecosistema del DNS son organizaciones y compañías que tienen los mismos desafíos en términos de seguridad que cualquier otra organización, una universidad, un banco o un operador de gTLD.

Algunos son más exclusivos para el DNS y también para los protocolos y sistemas que se utilizan, entonces podríamos cubrir la elección de tiempo de vida útil que está en registros también, pero podríamos ver cuán bueno es el sistema de contraseñas.

Estos fueron compactados aún más en los vectores que veremos a continuación en estas categorías. Resumimos todos estos vectores en estas categorías de vectores de ataques y vamos a hablar en más detalle de algunos de ellos, pero comenzamos con aquellos que son un poco más generales como la gestión de acceso de identidad, es un desafío en términos de seguridad que no es exclusivo para nuestro mundo.

Toda empresa tiene este tipo de dificultades, tiene que pensar en el acceso y en la identidad, lo mismo con las cuestiones de autorización y control de acceso, pero hay algunos otros vectores que son más específicos al sistema del DNS como, por ejemplo, la usurpación de recursos, todo lo que tiene que ver con la denegación de servicio y

cuestiones que tienen que ver con vulnerabilidades, tanto en la implementación de los códigos como dentro de los mismos protocolos.

La selección la hacemos cuando decidimos utilizar una determinada infraestructura que puede hacer que los sistemas sean vulnerables a estos vectores de ataques. Siguiente, por favor.

Entonces comencemos con el primero, la gestión de acceso y de identidad. Existen en todas partes, en el ecosistema y en el sistema de aprovisionamiento las credenciales, se utilizan para autenticar las interacciones entre los participantes, entonces si uno es un empleado de un registro tiene que usar un nombre de usuario y una contraseña para ingresar al sistema.

Si uno es un registrador también tiene que utilizar estas credenciales para ingresar al registro y así continúa toda la cadena hasta llegar al usuario final, cualquier punto en esa cadena o en ese sistema puede estar comprometido en términos de seguridad. Las organizaciones que se ocupan de administrar estas credenciales tienen que tomar decisiones sobre implementar políticas que permitan proteger esas credenciales para evitar la suplantación de identidad, la captura de esas contraseñas.

Entonces aquí estuvimos trabajando en esta área, focalizándonos en las credenciales de los registratarios, la autenticación entre los registros, los registradores, los revendedores y también la amenaza de utilizar credenciales que puedan estar comprometidas para iniciar transacciones en el registro, donde se usurpa una de las entidades en la cadena entre el registrador y el registro. Siguiente diapositiva, por favor.

Aquí tenemos un ejemplo de problemas de control de acceso y temas de autorización no adecuados, vemos la captura de un reclamo de un subdominio olvidado, aquí tenemos un registro de un nombre de dominio que tiene un alias, un registro de nombre C que apunta a otro recurso, esto permite que un atacante tome control de ese nombre de dominio sin que se valide que realmente sea el propietario de ese dominio.

El siguiente vector de ataque tiene que ver con la usurpación de recursos, aquí un atacante puede hacer que las consultas al DNS sean redirigidas a un tercero, este redireccionamiento puede tener diferentes consecuencias según donde sea en el sistema y cuál sea el sistema usurpado.

Sin embargo, hay empresas que pueden hacerlo de manera legítima donde la empresa no quiere que los usuarios de sus redes internas accedan a la red pública, pero también puede darse como consecuencia una actividad maliciosa como, por ejemplo, instalando malware en una computadora o en el dispositivo del usuario final.

Entonces esto podría implementarse a través de la usurpación de un resolutor recursivo usurpando el servidor autoritativo y dominios parecidos o dominios facsímil. Esto es algo diferente, podríamos decir que, en este caso, el objetivo de estos ataques son los usuarios de infraestructuras y no los usuarios finales.

Certificados fraudulentos y manipulación de rutas también son diferentes vectores de ataques. Aquí tenemos un ejemplo de lo que

hablamos cuando hablamos de los dominios facsímil, los ataques homográficos son el ejemplo más obvio de este tipo de ataque.

El siguiente vector de ataque del que vamos a hablar son vulnerabilidades en los códigos y en el protocolo. Hay diferentes problemas y desafíos aquí en estos dos tipos de vulnerabilidades, cuando hay un problema con el software del DNS que, en general, se mitiga de manera diferente cuando el problema está en el protocolo.

