SAN JUAN – Taller sobre las DNSSEC, parte 2
Miércoles, 14 de marzo de 2018 – 10:30 a 12:00 AST
ICANN61 | San Juan, Puerto Rico

RUSS MUNDY: No sé si Geoff Huston va a estar en la presentación pero es uno de los coautores que también está aquí con nosotros. Tenemos una sesión de 30 minutos ahora para la presentación sobre KSK Sentinel.

WARREN KUMARI: Estoy viendo dónde me puedo sentar y que tenga micrófono.

Hola a todos. Veo que en la sala hay varios que ya han visto esta presentación. ¿Hay alguno que no la haya visto? Me parece entonces que va a ser bastante interactivo. En esencia, es un trabajo que hice junto con Geoff Huston y Joao, que creo que no está en la sala. Aquí viene Geoff a ayudar.

¿Cuál es el problema que intentamos resolver con todo esto? Como muchos ya mencionaron, queremos implementar el anclaje de confianza del DNSSEC, la KSK, y los usuarios no tienen la KSK. Los usuarios que usan resolutores de validación todavía no tienen la KSK. Se va a romper, se va a detener el DNSSEC. Eso significa para ellos que la Internet se va a parar porque sin DNSSEC nada funciona. Lo que más nos preocupa es que no

tenemos manera de medir el despliegue real de la nueva clave. Eso significa que no sabemos cuánta gente va a sufrir este quiebro cuando se produzca.

Hace poco nos contaron que existe esto que se llama RFC 8145 que se publicó a mediados de 2017. Lo que se supone que hace es señalar qué resolutores tienen DNSSEC. Eso es lo que queremos saber. Qué resolutores tienen qué claves y cómo van a funcionar. Lamentablemente, no es así. Lo que hace, como decía, es proveer reportes de los resolutores de validación del DNSSEC pero estos resolutores no nos dicen qué clave en particular tienen. En mi sótano, yo tengo un resolutor de validación que funciona en un contenedor. Yo lo puedo reiniciar. Estoy apagando esto porque recibo la traducción.

Yo tengo un resolutor en mi sótano que reinicio todos los días por razones largas de explicar y esto significa que este resolutor nunca tiene oportunidad de aprender la nueva clave. Para poder aprenderla y empezar a confiar en ella hay que verla y hay que tener una vida de 30 días. Mi resolutor nunca lo tiene porque lo reinicio. Sin embargo, para mí esto no es realmente importante. Nadie está enviando ninguna query. Es un resolutor que está en el bosque, que no hace ningún ruido porque nadie lo utiliza pero reporta estadísticas. Esto significa que aparece en el gráfico de resolutores que hacen registros según la RFC 8145.

Para aquellos que no conocen este gráfico, fue publicado por Verisign. Creo que fue en octubre de 2017 y muestra la progresión del despliegue de los nuevos anclajes de confianza. A mediados de julio se publicó la nueva KSK. A mediados de agosto expira el cronómetro de retención. Eso significa que todos tenemos que empezar a implementar los nuevos anclajes de confianza y empezar a reportar. Un 5%-6% de los resolutores, por algún motivo, no tomaron la nueva clave. Si la gente vio las presentaciones de la mañana habrán visto que este número subió al 30% y la verdad es que no sabemos por qué.

Más allá de eso, la RFC 8145 solo da reportes de resolutores. Esto no da reportes de usuarios y para nosotros es mucho más importante entender cuál es el impacto en los usuarios y la implementación de la KSK. Está bien saber si los resolutores van a funcionar pero lo que realmente nos importa es cómo va a afectar a los usuarios de la Internet.

Tenemos un nuevo proceso que se llama KSK Sentinel que requiere una serie muy sencilla de actualizaciones del software resolutor y le permite a cualquiera que publica un nombre en el DNS establecer un servicio de medición. Lo que es más importante es que expone los resultados de las pruebas a los usuarios. El sistema actual de medición da reportes del resolutor a los operadores de servidores raíz y a la IANA, o a la IANA a

través de los operadores de servidores. Esto les permite a los usuarios individualmente ver su resolutor y ver si está okey o no.

También hacer mediciones de la Internet a gran escala. Seguramente ustedes han oído las presentaciones que hace Geoff sobre Google Ads u otros aspectos que sirven a gran parte de la población y que permite hacer pruebas. El plan es que Geoff haga una prueba usando esta infraestructura, el KSK Sentinel, para muestrear millones de usuarios y así tener informes mucho mejores de funcionamiento.

¿Cómo funciona la KSK Sentinel? El cambio sigue dos reglas muy sencillas. El resolutor de validación que fue actualizado para soportar esto hace todo el proceso normal de validación, toda la resolución normal del DNS. Cuando recibe una pregunta hace su trabajo estándar pero una cosa última que hace antes de enviar de vuelta la respuesta es que se fija si la etiqueta en el nombre a la izquierda empieza con esta cadena de métrica que es kskroll-sentinel-is-ta y un nombre de clave.

Si encuentra esta cadena y si tiene la clave en particular, es el ID de la clave, responde normalmente. Si no tiene el ID de la clave, toma la respuesta válida correcta y retorna un SERVFAIL. Esto lo que hace es Decir que durante la validación hubo cierto problema de validación de la resolución, intentó hacer la

resolución, buscó la respuesta y SERVFAIL es la respuesta genérica cuando algo anda mal.

La segunda regla es básicamente lo opuesto de la primera. Es kskroll-sentinel-not-ta. La pregunta a la que responde es que si no se tiene la clave, se tiene que responder normalmente. Si se tiene la clave, entonces se responde un SERVFAIL: Cuando lo vimos por primera vez esto nos parecía un poco extraño que se hagan dos preguntas, una siendo la opuesta de la otra. Era verdad y falso al mismo tiempo. Pero es exactamente así. Ambas pueden ser verdaderas y falsas al mismo tiempo.

¿Por qué? Veamos un ejemplo. Yo soy un resolutor de validación. Tengo soporte de Sentinel pero no se ve como un resolutor de validación. Tengo la nueva KSK. El id de la nueva KSK que se acaba de dar a conocer es 20326. Yo estoy trabajando y recibo una query de invalid.example.com. Este nombre en particular lo que implica es que es un registro firmado inválidamente, hago el procesamiento normal porque está firmado inválidamente. Por eso la respuesta es SERVFAIL. Hasta aquí nada cambió.

Luego hay una query de kskroll-sentinel-is-ta-20326.example.com. Hago todo el trabajo habitual, de siempre, el paso de resolución, el paso de validación y aparece una dirección de 20326. Esto es nada más que un ejemplo. Como tengo soporte de Sentinel y como estoy usando el id de clave

20326 respondo normalmente. La pregunta es: ¿Este es un anclaje de confianza lo que usted tiene? Como lo tengo, respondo a la pregunta con la respuesta que tengo.

Luego recibo un query de kskroll-sentinel-not-ta-20326. Hago la validación, recibo una dirección de IP del servidor autoritativo. No obstante, sí tengo y uso el ID 20326. Básicamente, no es que no tenga este anclaje de confianza. Por eso envío un SERVFAIL. No es que no tenga esta TA.

Para los participantes remotos, esta es la diapositiva siete. Todo lo que hemos hecho hasta ahora es sumar complejidad al DNS. Al hacerlo nos divertimos mucho pero en realidad debemos preguntarnos si es útil y cómo. ¿Pueden llegar a ver la diapositiva en pantalla? Invalid.example.com/fish, kskroll-snetinel-is-ta-20326.example.com/kitten y lo mismo con /puppy.

