Día Triple-I del GFCE @LACIGF2023, 3 de diciembre de 2023, Bogotá, Colombia

Informe de Roberto Zambrana, Lito Ibarra y Maarten Botterman

Resumen

El domingo 3 de diciembre de 2023, LACIGF incluyó el Día Triple-I del GFCE por segunda vez en la región de América Latina y el Caribe (ALC).

El Foro Global sobre Experiencia Cibernética (GFCE), como parte de las actividades del Día Cero del Foro Latinoamericano y del Caribe de Gobernanza de Internet, LACIGF 16, organizó el taller GFCE Triple-I "Creando juntos una experiencia de Internet más confiable". Este fue un taller híbrido que se llevó a cabo el domingo 3 de diciembre de 2023, con el propósito de:

• Explicar los aspectos más relevantes de los estándares abiertos de Internet, como DNSSEC, DANE, RPKI, ROA, TLS, DMARC, DKIM, KINDS, MANRS, SPF e IPv6, para soportar comunicaciones más confiables.
• Compartir e informar sobre buenas prácticas llevadas a cabo por diversas organizaciones del ecosistema de Internet, que contribuyen a mejorar la confiabilidad de Internet y la seguridad colaborativa; segmento que presentó varios ejemplos de buenas prácticas en la región LAC y también en otras regiones;
• Promover el intercambio entre los participantes para desarrollar y comprometerse con acciones concretas que ayuden a mejorar el ecosistema de Internet de la región.

Este taller contó con el apoyo de LACIGF (https://lacigf.org/), ICANN (http://www.icann.org), LACTLD (https://www.lactld.org/), LACNIC (https://www.lacnic.net/), nic.br/cgi.br (https://cgi.br/), Internet Society (http://www.Internetsociety.org) y EasyDMARC, y partes interesadas de éstas y otras organizaciones, que trabajan en el desarrollo de Internet en nuestra región LAC participaron en el taller, tanto en el rol de ponentes como de participantes, incluyendo el gobierno, el sector privado y la comunidad técnica. Se basó en los resultados del taller anterior en La Paz, Bolivia, organizado por LACIGF en 2019 (ver informe).

Con agradecimiento a todos los que ayudaron a que esto sucediera, y especialmente a Rafael Lito Ibarra y Roberto Zambrana. Además, no podríamos haberlo hecho sin el invaluable apoyo de la Secretaría del LACIGF, la organización COLNODO, que ayudó a lograr todos los arreglos logísticos en Bogotá.

Maarten Botterman, facilitador del GFCE Triple-I, explicó que la agenda incluyó tres bloques, con el fin de desarrollar los objetivos descritos. Se inició con la bienvenida de Lito Ibarra, agradeciendo a los asistentes por su participación en un domingo y cediéndole la palabra a Maarten Botterman.

Maarten compartió las palabras introductorias del taller, comentando los desafíos de los temas de seguridad y confianza en el contexto latinoamericano y caribeño. Luego describió la estructura del taller, explicando cada uno de los segmentos: Estándares, Buenas Prácticas y Próximos Pasos.

Finalmente, Maarten compartió el trabajo realizado hasta el momento, y particularmente las conclusiones a las que se llegó en el evento realizado en La Paz, en agosto de 2019.

Luego de revisar la agenda de todo el evento y explicar la metodología de intervención, comenzaron las presentaciones.

BLOQUE I - Mejor uso de los estándares abiertos de Internet actuales

El primer bloque sentó las bases para comprender el panorama actual de los estándares y mejores prácticas de Internet abierta, sus implicaciones prácticas y los esfuerzos de colaboración necesarios para mejorar su implementación en América Latina y el Caribe. El formato interactivo permitió a los participantes contribuir al diálogo, fomentando una comprensión compartida de los desafíos y oportunidades en este aspecto crítico de la gobernanza de Internet. La atención se centró en el uso y la utilidad de los estándares, protocolos y mejores prácticas de Internet abierta, que son importantes para la integridad y seguridad del DNS, el enrutamiento y el correo electrónico (DNSSEC/TLS/DANE, RPKI/ROA, DMARC/DKIM/SPF) e IPv6. Estos estándares son aceptados globalmente y representan conocimientos de vanguardia que, cuando se aplican, pueden ayudar a reducir los riesgos del uso de Internet y el correo electrónico en la actualidad. Estos también se reflejan en el Manual Triple I de GFCE. A continuación encontrará un diagrama que indica cómo se interrelacionan estos estándares:

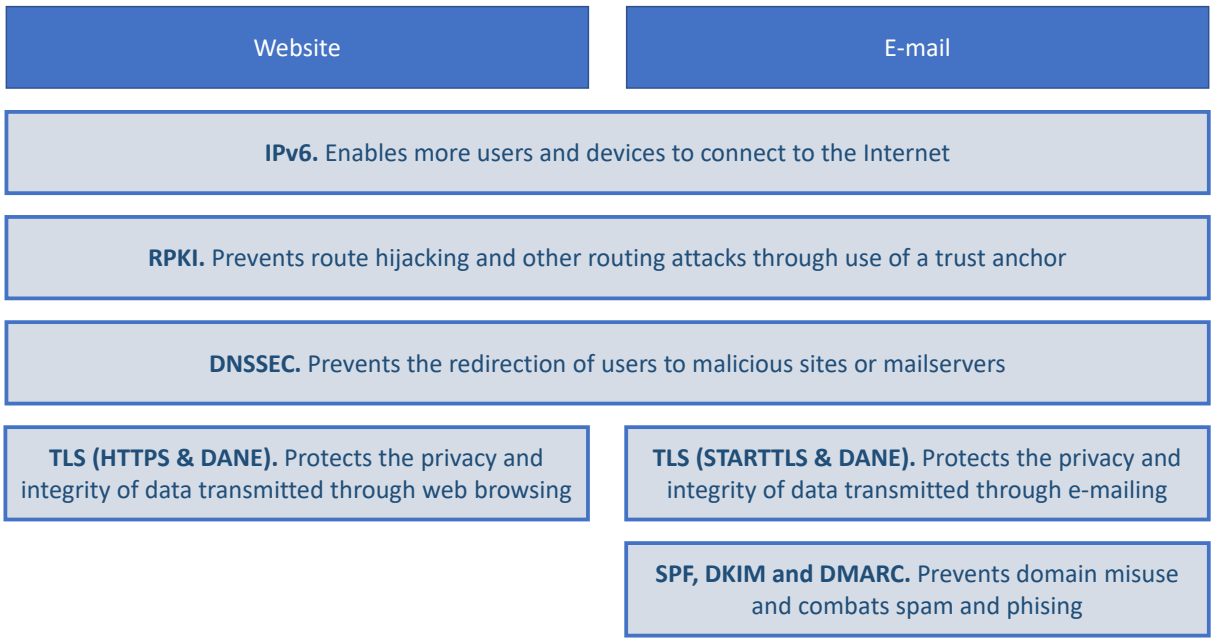

Fig.1: Los modernos estándares abiertos de Internet actuales con consideraciones de seguridad integradas

DNSSEC, TLS y DANE

Nicolás Antoniello, de ICANN (OCTO para la región LAC), presentó el tema de la implementación práctica y la importancia de DNSSEC, DANE y TLS para proteger el Sistema de Nombres de Dominio (DNS) y garantizar la integridad de los datos durante la transmisión. Estuvo de acuerdo en que hoy en día hay mucho en juego y que se debe hacer todo lo que podamos para garantizar una "confianza justificada".

Para que el DNS funcione de forma más segura, requiere que los operadores de registro y los registrantes firmen sus nombres de dominio. Esto debería ser facilitado por los registradores, proveedores de alojamiento de DNS y operadores de DNS, proveedores de servicios de Internet, operadores móviles, proveedores de alojamiento, etc., que deberían activar la validación DNSSEC para los dominios firmados. Extensiones de seguridad de DNS (DNSSEC): utilizan criptografía de clave pública y firmas digitales para proteger los datos de DNS proporcionando (1) autenticidad del origen de los datos (es decir, "¿esta respuesta realmente provino del servidor DNS correcto?") y (2) integridad de los datos. (es decir, "Los datos relacionados con el servidor DNS no han sido modificados después de la firma").