Porque cuando hay un problema con el protocolo de DNS, como ya se dijo muchas veces, hay una serie de vulnerabilidades que tienen que ver con el DNS y tenemos aquí el ataque Kaminski, por ejemplo, cambia las vulnerabilidades y el protocolo causando problemas de interoperabilidad, hay que trabajar en estrecho contacto con todas las partes interesadas porque si no se podría desestabilizar el sistema, pero estas vulnerabilidades deben ser consideradas abordadas y pueden tener diferentes impactos en los sistemas vulnerables.

Y como pueden ver, aquí tenemos envenenamiento de la memoria caché, por ejemplo, esto sería una vulnerabilidad de protocolos. Este es un ejemplo de cómo se da este envenenamiento de memoria caché, aquí ven las flechas, cuando un servidor recursivo recibe una consulta de un usuario final, está buscando ICANN.ORG, por ejemplo, y un atacante puede interceptar esa consulta o enviar una respuesta fraudulenta al servidor recursivo antes de que llegue la respuesta del servidor autoritativo.

En ese caso, la respuesta falsa es la que se envía al usuario final antes de que llegue la respuesta legítima al servidor recursivo. Opciones y

elecciones de infraestructura. En este caso, son las decisiones que toman los operadores del sistema DNS o los servicios de DNS que pueden tener consecuencias no buscadas en cuanto a la seguridad y disponibilidad del sistema.

Los TTL son un muy buen ejemplo de esto, el tiempo de vida. Los TTL muy largos o muy cortos pueden presentar problemas, entonces aquí se trata de buscar un TTL adecuado, ni demasiado largo, ni demasiado corto, en el medio.

También hay un escenario donde un TTL muy breve es útil y adecuado, hay otros casos en donde es adecuado uno largo, pero las consecuencias no buscadas significan que hay que evaluar correctamente los riesgos para conocer bien las consecuencias de las decisiones que se toman en términos de elección del TTL.

Si pasamos a la próxima diapositiva, donde veremos esto, aquí en este escenario se ha implementado un TTL en un servidor autoritativo y ese TTL (Time To Life) asegura que los usuarios finales seguirán recibiendo las respuestas a sus consultas dentro de un tiempo determinado.

El registro caché lo ofrece el resolutor, pero si el atacante puede interceptar la consulta, ya sea secuestrando el nombre de dominio o utilizando alguna de los otros vectores que ya mencioné antes, entonces la respuesta maliciosa es la que llega a la memoria caché y el usuario seguiría estando vulnerable, podría ser explotado por esta vulnerabilidad hasta que ese registro se venza y se pueda recuperar la respuesta correcta del servidor autoritativo. La próxima diapositiva, por favor.

Ya hablamos de DNS como vector de ataque, esto tiene que ver con el uso de DNS como canal oculto, aquí vemos cuando se pasan los datos sin ser filtrados o bloqueados; y esto ha sido explotado, estamos hablado de canales encubiertos, esto permite a los atacantes infiltrarse en un sistema o exfiltrar datos de un sistema y llevarlos hacia el exterior. La próxima diapositiva, por favor.

También hablamos de la denegación de servicio, para cualquier operador de infraestructura clave de DNS esto es un desafío continuo presente siempre por la forma en que funciona el protocolo de DNS, esto significa que los servicios de DNS son vulnerables a los ataques de spoofing y a diferentes tipos de ataques.

Los ataques de denegación de servicios pueden alterar e impedir el trabajo de muchas más organizaciones si el objetivo es el operador o los servidores raíz o a los servicios de los registros o registradores, esto afecta a una población mucho mayor que si solo se atacara al usuario final. La próxima diapositiva, por favor.

Con esto terminamos la descripción general de los vectores de ataques y ahora le doy la palabra a uno de mis colegas que va a hablar sobre las medidas de mitigación.

DUANE WESSELS: Yo voy a hablar de las mitigaciones, de las medidas de mitigación.

Como ya dijo Gavin, él ya habló de los ataques, pero también dedicamos tiempo a nuestro grupo a analizar las formas en que se podían mitigar esos ataques y desarrollamos diferentes factores y estrategias, algunos

no llegaron al informe final, pero voy a mencionar entonces las medidas que sí llegaron al informe final.