Aquí el plan es pedir a los usuarios que entren en una página web que tenga todo esto. Luego les pedimos a los usuarios lo siguiente. Cuando lanzan esta página, ¿aparece una imagen de un pez? Si aparece, puede ser un gatito o un cacharro, pero si aparece un pez significa que han logrado resolver exitosamente el dominio invalid.example.com. Si no lo hace significa que no están usando un resolutor válida. En ese caso, no nos importa la implementación de la KSK. De ninguna manera les afecta. Si pueden ver solo una imagen de un gatito y un cachorro, significa

que no reciben el registro inválido sino que pueden recibir a la vez el is-ta-20326 y el not-ta-20326.

Como lo ven, ambos simultáneamente, como ambos tienen y no tienen el anclaje de confianza significa que el resolutor que usan todavía no se actualizó con el soporte de Sentinel. Si solo ven la imagen de un gatito, eso significa que pudieron cargar is-ta-20326 y no pudieron cargar not-ta-20326. Eso significa que van a estar perfectamente bien durante el cambio de la clave. Tienen la nueva clave, están bien. Ahora, si solo ven la imagen de un cachorro, eso significa que solo tienen la clave antigua, que no tienen la 20326. Eso significa que cuando termine el cambio de la clave y la que tienen se elimine, su DNS se va a caer.

¿Estamos realmente planeando usar imágenes de peces, gatitos y cachorros? Lamentablemente, no. No se puede preguntar a todos los usuarios de la Internet que nos digan qué imágenes ven, de gatitos y demás. En cambio, les vamos a mandar un montón de JavaScript. Este JavaScript intentará cargar el equivalente el gatito, el pez y el cachorro y buscar cuáles de estos scripts pudieron resolverse hacia una prueba y luego indica cuál fue el resultado.

Con respecto a los gatitos, tampoco pasa lo mismo. No los vamos a ver. Tenemos una prueba que es ksktest.net. Como tengo un poquito de tiempo y están locos pero me dejaron usar

esta computadora, vamos a verificar que funcione. Vamos a tipear ksk-test.net. Está cargando los registros. Lo hizo. Está determinando que el resolutor que usa esta computadora es un resolutor validado y que es heredado, que todavía no soporta el método Sentinel. Esto significa que esta máquina en particular, y sé que a todos en la reunión de la ICANN no les podemos decir si van a sobrevivir o no el cambio de la clave. Esta es una imagen de pantalla de lo que hice, porque no estaba seguro de que fuera a funcionar.

La diapositiva nueve, perdón. Esta es entonces una revisión. Esta es la foto de los gatitos, que es lo que obligadamente tenía que mostrar. Seguramente la primera pregunta que me van a hacer es por qué tenemos gatitos que haciendo jardinería. La verdad es que no lo sé.

FREDERICO NEVES: ¿Están recabando los resultados de la página de prueba?

WARREN KUMARI: Más o menos. En mi página tengo un servidor que guarda estos recursos. Estoy registrando cuando la gente pide los tres registros. Lo que no se muestra es que cada registro tiene un número aleatorio y hay distintos números aleatorios. Sí se registra pero no consulto la información de los registros. No

tengo información suficiente. Sí tengo información suficiente para saber cuáles son los porcentajes pero la verdad, no me ocupé de hacerlo ni tengo intención de hacerlo porque la mayoría de los resolutores, por ahora, no han sido actualizados. Esto fue básicamente una prueba de concepto. Si leen el código, se darán cuenta de que fue solo una prueba de concepto. No tengo planes de hacer registro cronológico de los resultados por las implicancias de privacidad que esto tiene. Buena pregunta, igual.

VIKTOR DUKHOVNI: Warren, ¿conoce algún trabajo que nos lleve más allá del RFC 5011? Creo que podríamos hacer algo mejor que lo que estipula este RFC.

WARREN KUMARI: A ver, sí y no. Seguramente Frederico tiene algo que decir al respecto. Wes ha escrito un documento que señala que el documento 5011 en ciertos aspectos es vago. Uno de ellos es que facilita que nos disparemos en el pie con mucha facilidad. Hay otras áreas que no obstante pueden ser mejoradas. Hasta ahora, el problema tiene que ver con cosas que son culpa directa del RFC 5011. La gente implementó mal el RFC 5011 porque no pudo entender el estilo de redacción. Digamos que la gente configuró el anclaje de confianza de la manera que nosotros le dijimos al

comienzo. Abrir el archivo con BIND y confiar en los equals y poner la clave. Para los que no tienen BIND, las claves confiadas dicen: “Este es el anclaje de confianza y siempre lo va a ser”. No intenten implementar otro anclaje de confianza porque yo les voy a decir cuándo cambiarlo.

Esto nosotros lo dijimos, porque en su época la mejor práctica. De hecho, era la única práctica. Cuando empezamos a decir eso, se introdujo el RFC 5011 en los resolutores y se habilitó otro método, pero la gente no se preocupó en cambiar las claves para ser claves administradas. El problema de la 5011 o del cambio en general es que es muy común que la gente use cosas como VM o instancias Docker para correr sus servidores de nombres.

La 5011 dice: “Cuando se ve una nueva clave firmada con la clave antigua, no la confíen, por lo menos durante 30 días”. Eso significa que hay un sistema de archivos sin capacidad de escritura o si el servidor es seguro porque se ha eliminado la inestabilidad o lo que fuera, nunca va a prender la nueva clave.

En su mayor parte, estos problemas no son problemas del 5011 sino de cómo los usuarios configuraron las cosas incorrectamente, porque hicieron lo que nosotros les dijimos al principio de lo que tenían que hacer y luego no siguieron la nueva información o porque el nuevo sistema no pudo escribir la nueva clave. Si remplazamos 5011, no obstante van a continuar

los mismos problemas pero estoy de acuerdo en que la 5011 tiene muchas palabras.

Una persona una vez dijo que como nosotros esperábamos que este iba a ser un documento operativo, siempre tuvimos dos KSK implementados. Así funciona mejor pero estoy de acuerdo en que debería remplazarse el 5011. Se habló mucho de remplazarla pero esto implica, por ejemplo, sacar el anclaje de confianza de www.iana.org. Sí, ha habido algunas discusiones pero no buenas ideas.

VIKTOR DUKHOVNI: Me gustaría ver la capacidad de rollover con cualquier anclaje de confianza transferido. Pasar de ahí a una cadena de firmas en el DNS, inmediatamente sin un periodo de 30 días.

WARREN KUMARI: Creo que se podría empezar con la clave antigua, esperar 30 días y pasar a la nueva pero esto sería bastante horrendo.

VIKTOR DUKHOVNI: ¿Por qué no olvidamos los 30 días y lo dejamos en 0?

WARREN KUMARI: Habría que probarlo. Yo tengo otro sitio que es… No recuerdo el nombre. Keyroll.systems. A ver si funciona. Funciona. Fíjense, es

un nuevo gTLD. Este es el lugar equivocado. Este el sitio demo que se estableció hace bastante tiempo y que permite que los que operan el 5011 hagan un testeo. Es una clave que se aplica cada 90 minutos.