Sin embargo, DNSSEC no proporciona confidencialidad para los datos DNS, a menos que se combine con estándares como HTTPS (DoH – RFC 8484) o TLS (DoT – RFC 7858) y logre el cifrado DNS entre el cliente y el solucionador. Transport Layer Security (TLS) es un protocolo criptográfico que proporciona seguridad de extremo a extremo de los datos enviados entre aplicaciones a través de Internet garantizando

autenticación, confidencialidad e integridad, permitiendo que las aplicaciones cliente/servidor se comuniquen a través de Internet de forma segura (evitando escuchas, manipulación y falsificación de mensajes), utilizando certificados digitales firmados por un tercero (Autoridad de Certificación).

Para ir más allá de la protección de DNSSEC (idealmente en combinación con SSL/TLS o HTTPS), la autenticación de entidades nombradas basada en DNS (DANE – RFC 6698) permitirá a los administradores de un nombre de dominio certificar las claves utilizadas en los clientes TLS de ese dominio o servidores almacenándolos en el DNS. Esto permite a los propietarios de dominios especificar qué autoridad de certificación (CA, por sus siglas en inglés) puede emitir certificados para un recurso en particular, ya que hoy en día existen muchas CA.

En combinación con la Autenticación de Entidades Nombradas basada en DNS (DNS-based Authentication of Named Entities - DANE) (DANE es un protocolo que ayuda a autenticar la identidad de los puntos finales de Internet utilizando la infraestructura DNS protegida por DNSSEC), los usuarios tendrán las mejores garantías de integridad de los datos y los puntos finales.

En la Guía de implementación de DNSSEC se puede encontrar una lista de verificación de implementación de DNSSEC con elementos de acción ajustables cuyo objetivo es simplificar su recorrido hacia la implementación de DNSSEC.

ICANN apoya el desarrollo de capacidades de DNS y DNSSEC y mucho más: comuníquese con los equipos de TE o GSE, descargue la Guía o consulte el programa KINDNS que está configurado para promover las mejores prácticas para los operadores de DNS.

RPKI y ROA

Ignacio (Nacho) Estrada (LACNIC) se centró en el rol de la Infraestructura de Clave Pública de Recursos (RPKI) y las Autorizaciones de Origen de Ruta (ROA), y discutió los desafíos del enrutamiento que involucran las direcciones IP. Explicó que, para el enrutamiento de Internet, es importante que se registren las direcciones IP anteriores y posteriores a la dirección específica. Básicamente, el enrutamiento se ejecuta en BGP (Border Gateway Protocol), un modelo de confianza que originalmente no se creó para ser seguro, sino para funcionar, y en el que las interrupciones pueden causar cortes y alteraciones en la comunicación. Con el tiempo, cada vez más fugas en las rutas han provocado cortes, ya sea intencionalmente o por error.

En resumen, mediante el despliegue global de RPKI:
1- Las redes firman sus prefijos, es decir, "crean ROA" y:

2- Las redes validan la “firma de otras redes”.

Esto es para evitar el "secuestro de prefijo" (es decir, que alguien pretenda que está originando un bloque de IP que no le pertenece) y la "fuga de ruta" (es decir, anunciar una ruta por alguien que no debería hacerlo), garantizando la integridad de la fuentes. Firmar es una cosa; sin embargo, comprobar si la firma es correcta cierra el ciclo (es decir, la validación). Esto lo hace RPKI.

Nacho lo explicó muy vívidamente haciendo una dinámica participativa y muy ilustrativa para explicar RPKI y ROA. Al colocar a los participantes en la sala, y hacerlos conectarse como servidores autónomos, así como el rol de la autoridad certificadora, mostró cómo RPKI y ROA son buenas prácticas y estándares que buscan evitar el secuestro de direcciones IP y prevenir la IP incorrecta o ilegítima. (Protocolo de Internet) aborda los anuncios para que tengan éxito.

DMARC, DKIM, SPF

Gerasim Hovhannesyan de EasyDMARC profundizó en la importancia de DMARC (Autenticación, Reportes y Conformidad de Mensajes basados en Dominio), DKIM (Correo Identificado con Claves de Dominio) y SPF (Marco de Políticas del Remitente) en la Autenticación de Correo Electrónico y la Protección contra Ataques de Phishing.