Dedicamos mucho tiempo en nuestro grupo a debatir sobre la autenticación, muchas de las recomendaciones y medidas de mitigación tienen que ver con control de acceso y otros temas de autenticación. Lo mejor que se puede hacer para que los recursos del DNS estén seguros y protegidos es utilizar contraseñas complejas, hay varios casos en los que se utilizan contraseñas demasiado simples que pusieron en peligro el DNS.

A veces se utilizan contraseñas muy complejas, pero también se pueden utilizar credenciales de un solo uso o credenciales con autenticación multifactor, cuando las contraseñas se vuelven más complejas es necesario utilizar un administrador de contraseñas que nos ayude con esto en lugar de tratar de recordar cada contraseña. Cuando hablamos de conciencia y concientización acerca del riesgo, se trata de saber las formas en que se pueden comprometer las credenciales, por ejemplo, ataques de phishing.

Hablamos sobre la disponibilidad y el uso de servicios que pueden evitar el uso de contraseñas muy débiles, por ejemplo, quizás haya algún código que nos pueda evaluar si una contraseña es lo suficientemente sólida o si incumple con ciertos requisitos. También hay bases de datos donde se pueden buscar las contraseñas comprometidas y siempre podemos saber que los delincuentes también pueden acceder a estas contraseñas, así que, no debemos utilizar contraseñas que ya se han visto comprometidas.

Hablamos también en nuestro grupo acerca de las soluciones que se pueden utilizar en el caso de un ataque, hablamos, por ejemplo, de las formas en que los dominios y los registratarios puedan ser verificados y validados por los clientes cuando presentan una solicitud de registro. La próxima diapositiva, por favor.

Las mitigaciones en cuanto a la disponibilidad, integridad y privacidad algunas ya son muy conocidas, en el caso de la disponibilidad creo que, muchos de ustedes ya saben, un único punto de falla no es una buena idea y muchas veces pensamos tener esto en términos de redes, servicios de redes, no hay que poder todos los servidores de DNS en la misma red y en el mismo centro de datos.

Y, además, por supuesto, hay otros aspectos, otros tipos de punto único de falla que habría que tener en cuenta como, por ejemplo, utilizar solamente un tipo de software o un tipo de hardware, también como muchas personas entendieron, después de un ataque reciente, se utiliza servicios de DNS secundarios. Es una buena idea utilizar diferentes plataformas porque si tenemos una sola plataforma que deja de operar la red se cae.

En cuanto a la integridad una de las mejores medidas de mitigación es DNSSEC, tener dominios firmados que implementen DNSSEC tanto del lado de la publicación como del lado de la resolución que utilice la validación, bloqueo de registros, hay algunos productos y herramientas similares que sirven para evitar el secuestro de dominios y después también hablamos del uso de algunos protocolos más modernos, como CDS, CDNSKEY y CSYNC que facilitan la transmisión de material de DNSSEC entre una zona hijo y una zona padre.

En cuanto a la privacidad, obviamente se ha trabajado mucho, últimamente en cuanto al uso de transporte de DNS encriptado cada vez vamos a ver más de esto y esa es una muy buena manera de implementar la privacidad en el DNS. La próxima diapositiva, por favor.

Hay otras medidas de mitigación que habría que conocer, por ejemplo, el monitoreo, podemos contratar servicios de protección de marcas que nos alertarían si la marca de nuestra empresa o nuestro nombre de dominio es registrada como dominio de alto nivel en otro registro. La transparencia de los certificados, bueno, es un proyecto por el cual hay certificados que se pueden solicitar para ver los servicios y esto nos alertaría si se emitió un certificado contra nuestro dominio.

También hay una autorización de la autoridad de certificación, un registro CAA que se puede poner en la zona que especifica qué autoridad de certificación está autorizad a emitir certificados para ese dominio. Esa es una buena estrategia también.

En cuanto al enrutamiento RPKI, la autenticación del origen de ruta, esto ayuda a proteger las redes de publicidad falsa, eso también se puede monitorear. Para las organizaciones que implementan o que deben implementar un proceso de inspección de los datos que pasan por su red probablemente deban pensar en routers o switches que permitan la inspección de los paquetes para poder saber qué está pasando por las redes.