El problema es que cuando yo lo configuré, la mayoría de los resolutores no estaban esperando para el anclaje de confianza. Uno ponía la máquina y no funciona. La gente sabe bien qué es ese periodo de 30 días de espera. Los resolutores empezaron a decir que no estaban siguiendo la RFC y empezaron a seguirla y a esperar 30 días. Era una regresión que no esperasen los 30 días. Es bueno saber que sigue funcionando. ¿Quién más tiene preguntas? ¿Frederico?

FREDERICO NEVES: ¿Qué esperan ustedes si todo funciona en las próximas semanas del IETF? Esto es más para Geoff, esta pregunta. ¿Ustedes esperarían hasta que empecemos a hacer sus test o esperarían un mes y esperarían que todos apliquen estos nuevos resolutores? ¿Qué esperan?

GEOFF HUSTON: Necesariamente este es un cambio al comportamiento de los resolutores que operan de un modo que tienen el mismo banco del DNSSEC porque todas las respuestas tienen que mirar la

misma etiqueta y ver que haya una clave importante. Si es así, que se aplique el comportamiento. Por lo que yo sé, un módulo que no resuelve CZ.NIC ha implementado esto. BIND y Unbound y todo lo que ustedes usan, no se ha implementado.

Si ustedes quieren ver la porción de mercado de CZ.NIC, yo podría hacer ese test ahora y me mostraría esto. Si bien es importante ver a CZ.NIC, yo esperaría a que los tres tengan una integración en las relaciones que existen allí y luego sería bueno si el RedHat bug se pudiese integrar con un resolutor en sus lanzamientos. Esto sería bueno que ocurriera antes de agosto para tener datos. Como todo en el DNS, hay muchas variables y esto no se implementó hasta ahora. Yo no puedo hacer una medición en este momento porque no hay resultados que merezca la pena ver.

WARREN KUMARI: La gente que estaba mirando la presentación de [inaudible], había una línea de resolutores que tienen la RFC 8145, donde todo baja, y luego hay una subida muy pronunciada. Allí pareciera que hay gente que actualiza la versión de las resoluciones para este bug de seguridad. Lo que tenemos que hacer es esperar que se implementen los resolutores y que luego alguien exponga la vulnerabilidad para poder poner una

actualización. Hay que empezar a ver ahora. No soportar Sentinel es una vulnerabilidad.

JAAP AKKERHUIS: Hola. Soy de NLnet Labs. Nosotros estuvimos esperando para testear el Sentinel pero estamos en medio de Unbound en este momento. No es algo muy complicado.

WARREN KUMARI: Creemos que el sistema core es bastante estable. Para aquellos que no estuvieron siguiendo la actualización, cualquiera que sea el string que se use, se va a haber que se aplicó cuatro o cinco veces. Esto no es algo demasiado importante pero es algo que a nosotros nos parece que es estable. La implementación debería ser confiable.

RUSS MUNDY: Adelante, Geoff.

GEOFF HUSTON: Quería hacer un comentario que ilustra por qué tenemos una segunda implementación y qué es lo que era problemática de 8145. Cuando miramos el DNS hay dos perspectivas. Una es tratar de entender el comportamiento de los elementos individuales en el sistema de resolutores, es decir, resolutores

individuales y tratar de entender cómo estos resolutores individuales se comportan pero los usuarios no hacen esto. Ellos tienen una lista de resolutores y si no tienen la primera respuesta, van a la segunda o a la tercera. La verdadera pregunta es qué sucede, qué le sucede a los usuarios con cada uno de los resolutores.

Por ejemplo, si hay dos resolutores configurados localmente, uno valida y el otro no, el keyroll es irrelevante. Esto es así porque si no se sigue un keyroll, todo el tiempo van a SERVFAIL y SERVFAIL le va a decir: "Prueben el otro". El usuario va a estar bien incluso si los resolutores no lo están. Este Sentinel no va a descubrir los resolutores recalcitrantes. No tiene la intención de hacerlo y no lo va a hacer. Lo que sí puede decir es que antes de una implementación de llave, cuál pensamos nosotros que es la población de usuarios que podría quedarse en la mitad del camino sin resolutor que funcione. Este es el escenario de daño y es todo lo que hay que medir.

La pregunta de Viktor, qué pasa con los resolutores, cómo resolvemos esto. Si queremos este conocimiento en el DNS hay que pensar más y hacer más cambios a los protocolos o resolutores porque no tenemos esa capacidad hoy. Gracias.

WARREN KUMARI: Una pregunta más, Jaap.

JAAP AKKERHUIS: La pregunta que tengo yo es: ¿Tenemos una etiqueta que está reservada para este test específicamente?

GEOFF HUSTON: La etiqueta provoca el comportamiento. El dominio donde está ubicada esa etiqueta depende de mí y de usted y de cualquier otro que quiera operar o realizar este test.

JAAP AKKERHUIS: La pregunta que yo tenía es si existen otras etiquetas que ejerzan distintos comportamientos. ¿Hay un registro de IANA de etiquetas de comportamiento?

WARREN KUMARI: Sí, hay xn--. Algunos dicen que todas las etiquetas underscore no muestran un comportamiento en el DNS. Ciertos resolutores como BIND y algunos resolutores stub no pueden utilizar etiquetas underscore. Android simplemente no lo cargaría. Yo entiendo que estamos viniendo de un string que está documentado en algún lugar. Lo obvio sería poner un nombre de registro especial pero podemos también elegir un registro diferente, [inaudible], etc.

FREDERICO NEVES: Me olvidé de decir al principio que esta sesión está traducida al francés y a español. Están disponibles aquí los auriculares.

RUSS MUNDY: Vamos a agradecer a Warren y a Geoff por esta información y este trabajo.

ORADOR DESCONOCIDO: Tengo un comentario sobre xn--, no afecta al DNS sino a la próxima capa. Por lo tanto, es diferente.

RUSS MUNDY: Muy bien. Gracias a Warren y a Geoff, se lo agradecemos. El próximo orador es Ondrej. Ondrej Filip, de CZ.NIC. Vamos a escuchar sus experiencias en este proyecto.

ONDREJ FILIP: Buenos días. Mi nombre es Ondrej Filip. Trabajo para CZ.NIC. Quisiera hablar de un aspecto del proyecto que se llama el proyecto Turris. No es un CPE común, tiene algunas otras características. Se lo quiero presentar. ¿Qué es el proyecto Turris? Empezó hace un tiempo en 2013 y el foco principal tiene un nombre bastante raro pero la idea aquí es crear maneras de poder extenderse en la red que recolecten información, validarla y también brindar algunas reglas y recomendaciones de

seguridad. Esta fue la idea básica y después continuamos trabajando sobre eso. Decidimos que lo mejor sería un router y empezamos a trabajar en eso. También agregamos algo más móvil porque la situación en este campo es bastante mala. Muchos de esos routers tienen un firmware bastante raro. Hay actualizaciones que tienen bugs de seguridad y que tenemos que ver cómo poder solucionarlo. El apoyo de tecnologías como IPv6 y la validación de DNSSEC fue muy mala.

Continuamos de esta manera. Esperamos poder encontrar algún dispositivo en el mercado que nos dé una adición al firmware. No pudimos encontrar nada lamentablemente y el resultado fue que creamos nuestro propio hardware, nuestro propio router. Para el proyecto que acabamos de crear la primera generación que es el Turris 1.0 hicimos mil de esos dispositivos. Lo pueden ver en la pantalla. El router azul está arriba a la izquierda.

Tuvimos resultados muy interesantes. Quisimos extender un poco el proyecto. Creamos una nueva versión que se llama Turris 1.1 y luego hicimos unos mil de ellos. El foco principal fue el del público. No los dábamos en forma gratuita sino que se los dábamos a otras personas pero la gran mayoría de los routers estaban en la República Checa. Luego empezamos a publicar los resultados del proyecto. Algunos empezaron a preguntarnos si podemos comprarlo, si podemos conseguir uno. También hubo quien quiso sobornarme. Algunos tuvieron éxito con esto.

También decidimos ampliar el proyecto y creamos una campaña de crowdfunding porque no sabíamos muy bien si podríamos vender en el mercado estos dispositivos. Fue una campaña muy exitosa. Recolectamos mucho dinero y creamos este nuevo router llamado Turris Omnia. Tengan en cuenta que somos una organización sin fines de lucro. Por lo tanto, muchas de nuestras actividades no generan un ingreso. Esta es una adición a esta situación en este campo que esperábamos que mejorase.

Lo que es diferente en el Turris Omnia es que es de código abierto, como todo lo que hacemos. Tanto el software como el hardware es de código abierto. El hardware es muy poderoso. Tenemos mucha más memoria que las mismas máquinas en esta categoría y por eso podemos hacer muchas más cosas con este hardware. El sistema operativo se llama Turris OS pero básicamente está tuneado de un modo tal que sea un OpenWRT. Lo principal es que tiene actualizaciones automatizadas. Cada vez que hay un problema, si hay algún bug de seguridad, hay que dar una nueva clave de raíz o hacer una actualización y nosotros lo hacemos bastante seguido. No son solo reparaciones de seguridad sino que, como dije, el hardware es muy poderoso y el dispositivo se puede usar para muchas otras cosas, no solo como router.

Iniciamos este proyecto de seguridad, la seguridad es lo clave aquí. El énfasis principal es que este dispositivo no debe permitir

hacer una configuración insegura. Nos va guiando a través del proceso de configuración. No permite que haya puertos abiertos, etc. La comunicación con el centro, la forma en la que está configurado, tiene su propio criptochip, tiene la actualización de siempre. También tiene muchas otras cuestiones de seguridad que no están vinculadas con esta charla pero puede correr como honeypot. Así es como recolectamos la información. Hace análisis de flujo. Puede ver si hay alguna otra vulnerabilidad en Internet o algo inesperado.

Como dije, también brindamos los resultados del análisis colectivo. Por lo tanto, tiene un firewall adaptativo de acuerdo a la situación de seguridad, que también puede ser un VPN, etc. Es completamente compatible con IPv6. Es muy flexible. Se puede correr también LXC en otro servidor como máquina virtual, lo cual nos muestra lo poderoso que es.

Lo más importante para nosotros es que está haciendo validación de DNS por defecto, con lo cual una de las cuestiones de este proyecto es que no es tan fácil. Un comentario más. DNS utiliza mucho en este dispositivo. Por ejemplo, vemos a través de DNS un conjunto de claves que el dispositivo debe utilizar porque si hay alguna instancia o un incidente de seguridad el key set se va a ver comprometido y en ese caso podemos pasar a otro conjunto de claves. Por eso el DNS es importante y por lo tanto la validación también lo es en este dispositivo.

Cuando nosotros empezamos había muchas lecciones por aprender. Como dije, el sistema operativo se desarrolla constantemente. Fuimos bastante naif al pensar que íbamos a tener validación de DNS, pero vimos que no era tan simple.

Quisiera ahora referirme a un grupo de organizaciones que son muy creativas en cómo trabajan con el DNS y el DNSSEC. Muy rápidamente vimos que nosotros teníamos que proveer algunos GUI adicionales, formas de informar de por qué no está funcionando bien el router. Algunas actualizaciones en el sistema operativo. Los problemas principales son que los ISP suelen tener alguna falla en la infraestructura. Creo que esto puede ocurrir mucho. Puede haber una implementación vieja del DNS que esté causando muchos problemas. Puede haber un recursor upstream. A veces son muy creativos e instalan middleboxes y hacen magia con el tráfico en el DNS. Hay algunas razones para hacer esto. Quizá en algún momento de la historia instalaron esto y se olvidaron. Algunos de ellos simplemente redirigen el tráfico del puerto 53 a algún recursor, lo cual resulta bastante complicado para ver cómo operar en esa red, si es que el resolutor está fallando y eso suele ocurrir bastante.

Algo que no solamente ocurre del lado de los ISP sino que es un problema antiguo, empezó con uno de los resolutores. Estos blue books utilizan Unbound y Omnia utiliza los Knot resolvers. Con esa implementación tenemos una experiencia muy

interesante. Tuvimos algunos bugs en los resolutores y de nuevo esto se debe al efecto de que podemos actualizar el sistema inmediatamente y así pudimos encontrar muchos bugs y resolverlos rápido. Esto se debe fundamentalmente a que los resolutores del proyecto están muy bien testeados.

Por último, pero no menos importante, muchas veces hay problemas con algunos servidores autoritativos que fallan. Básicamente, estos son los problemas de EDNS de los cuales voy a hablar un poquito más adelante.

Esta es la página que hicimos solo para el DNS. Como ven, hay una descripción bastante extensa de lo que está pasando porque mucha gente no lo usa. Intentamos educar sobre lo que pasa con el DNS y hay varias opciones. Pueden usar o no usar el [forwarding] y también pueden inhabilitar por completo la validación DNSSEC. Si eligen cliquear en Disable DNSSEC, habrá varias advertencias. Lamentablemente es la última opción de conectividad indicando que los routers no se podrán conectar a la Internet.

Luego hay varias pruebas que muestran lo que está funcionando mal. Algunos son lo suficientemente valientes como para reportar lo que sucede al ISP. Nosotros podemos resolver algunos de los problemas en algunas redes de ISP pero algunos ISP creen que tienen seguridad perfecta, que DNS hack es la

mejor solución. Lamentablemente, a veces no es así. Estos dos botones ayudan mucho.

Como conclusión, en su mayor parte los problemas son en los ISP. Hay algunas cuestiones, algún problema de seguridad con el DNS. A veces introducen algunas soluciones y se olvidan del tema. Es necesario hablar con ellos. No es algo que el usuario pueda hacer solo. Tratamos de ayudarlos pero no ocurre con frecuencia. Tuvimos que introducir una interfaz de configuración con pruebas incorporadas que ayuda mucho porque por lo menos ayuda a entender el problema. Si el ISP tiene un operador con cerebro, a veces entiende lo que está implicado. Así se va a reducir además el número de llamadas a soporte.

La semana pasada en DNS-OARC se implementó una prueba y los resolutores empezaron a analizar lo que va a pasar en el 2019. Este es un lugar donde se puede saber más información sobre lo que va a pasar en el 2019. Por favor, si ustedes creen que tienen problemas, por favor, dígannos, así podemos probar su dominio. Después de febrero de 2019 habrá otra serie de circunstancias.

Quiero decir una última cosa. Estamos por lanzar una nueva versión del Turris. Como ven, es un dispositivo muy flexible, con muchas partes con las cuales se podrá jugar. Es modular. Vamos

a hacer campañas nuevamente de crowdfunding. Si les interesa este proyecto, cliquen en el sitio. Eso es todo. Muchas gracias.