En el caso de desarrolladores de software hablamos de la necesidad de contar con buenas prácticas del ciclo de vida de desarrollo de software en términos de la seguridad, cuando se desarrolla software hay que

utilizar mejores prácticas para que el software esté actualizado, que se implementen los parches y seguramente todos sabrán que es importante aplicar los parches en forma periódica, no solo del lado del usuario, sino también del lado de los operadores ir aplicando los parches a medida que aparecen para evitar problemas.

La mitigación en relación al control de acceso incluye el uso de lo que llamamos arquitecturas de acceso basado en conductas, por ejemplo, Zero Trust es una de las que está empezando a conocerse. Siempre es una medida particional los servicios críticos, por ejemplo, separar los servicios de DNS de los servicios de correo electrónico, de los servicios web, ponerlos en diferentes sistemas de manera que, si se ataca a uno no estén todos atacados.

Habría que considerar, por supuesto, controles de acceso más restrictivos para las cuentas que quizás sean más sensibles y en los casos donde se puede particionar los servicios es una buena idea limitar el acceso a los servicios de DNS solamente a los puertos de DNS, el 53, el 853 con TLS y quizás el 443 con DNS/HTTPS. Y si operan un resolutor de DNS que no ha sido pensado para ser utilizado por terceros, asegúrense de que tengan un control de acceso que limite su uso solamente a los usuarios que deberían estar utilizándolos.

Medidas de mitigación para controles de punto final y de red. Los antivirus ya existen desde hace mucho tiempo y siguen siendo importantes para muchos usuarios, no hablamos mucho de los antivirus, ni les dedicamos mucho tiempo, pero los mencionamos. Control estricto sobre la selección de los resolutores de DNS.

En la actualidad, muchos dispositivos reciben de la red de los servidores de DHCP, por ejemplo, el servidor les dice qué resolutor utilizar y esto, en general, funciona, pero también hay formas en que el malware u otros vectores de ataques pueden cambiar el servidor de nombres recursivos que ha sido ofrecido por el dispositivo, hay que prestar atención a esto, quizás bloqueando los resolutores de DNS no autorizados en el firewall o hacer otras verificaciones para asegurarse de que el resolutor de DNS que está utilizando el dispositivo sea el correcto.

Y, por supuesto, una vez más, para las organizaciones que pueden proteger a sus usuarios un firewall de DNS es una muy buena idea porque sirve para garantizar que los usuarios solo lleguen a destinos apropiados y seguros. Entonces de todas las mitigaciones que hablamos hasta ahora, bueno, las dividimos en las siguientes categorías.

La mayoría ya las mencioné, desafíos relacionados con las credenciales, control de acceso para las cuentas de usuarios, usurpación de recursos… Esto algo de lo que Gavin habló, también vulnerabilidades de código de protocolo. El informe habla del uso de DNS como vector de ataque versus DNS como objetivo del ataque, ataques de denegación de servicios, por supuesto, y mecanismos de respuestas a incidentes. Creo que con esto terminé de cubrir mis diapositivas y ahora le doy la palabra al próximo orador.

MARC ROGERS: Hola. Bueno, pasemos a la siguiente diapositiva. Vamos a hablar de las recomendaciones que fueron elaboradas a partir de lo que discutimos en el grupo, obviamente esto está vinculado con los sistemas de ataque y las medidas de mitigación que se presentaron. Todo esto se resume en estas cinco áreas, donde tenemos aquí la educación con respecto a la autenticación y las otras áreas que ustedes ven aquí en la pantalla.

En primer lugar, hablamos de que la ICANN tendría que trabajar con otras organizaciones como SSAC, GNSO, ccNSO, operadores de TLD y otras entidades para poder desarrollar un programa de ejercicio de análisis específico a la tarea, para poder ver las funciones operativas que se dan durante situaciones de incidentes para encontrar aquellas brechas operativas que podrían existir.

Al hacerlo de manera continua estas brechas operativas, podrían ser identificadas, registradas y se le podría dar seguimiento dentro de la ICANN para luego poder llegar a otras recomendaciones futuras. Hay distintas recomendaciones en torno a la investigación, primero con respecto al uso indebido del DNS, sabemos que este es un panorama que nunca es estático, que está en constante evolución y también lo está el uso indebido del DNS.

Las técnicas de ayer evolucionan y son las mismas de que tendremos mañana, hay distintas tecnologías que pueden implementarse y también distintas arquitecturas del DNS que pueden utilizarse.