RUSS MUNDY: Gracias, Ondrej. Jacques.

JACQUES LATOUR: ¿Con flexibilidad ustedes se refieren a que este dispositivo lo agarramos y nos lo llevamos?

ONDREJ FILIP: Me parece que una palabra mejor es modular. Usted podrá diseñar su propia cadena de enrutadores.

VIKTOR DUKHOVNI: ¿Tienen estadísticas sobre las mejoras en los ISP, gráficos que publiquen cada tanto?

ONDREJ FILIP: Nuestra empresa es checa y como operamos en la República Checa a veces tenemos dificultades para organizar estadísticas fuera del país. Es importante el porcentaje de usuarios que tienen problemas. La mayoría de los ISP, o por lo menos los grandes ISP, tienen un soporte pero es importante el porcentaje de usuarios que tienen problemas.

FREDERICO NEVES: Ondrej, ¿las versiones antiguas de hardware son compatibles con el software nuevo?

ONDREJ FILIP: Sí. Tiene el mismo sistema operativo aun cuando la plataforma de la CPU es distinta. Son compatibles. Tienen las versiones más actualizadas de todo.

FREDERICO NEVES: ¿Ustedes soportan alguna otra plataforma? Está basada en OpenWRT. ¿Alguna otra plataforma puede correr el software de Omnia?

ONDREJ FILIP: En realidad no. No hay demasiado en el mercado que digamos. Incluimos en el sistema de configuración hay características de seguridad como honeypots y demás. Es algo que podríamos explorar.

RUSS MUNDY: Hay un micrófono ahí atrás.

ABDALMONEM GALILA: Soy Abdalmonem Galila. Los administradores prefieren no hacer validación porque les parece difícil administrar el DNSSEC o los servidores con validación de DNSSEC. ¿Este Turris va a disminuir la carga de administración?

ONDREJ FILIP: Sí. Es poco realista creer que el 100% de los ISP tendrán la misma versión de enrutador. No creo que sea realista esperar que no tengan trabajo pero sí, con el Turris la validación está cerrada para el usuario. Sería lo ideal que se cerrar aun más a las computadoras personales y al teléfono celular pero al cerrarse solo al router con Turris, la administración es mucho menor.

RUSS MUNDY: Gracias, Ondrej. Ahí tengo otra pregunta. Hay un micrófono volante y otro en la mesa.

ORADOR DESCONOCIDO: Tengo una pregunta. ¿La validación DNSSEC se hace en CPE? ¿Eso está bien?

ONDREJ FILIP: ¿Por qué no iba a estar bien? Es un router hogareño y la validación se hace ahí, así que está bien. El título es Validación

en CPE, que es el equipo en la instalación del cliente. Es el enrutador hogareño. Eso concuerda con el título.

ORADOR DESCONOCIDO: ¿Quién valida?

ONDREJ FILIP: El enrutador en el hogar.

ORADOR DESCONOCIDO: ¿Qué software usan en la instalación del cliente?

ONDREJ FILIP: ¿Para la validación de DNS?

ORADOR DESCONOCIDO: Sí.

ONDREJ FILIP: Como decía, la versión antigua usaba Unbound y todos los Omnia, la mayoría de estos dispositivos, utilizan un software que nosotros desarrollamos en CZ.NIC.

ORADOR DESCONOCIDO: CPE usa Unbound o Knot resolver, ¿no?

ONDREJ FILIP: Sí.

RUSS MUNDY: Durante la presentación me di cuenta de que alguien de mi ISP, donde yo vivo, está sentado a la mesa, Joe de Comcast. Yo uso un router Turris en mi casa y tengo acceso directo si tengo problema pero debo decir que después de tres años de usar el Turris en casa y con la validación de Comcast, no tuve ni un problema. Funciona muy, muy bien. Quería decirlo en voz alta. Gracias, Ondrej, por su presentación. Creo que tenemos que seguir adelante.

ORADOR DESCONOCIDO: Si combinamos la presentación del cambio de la KSK y Turris, ¿Turris hará el cambio automáticamente y habrá que hacer alguna intervención?

ONDREJ FILIP: Por supuesto, es automática.

RUSS MUNDY: Gracias, Ondrej. El siguiente orador de la sesión de la mañana es Jake Zack, de .CA/CIRA. ¿Dónde está? Será usted. La presentación la hará Jacques Latour.

JACQUES LATOUR: Jake no se encontraba bien. Tuvo que irse porque estaba resfriado. Me haré cargo en su nombre de esta presentación. Esta presentación habla de la nueva generación de signer que CIRA acaba de implementar. Vamos a hablar un poquito sobre esto. Primero una breve reseña, similar a lo que vimos a la mañana. Tenemos 2.7 millones de dominios de los cuales 2.400 están firmados. Algunos registratarios están presentes en esta sala. No hay mucho que esté pasando en este campo.

Hace un par de reuniones de la ICANN, hace un par de años, presentamos nuestra solución con el signer de alta disponibilidad BIND y junto con eso pusimos una infraestructura de DNSSEC abierto y el HSM Gemalto. Migramos con el cambio de la KSK. Migramos toda la infraestructura con la nueva solución de firma. Esta es la charla de hoy.

La configuración que armamos hace unos cinco o seis años era una infraestructura de muy alta disponibilidad. Estábamos mitigando el riesgo de añadir fallos de DNSSEC. En ese entonces, generamos una zona dos veces. La firmamos con distintos signers, con OpenDNSSEC y BIND. Hicimos extensas validaciones de zonas para poder comparar y asegurarnos de que no hubiera diferencias. Luego publicamos estas zonas en la Internet.

Al ir a producción, el primer año encontramos algunos bugs que podrían haber sido operativos. El valor de ese sistema demostró

que funcionaba. La lección aprendida fue importante. Aprendimos mucho de esta infraestructura. Así produjimos algo más eficiente. Utilizamos Oracle como base de datos y también como standby, siempre con datos actualizados. Era un poco complicado ir al sitio de backup.

Teníamos una base de datos activa y de backup. Usamos la versión beta de OpenDNSSEC cuando se instaló y fue la misma versión que usamos en producción. Nunca actualizamos esa versión. Algo que funciona bien no hay que cambiarlo. Luego tuvimos muchos problemas internos. Con la validación de las zonas, cuestiones de terminal. A lo largo de los años hicimos algo de customización para que la configuración heredada pudiera funcionar.

El proceso. Lleva 30-35 minutos generar una zona. Está basada en CRON. Generamos la zona, la firmamos, hacemos un par de validaciones, mucho copiado de archivos. El archivo de zona es SEP, para ver cómo se compara con DNSSEC. Medimos, copiamos la zona en el sitio de backup, firmamos la demostración en el sitio de backup, comparamos todo. Es un proceso de manipulación de datos bastante extenso. Con el tiempo lo fuimos optimizando.

El sistema. Nunca tuvimos una caída de la zona. No tenemos failover automático de sitio a sitio. Esto es algo que queríamos.

Todos los validadores, todos los servidores eran blades con mucha copia, con mucho procesamiento para hacer la zona. En esa época era demasiado. Usábamos AEP keyper, que tenía un límite de cinco años. Empezaban a morir entonces consideramos remplazarlos con balanceadores de carga mucho mejores y un proceso mejor. El AEP keyper hay que manipularlo manualmente, poner tarjetas. En ese entonces servía pero luego las cosas se modernizaron. Los HSM son mucho más eficientes y ofrecen la misma seguridad.