Entonces nosotros creemos que hay que seguir llevando la investigación, aplicarla al DNS para ver cuáles son las formas de uso indebido y para poder anticiparnos a ellas. La siguiente recomendación

es que, tenemos que investigar las ampliaciones y mejoras a la seguridad del DNS, justamente por estas amenazas que cambian en forma constante.

También las mejoras de la seguridad tienen que ir cambiando y creemos que tienen haber un programa para investigar los límites, los riesgos y los beneficios de distintas mejores de seguridad del DNS. Hay algunas aquí enumeradas en este informe y el pensamiento general es que, al igual que con el uso indebido tenemos que anticiparnos a hacerle un seguimiento y tener un ciclo de retroalimentación donde se identifiquen las brechas, las mejoras y luego se pueda retroalimentar.

En relación con la autenticación y las secciones anteriores, también creemos que tiene que haber una investigación de las buenas prácticas y las prácticas adecuadas para la autenticación. La ICANN junto con otras organizaciones y comunicaciones pertinentes debería realizar un estudio y ofrecer un informe sobre cuáles deberían ser las mejores prácticas de autenticación cuando se consideran las distintas funciones y riesgos en el DNS.

En cuanto a los contratos y el financiamiento la recomendación es que, la ICANN debería trabajar para empoderar a las partes contratadas para que puedan adoptar mejoras a la seguridad para los sistemas de registración de dominios y los servicios de nombres autoritativos, según resulte práctico. Al hacerlo podemos asegurarnos de empoderar a las organizaciones para que implementen medidas de seguridad mucho más firmes para el DNS.

Y, a continuación, tenemos la financiación para los programas de búsqueda de fallas o bug bounty. Este es un tema realmente de mucho interés para el grupo porque hay distintas perspectivas en torno a él, cuáles son las ventajas, cómo se debería adoptar… Todos estamos de acuerdo, sin embargo, en que deberíamos en la ICANN conducir un esfuerzo para trabajar en la factibilidad de implementar estos programas de búsqueda de fallas porque hay distintas maneras, distintos modos donde la infraestructura del DNS no es propiedad de una organización o no está mantenida de la misma manera.

Entonces sería una ventaja tener un programa de búsqueda de fallas que se concentre en estas áreas y en software que permita identificar esas fallas, esas vulnerabilidades. Como es un tema tan polémico creemos que hay que hacer un estudio de factibilidad para determinar cuál es el mejor abordaje, ver también la eficacia en función de los costos y cuáles serían las entidades adecuadas que podrían llevar esto adelante.

También creemos que hay una necesidad de educar y de generar conciencia, pensamos que la ICANN debería trabajar para desarrollar programas educativos y comunicarlos, que alienten a las partes interesadas del DNS a establecer todos los mecanismos de autenticación basados en las normas que corresponda para todas sus interacciones, para que haya autenticación e informar a las partes interesadas de los riesgos asociados con esos esquemas débiles de autenticación.

A su vez, aquí se trata de aprovechar muchas veces en los ataques la ignorancia, entonces a través de la concientización y la educación podemos pasar a esquemas de autenticación mucho más sólidos.

El bloqueo de registros. La ICANN debería iniciar esfuerzos para mejorar la documentación y la comprensión de las funciones de bloqueo de registros y promover su uso cuando se adecuado, también mejorar la comprensión con respecto a las diferencias entre el bloqueo de registro y de registrador. Los registratarios deberían tener definiciones claras de qué ofrecen estas funciones, qué no ofrecen y cuál es la diferencia entre ellos.

A su vez, la ICANN también debería considerar facilitar la estandarización de los requisitos mínimos para los servicios de bloqueo de registros y registradores. Siguiente diapositiva, por favor.

Creemos que existe la necesidad de generar conciencia sobre las buenas prácticas para la seguridad de la infraestructura, la ICANN debe trabajar con iniciativas como manner y kindness para medir e informar sobre su adopción y utilizar esos informes para dirigir el material educativo que mejore el conocimiento sobre la seguridad de la infraestructura. La ICANN debería tomar las mejores prácticas que surjan de estas iniciativas y asegurarse de que las partes contratadas y la comunidad de la ICANN las conozcan.

Cuando no existen estas prácticas la ICANN debería alentar su desarrollo y su implementación, y promover la adopción también de funciones que mejoren la seguridad del DNS a través del ecosistema, como DMARC, SPF, TLSA, DANE, DNSSEC, etc.