En lo que hace a la validación, al principio, comparar ambas zonas nos permitió encontrar muchos bugs y encontramos situaciones problemáticas en la implementación. En .CA firmamos también dominios de segundo nivel porque tenemos provincias. Tenemos delegación a tercer nivel. Esto generó problemas en la validación de zona. Cuando alguien pone el registro DS, también tenemos legacy para cuatro niveles de zona. Tenemos ciudad, provincia. Cuando agregamos el DS al cuarto nivel, la ciudad no estaba firmada. No muchos validadores soportan este tipo de infraestructura. Llevó un tiempo resolver estas cuestiones. Además, BIND y ODS utilizan las firmas de manera distinta. Cada tanto, Jake tiene que ir ahí y limpiar el signer, porque estamos comparando BIND y ODS. A veces hay que hacer algunas intervenciones manuales para

reiniciar el signer, en especial durante el fin de semana de la Super Bowl o los fines de semana largos. A Jake no le gusta esto.

La nueva configuración que tenemos ahora es mucho más sencilla. Pasamos de 16 máquinas físicas a 8 máquinas virtuales. Queríamos tener cuatro al principio, para que sea más simple, pero después quisimos que el distribuidor tuviera su propia instancia de zona. Todas estas máquinas están en distintas zonas de seguridad con firewall interno. Es una arquitectura mucho más prolija. Tenemos generación, firma y validación en un equipo. Luego tenemos dos para disponibilidad y dos para distribución. Así funciona.

Después de varias evaluaciones decidimos usar Gemalto, Luna, Safenet. Es una de las grandes compañías de HSM. La gente los llama con distintos nombres. Nosotros los llamamos Gemalto y nos gustan porque podemos hacer casi todo lo que queremos con ellas. Tenemos particiones. El motivo por el cual pasamos de AEP keyper a Gemalto es que la solución de signer que tenemos está integrada en el nuevo servicio que queremos desarrollar, que es el servicio de firma de DNSSEC. Queremos usar esta infraestructura para aprovechar las zonas. Entonces las zonas de segundo nivel se van a firmar y se retornarán al cliente sin tener que replicar toda la infraestructura. El Gemalto es una buena infraestructura que soporta todo esto.

Hay mucha capacidad. Permite hasta 20 particiones, varios años de claves para cada una de las particiones. Es muy flexible. Otra cosa es que era mucho más fácil con Gemalto hacer la ceremonia de cambio de la clave. Con AEP keyper llevaba toda la vida. Con Gemalto y con el proceso que tiene es una hora en lugar de varias horas la ceremonia. Es más fácil el proceso.

Otra cosa que hicimos es pasar del Oracle estándar al Oracle ODA y Dataguard. Este es el equipo Oracle que es activo. Es bastante fácil para el registro. Generamos el signer DNS. Genera activo/activo en ambos sitios. Luego se distribuye en las zonas prácticamente en tiempo real en el sitio primario y el sitio de backup. Nuestro sitio de backup está un segundo por detrás del de protección. Funciona muy bien. Es un poco caro pero funciona.

No hacemos dual-sign. Tomamos ODS. Fue una decisión. No tenemos más problemas con nodos terminales vacíos. Usamos Springbatch, orquestación, etc. La generación de la zona funciona bastante mejor ahora con la firma. Los HSM tienen bajo balance. No hay ningún punto de falla. Hay un HSM disponible para la firma.

Utilizamos el mismo marco de control de seguridad de HSM que hicimos para la firma de la llave. Esta es una palabra que usó uno de ustedes que creo que no había oído en mucho tiempo: DPS.

Define la estructura para la gestión de las claves. Tenemos distintas personas en la oficina con distintos roles que hacen distintas cosas en HSM y con Gemalto dan el mismo apoyo que el AEP keyper. Tenemos un crypto officer. Tenemos un administrativo. Hay ciertas personas que tienen acceso a la sala y otras no. Con el AEP keyper pudimos replicar y mantener el mismo DPS, las mismas prácticas de DNSSEC que habíamos tenido anteriormente.

Todo esto funciona con el Gemalto. Es algo bueno porque no tuvimos que reinventar el proceso de ceremonia de la firma de la clave. Es mucho más fácil hacerlo con un pendrive. Hay un teclado y un pendrive que se puede utilizar para gestionar las criptoceremonias, por eso nos parece que era un poco más eficiente.

Al mismo tiempo que hicimos la implementación de la llave de HSM tuvimos que hacer una implementación de la KSK porque teníamos una nueva KSK en el HSM y el KSK antiguo en el AEP keyper. La nueva llave estaba en el nuevo HSM. Por lo tanto, nosotros lo hicimos lentamente para hacer la implementación de la KSK y del HSM. Es decir, también se aplicaba esto a la totalidad del proceso. Es un poco difícil verlo pero tenemos un KSK que estaba en producción e introdujimos una nueva KSK en la zona con el nuevo firmante.

Con el tiempo, migramos. Teníamos una llave y teníamos la nueva llave firmada con la llave anterior. Pasamos a HSM y la vieja llave se firmó con la nueva llave, etc. Hubo cambios que se fueron haciendo que fueron bastante directos. Todo el proceso de implementación de la llave fue bastante directo. Hubo un momento en el que hablamos de hacer un cambio en el protocolo. En base a lo que aprendimos en el DNS-OARC podría haber sido algo malo. Queríamos simplemente hacer una migración de la KSK pero lo hicimos despacio. Esperamos durante semanas pero no había ninguna prisa. Tuvimos múltiples KSK que se hicieron un poco grandes con el tiempo pero todo el proceso funcionó bastante bien.

Todo funcionó bien. Nadie nos mandó ningún email. Nosotros antes generábamos nuestras propias bases cada hora y ahora lo hacemos cada 30 minutos. De hecho, nos toma 11 minutos hacerlo. Podríamos incluso ir más rápido pero queríamos esperar un poco. La ceremonia de KSK la podemos gestionar remotamente. El HSM toma minutos para procesar y de hecho entrar al sitio y utilizar las cartas y HSM, eso ya no lo tenemos que hacer. El pobre Perl ya no está tampoco. Eso es todo en cuanto al proceso. No hay notas aquí. ¿Hay preguntas?

RUSS MUNDY: Gracias, Jacques. Quisiera saber si hay preguntas. Adelante, Robert.

ROBERT MARTIN-LEGENE: Hola. Soy Robert Martin, de PCH. Puedo hablar en español si quieren. Usted mencionó algo sobre el HSM anterior y el nuevo en cuanto a los cambios en la gestión. Sonaba como que ustedes tuvieron muchos beneficios por el cambio y que no necesitaban un hardware adicional de backup. ¿Esto se debe a que ustedes cambiaron o es solo una optimización que se hizo al mismo tiempo? Tenían el mismo Gemalto, la misma unidad y antes necesitaban un HSM total. ¿Ya no necesitan HSM ahora?

JACQUES LATOUR: Antes teníamos HSM offline. Nosotros hacíamos la ceremonia de firma. Generábamos la nueva clave y usábamos smart card. Con esa smart card entrábamos en las HSM y las reprogramábamos. Con Gemalto, hay un marco donde se puede tener un control y un teclado donde podíamos cambiar las distintas claves, hacerlo seguramente desde una ubicación central. Es decir, creo que es una llave negra la que crea la confianza en todos los HSM. Desde nuestra oficina podemos reconfigurar todos los otros HSM utilizando ese teclado. Es decir, el HSM offline estaba en un lugar de seguridad al que solo tu abogado podía acceder. Ahora tenemos el teclado en un lugar protegido.

ROBERT MARTIN-LEGENE: PCH utiliza HSM y nosotros no viajamos por todo el mundo cargando las llaves. No sé por qué hay que hacerlo.

JACQUES LATOUR: Cuando usted pone todo offline, todo el HSM queda offline, ¿no?

ROBERT MARTIN-LEGENE: Todas nuestras KSK HSM están offline, sí.

JACQUES LATOUR: Nuestras KSK están en vivo ahora. Si queremos agregar algún cliente nuevo lo podemos hacer ahí en ese mismo momento. No hace falta esperar a la ceremonia de la firma de la llave que uno hace trimestralmente para hacer altas y bajas de clientes.

ROBERT MARTIN-LEGENE: Hay pros y contras en los dos lados. ¿Tienen un vídeo de la ceremonia de la llave? ¿Es algo que ustedes publican?

JACQUES LATOUR: No se publica pero si lo quieren ver…

ROBERT MARTIN-LEGENE: Sí, lo quiero ver.

JACQUES LATOUR: Le va a costar una cerveza.

ROBERT MARTIN-LEGENE: Adelante, Joe.

JOE ABLEY: Recuerdo los primeros días en que se aplicaba DNSSEC y qué es lo que pasaba en la raíz, incluso los modelos de HSM. En un punto, ese era el único tipo de HSM que estaba certificado a un nivel que el Departamento de Comercio de Estados Unidos requería a ICANN que usara. No había mucha elección en ese momento. Parece que ahora todo el proceso evolucionó de lo que era adecuado en la zona raíz, que estaba focalizada en la seguridad física en algo que es más adecuado para las operaciones. Hay mucha gente que copió a ICANN cuando diseñó sus procedimientos. Creo que esa evolución es algo bueno de escuchar.

ORADOR DESCONOCIDO: Viktor.

ORADOR DESCONOCIDO: Soy de AFNIC. Tengo una pequeña pregunta sobre el proceso. Creo que tiene más que ver con las calificaciones. Usted dice que

con el nuevo proceso se demoran unos 11 minutos. ¿Todavía hacen una generación de archivo allí completa?

JACQUES LATOUR: Sí.

ORADOR DESCONOCIDO: ¿Consideraron usar algo más dinámico?

JACQUES LATOUR: Sí.

ORADOR DESCONOCIDO: ¿Por qué no lo hicieron?

JACQUES LATOUR: Se necesitan 11 minutos para hacer la zona total. Si pudiésemos mantener el proceso que tenemos dentro de los 15 minutos sería bueno, pero solo tenemos 2.000 delegaciones firmadas. Una vez que lleguemos a los millones, revisaremos.

ORADOR DESCONOCIDO: Esa era mi segunda pregunta. Si ustedes van a hacer el mismo proceso con 10 o 20 personas en la delegación de la firma, ¿eso escala?

JACQUES LATOUR: Eventualmente. Si se adopta en .CA para DNSSEC, entonces vamos a tener una solución dinámica.

ORADOR DESCONOCIDO: La última pregunta. ¿Hicieron algún test con ZSK? Sé que el proceso es más largo con 2048. ¿Testearon ustedes eso?

JACQUES LATOUR: No creo que lo hayamos hecho. Los niveles de desempeño entre Gemalto y AEP son 10 veces más rápido.

ORADOR DESCONOCIDO: Lo digo porque sé que hay un factor entre Gemalto y AEP con distintos tamaños de la llave. A veces la diferencia no es tan grande. Se deben hacer algunos testeos.

RUSS MUNDY: Muchas gracias, Jacques. Nuestro próximo presentador es Joe Crowe, de Comcast, quien nos va a hablar de los anclajes de confianza negativos.

ORADOR DESCONOCIDO: Tengo un breve comentario. Estamos comparando dos cosas diferentes. Hasta donde yo sé, el Keyper sigue siendo el único nivel para HSM validado en el mercado. Gemalto es nivel tres.

JACQUES LATOUR: Y no tenemos ningún requisito de certificación.

ORADOR DESCONOCIDO: Ese no es el comentario. Solamente hago un comentario sobre lo que dijo Joe.

JOE CROWE: Buenas tardes. Joe Crowe, de Comcast. Soy ingeniero sénior. Hacemos DNS, NTP y DHCP. En Comcast hacemos unas 500.000 millones de queries por día. Hacemos validación de DNSSEC desde 2012. DNSSEC escala. Si están ahí fuera, les permitimos que validen DNSSEC. Es fácil. ¿Qué significa esto para Comcast? Cuando falla DNSSEC, nosotros tenemos la culpa. La gente cree que nosotros bloqueamos los sitios web. Los clientes muy rápidamente vienen a nosotros cuando no pueden acceder a su sitio. Yo sé que este es el lugar del que todos hablan. Aquí estamos hablando de HBO Now. En cuanto ellos lanzaron su sitio, la validación de DNSSEC falló. No podíamos validar correctamente y Twitter explotó. Estábamos rompiendo la neutralidad de la red. Hay gente que se incluyó en un resolutor

de no validación y Google estaba haciendo lo mismo desde que aplicaron la validación de DNSSEC.

Una de las soluciones temporarias era poner un anclaje de confianza negativo. ¿Por qué hicimos esto? Es muy grande para que falle. Hay una instancia de cuestiones de seguridad. ¿Sabemos nosotros si nasa.gov, state.govs…? Disculpen, a veces son muchos .gov. ¿Sabemos si realmente tienen temas de seguridad o son cuestiones operativas?

La mayoría de las veces tenemos experiencias donde nos dice que sí son cuestiones operativas. Muy pocas veces vemos un tema de seguridad. Desde que yo estoy en Comcast haciendo esto, creo que nunca he visto un tema de seguridad. Todos han sido temas operativos. ¿Qué hacemos en ese caso? Tenemos algunas opciones mientras sigue fallando el dominio. Podemos apagar la validación DNSSEC, deshabilitarla o simplemente poner un anclaje de confianza negativo para ese dominio específicos que permita que continúe resolviendo con los resolutores que tenemos con el hecho conocido de que falla la validación DNSSEC.

Implementar un anclaje de confianza negativo. Cuando lo empezamos a hacer lo que hicimos fue tener un buen proceso. Hay que reunirse con el equipo para ver cómo y por qué lo hacemos. Tenemos que saber cómo lo implementamos en todos

los resolutores. Internamente nosotros utilizamos muchos proveedores para estar seguros de que tengamos un proceso y que el proceso funcione para todos los proveedores porque si sigue fallando hay que saber cómo implementarlo. Hay que ser consistente con el proceso. Si hay algo que cambia en cuanto a cómo el proveedor lo está implementando, tenemos que estar seguros de haber actualizado todo correctamente dentro de la automatización y que el equipo sepa lo que tiene que hacer.

Queremos saber cuáles son los riesgos de que ese dominio siga fallando. Queremos saber si va a haber una causa asociada a esto, si es que va a fallar durante mucho tiempo. Cuantas más llamadas recibimos en Comcast, más costoso es para nosotros. Tenemos que ver si está fallando por un tema operativo. En ese momento hacemos nuestras verificaciones para ver que nos conectemos con la gente adecuada, ya sea por email, por Twitter. Hacerle saber a la gente que vimos que el dominio falla y que estamos conectándonos con la gente adecuada.