La siguiente recomendación tiene que ver con el bloqueo y le filtrado del DNS. La ICANN debería crear materiales educativos e informativos que ayuden a la comunidad de la ICANN, a las partes contratadas y a otras partes interesadas a entender los riesgos y beneficios del bloqueo y el filtrado del DNS por motivos de estabilidad y seguridad en toda la comunidad de la infraestructura global del DNS.

Con respecto a la respuesta a incidentes, la ICANN junto con las partes que corresponda debería fomentar el desarrollo y la implementación de un proceso de respuesta ante incidentes formalizado en toda la industria del DNS que permita la interacción con otros en el ecosistema. Este tipo de iniciativa incluiría el manejo de la respuesta a los incidentes y también la protección compartida de la información sobre incidentes y las amenazas.

Esto es para asegurarse de que no haya ninguna brecha en la funcionalidad operativa y que de haberla se pueda identificar. En la recomendación E6 se habla de la toma de conciencia sobre los canales encubiertos, la ICANN debería publicar material educativo sobre el uso de estos canales encubiertos como vectores de ataques que pueden verse como un uso indebido del DNS en sí mismo y, por lo tanto, tienen que ser manejados junto con otras cuestiones relativas al uso indebido del DNS.

Con respecto a las dos principales prioridades que podemos seleccionar de todas las recomendaciones que formulamos creemos que, en primer lugar, tenemos la recomendación E3, investigar las buenas prácticas adecuadas para la autenticación y, en segundo lugar, la recomendación E5, respuesta ante incidentes. Siguiente, por favor.

Bueno, le doy la palabra nuevamente a Merike.

MERIKE KÄO: Muchísimas gracias. Para toda persona que quiera tener más información sobre el grupo de análisis técnico y repasar su carta orgánica, su documento de definición de alcance, el plan de trabajo y sus plazos, las agendas de reuniones, los apuntes y los recursos, ingresen a este sitio.

Como se mencionó, este informe estará disponible junto con un blog la semana la semana próxima y quiero anticiparles que tiene muchísimo contenido mucho más detallado de lo que nosotros pudimos presentar aquí en este tiempo tan breve, pero creo que van a encontrar que es contenido sumamente valioso y el director ejecutivo de la ICANN también va a encontrar valor en este informe.

Bueno, ahora quisiera abrir el espacio de preguntas. No veo en este momento preguntas.

WENDY PROFIT: Creo que ya se respondieron por escrito todas las preguntas.

MERIKE KÄO: Si tienen alguna pregunta nueva pueden escribirla en la sección de preguntas y respuestas, y la vamos a responder aquí.

Muy bien, hay una pregunta: “¿Dónde se puede conseguir el informe final?” El informe final va a estar disponible la semana próxima junto con un blog y entiendo que también en el sitio Wiki que les acabo de

mostrar en una diapositiva van a tener allí la forma de acceder a ese informe.

La pregunta es: "¿Estas preguntas y respuestas acompañan el informe?" Lo dejo en manos del personal, "¿va a haber una transcripción de esto junto con el informe?"

WENDY PROFIT: Lo voy a verificar con el equipo de MTS.

MERIKE KÄO: Muchas gracias y gracias por la pregunta, Donna. Como saben, en los últimos 18 meses dedicamos mucho tiempo a este trabajo y los expertos para experiencia interfuncional ha sido excelente, quiero agradecer a cada uno de los miembros del equipo que contribuyó a redactar este informe. En este momento no veo ninguna otra pregunta.

En ese caso, quiero agradecer a todos los que participaron en esta sesión preparatoria y, una vez más, lean el informe cuando esté disponible la semana que viene y vamos a ver qué pasa después con este informe.

WENDY PROFIT: Hay otra pregunta en la sección de preguntas y respuestas, la pregunta es: "¿Cuáles son las principales motivaciones de los atacantes y de qué países son esos atacantes?" A ver si alguien puede contestar…

MERIKE KÄO: Yo voy a contestar la primera parte. Las motivaciones pueden ser varias, pueden ser personas, también hay bandas organizadas y esto puede tener origen en cualquier país, es la naturaleza del mundo virtual en el que estamos viviendo.

Bien, entonces cerramos la sesión, les agradezco a todos por participar.

**[FIN DE LA TRANSCRIPCIÓN]**