Tenemos nuestro Twitter @ComcastDNS, que está muy bien gestionado por nuestro equipo. Luego tenemos que automatizar. Tenemos que estar seguros de que si estamos tocando más de 25 servidores, más de dos en realidad, tenemos que automatizar todo. El anclaje de confianza negativo empieza a pasar al liderazgo sénior. Si nosotros le podemos probar a nuestro liderazgo sénior que sí está fallando por un tema

operativo y que hemos contactado a la gente adecuada pero que está tomando más de 15 a 20 minutos o 30 minutos en volver a tener una respuesta, si es un sitio grande como nasa.gov o state.gov o HBO Now, tenemos que estar seguros de que lo implementemos en el NTA porque la causa asociada podría ser un gran fracaso pero tenemos que demostrar al liderazgo sénior que estamos haciendo lo correcto.

La automatización ayuda a escalar. Nosotros tenemos múltiples proveedores con diferentes comandos para implementar las NTA. Si hay un error y hay algo que no funciona, va a dejar de funcionar del mismo modo. Lo podemos reparar bastante rápido de ese modo de la misma forma que con un equipo podemos hacer un test en el laboratorio. Todos nos dicen: “Yo hago los testeos en producción” pero no es el mejor lugar para hacerlos.

La automatización básica en Comcast. Utilizamos nuestras herramientas de automatización. Tenemos datos de pilar que nos permiten tener un solo lugar con el dominio que nosotros creemos que está fallando. También nos permite poner los datos pilares por un solo script y en un solo proveedor. Tenemos un comando que se ejecuta hacia cientos de servidores. Lo podemos hacer con una implementación push. Podemos implementar una sola área y luego implementar después en todos lados. Esto implica que vamos a necesitar entre 2 y 10

minutos, dependiendo de cómo lo testeamos, cómo lo implementamos y que lo hagamos sin errores.

Nuestra estructura básica para los datos pilares, como vemos aquí a la derecha, es un formato YAML. Tenemos un NTA cliente y un NTA interno. Todas estas son malas prácticas internas que pueden hacer que falle DNSSEC. Hay una delegación inadecuada. Cuando estamos tratando de implementar DNSSEC internamente, este es uno de los obstáculos más grandes que tenemos. Cuando aplicamos todos los NTA a nuestros resolutores, como dije, puede haber un formato YAML y los datos van a ser consumidos por scripts, que son consumidos por otro archivo y después hacemos nuestro testeo.

La mayoría de ustedes saben cómo se hace la identificación de fallos. El fallo de DNSSEC genera un SERVFAIL. Si se puede hacer una exploración, ese es el primer paso. Luego se testea con otros resolutores de validación DNSSEC para garantizar que no sea solo el resolutor propio. DNSviz.net es su amigo. Si ustedes quieren activar validación de DNSSEC en sus resolutores pueden usar este dominio como dominio de prueba para asegurar que se está validando o en este caso que no se está validando correctamente.

En el caso del tema de la implementación de la clave, vamos a hacer un cache flush generalizado para arreglar los fallos de

DNSSEC en ese momento. Algo que surgió con la conversación con los operadores es cómo compartir los NTA con los grandes como Google, Comcast y otros validadores de DNSSEC. Internamente hablamos de automatizar las zonas y usar DNSviz y cargar las propias zonas para hacer chequeos para hacer el Cron para ver si están funcionando bien con DNSSEC. Si fallan, envían una alerta por email. En ese momento, identificar el problema antes de que salga al mundo. A veces los TTL juegan a nuestro favor. En este caso, state.gov falló durante un tiempo. Después de un rato se resolvió. Fue simplemente un cache flush lo que tuvimos que hacer. Eso es todo. No sé si tienen preguntas.

RUSS MUNDY: Una pregunta para Joe. ¿Paul? Acérquese al micrófono y diga quién es.

PAUL WOUTERS: Como dice [John Gilmore] sabiamente, si no podemos no confiar en nuestros amigos, ¿en quién no podemos confiar? En este caso no sabríamos si ponemos un anclaje de confianza negativo por fines maliciosos, imagínense que el gobierno nos pone un arma en la cabeza y nos dicen: “Tienen que hacer esto porque nosotros lo exigimos”. ¿De alguna manera, ustedes publican los anclajes de confianza negativos que han insertado? Por supuesto, ¿cómo evitan la vergüenza, que es algo que nadie

quiere? Sería bueno si tenemos alguna manera de auditar lo que ustedes están haciendo.

JOE CROWE: En este momento no tenemos nada publicado. Estoy de acuerdo con usted en que este muro de vergüenza no es la mejor manera de llamar la atención a la gente de lo que está funcionando mal pero lamentablemente en Comcast tuvimos que hacer saber a nuestros clientes que teníamos conocimiento de que había un problema. Por eso el Twitter de @ComcastDNS resulta muy útil. Ahí podemos decir: "Sabemos que este sitio web falla en la validación DNSSEC. Hay una chance de arreglarlo y de ahí en más seguimos adelante".

En lo que hace a la publicación de los registros, lo hemos hablado desde hace un par de días. Creo que eso tiene que ser la decisión de la comunidad en su conjunto. Decidir todos cómo vamos a publicar algo así. No me imagino que una compañía como Comcast pueda dictar este tipo de acción.

RUSS MUNDY: ¿Alguna otra pregunta para Joe? Robert.

ROBERT MARTIN-LEGENE: ¿Qué ocurre si DNSSEC está habilitado en Twitter.com y falla?

JOE CROWE: Llegado el momento, trataríamos de encontrar otra manera. Nuestro soporte de frontline sabría que DNSSEC está fallando para los grandes dominios. En este momento nos ocupamos de los más grandes, los sitios que pueden causar la mayor conmoción en la gente.

VIKTOR DUKHOVNI: La última pregunta. Sé que el equipo de mail tiene el mismo proceso para dominios mail que fallan. ¿Tienen la misma logística o algo distinto?

JOE CROWE: Es totalmente aparte. El equipo de mail tiene sus propios procesos. Es un proceso distinto del que tenemos nosotros.

RUSS MUNDY: Está entrando gente para otra reunión a las 12:15. Tenemos un fallo de agendas aquí. Bueno, nuestro almuerzo no va a estar listo hasta dentro de un rato. Hay un conflicto de salas. Creo que hay un error de agenda aquí. Bueno, bien. Tenemos que cambiar. Nuestro comité de taller no sabía lo que usted dice. Vamos a tener que dejar la sala. El almuerzo está planeado para las 12:15 o 12:20. Si les parece, vamos caminando despacito

hasta allí y el quiz lo hacemos después. Los tickets del almuerzo son estos. Tengan en la mano el ticket. El almuerzo será en la terraza del tercer piso. Tomen sus cosas, sus tickets del almuerzo. Reanudamos a las 13:30.

ORADOR DESCONOCIDO: Tengo una petición, que la gente llegue a tiempo. Tengo muchas diapositivas.

ORADOR DESCONOCIDO: Además, tenemos que estar seguros de que tenemos la sala.

RUSS MUNDY: Sí, de vuelta a las 13:30.

[FIN DE LA TRANSCRIPCIÓN]