Hoy en día, el problema es que cualquiera que esté en Internet puede enviar un correo electrónico en nombre de otra persona. Los dos grandes cambios en 2023 son:
1- Detectar correos electrónicos de phishing se ha vuelto mucho más desafiante debido al uso de IA;
2- El volumen y las áreas objetivo de los ataques de phishing han aumentado drásticamente.
De todos los ataques exitosos a nivel mundial, el 93% se habría evitado si se hubiera aplicado la seguridad adecuada al correo electrónico. Es crucial establecer mecanismos para verificar la autenticidad del remitente y la integridad del mensaje.

Los estándares mencionados anteriormente, en conjunto, manejan en gran medida estos problemas. SPF permite a los propietarios de dominios especificar qué servidores de correo están autorizados para enviar correos electrónicos en su nombre. DKIM agrega una firma para verificar que el contenido no ha sido alterado y que el mensaje efectivamente fue enviado por el remitente reclamado. Y DMARC se basa en SPF y DKIM para brindar protección e informes adicionales al permitir a los propietarios de dominios especificar cómo se deben manejar sus correos electrónicos si no superan las comprobaciones de SPF y/o DKIM.

DMARC hace que el correo electrónico sea realmente seguro y, una vez que comienzas a monitorearlo, la implementación es relativamente fácil. Sin embargo, es importante utilizar bien DMARC: hoy en día, una política que simplemente "rechace" correos electrónicos que no se pueden confirmar a través de SPF y/o DKIM provocará que muchos correos electrónicos no le lleguen en absoluto. Actualmente, la cuarentena es probablemente una mejor política: el peligro se contiene, pero aún se puede controlar.

En el debate, Nico subrayó la importancia de proteger Internet y el correo electrónico, pero que sería muy importante hacerlo mediante la implementación de estándares y buenas prácticas en lugar de regulaciones. Nacho no considera que pueda producirse ningún impacto especial que deba preocuparnos. Sin duda, la Inteligencia Artificial cambia las reglas del juego y, sin duda, traerá muchos cambios en el tema de la seguridad, como nos recordó Gerasim. Todos estuvieron de acuerdo.

BLOQUE II - Inspiración a partir de acciones de buenas prácticas

Durante el segundo bloque del día, tuvimos presentaciones y discusiones sobre una serie de buenas prácticas globales y buenas experiencias de la región que se consideran potencialmente relevantes para el desarrollo de capacidades e inspirar acciones en la región.

Medición de la resiliencia de Internet

Christian O'Flaherty (ISOC para la región de ALC) presentó el Índice de Resiliencia de Internet (IRI), un indicador derivado de pilares clave que evalúan la resiliencia de Internet de un país. Estos pilares incluyen Infraestructura (existencia y disponibilidad de infraestructura física que proporcione conectividad a Internet), Rendimiento (capacidad de proporcionar servicios de Internet fluidos y confiables), Seguridad (capacidad de resistir interrupciones intencionales o no intencionales) y Preparación del Mercado (capacidad del mercado para auto regularse y ofrecer precios asequibles). Destacó la importancia de la recopilación de datos de más de 30 indicadores diferentes, incluida la higiene de las rutas. Se puede acceder a las clasificaciones de países a través del portal pulse.internetsociety.org. Además de la resiliencia, Pulse también rastrea los apagones de Internet; qué estado de despliegue de las tecnologías es crítico para la evolución de Internet; y Concentración de servicios (cuánto se concentran los servicios en manos de unos pocos).

La definición de resiliencia de Internet utilizada es: "Una conexión a Internet resiliente es aquella que mantiene un nivel aceptable de servicio frente a fallas y desafíos para el funcionamiento normal". La atención se centra en Internet, no en las aplicaciones y servicios que se encuentran sobre Internet. Cabe señalar que los datos se obtienen de fuentes públicas externas y no siempre están actualizados, por lo que

son meramente orientativos. Sin mediciones nacionales, es difícil validar los datos, pero la metodología utilizada es reproducible y "robusta" en ese sentido.

Este recurso de medición, disponible gratuitamente para todos, puede ser utilizado por los responsables políticos y de toma de decisiones para comprender mejor las diferencias locales y regionales con respecto a diversos aspectos, de modo que se puedan establecer planes de mejora específicos. Quienes abogan y ejercen presión para lograr más inversiones y mejoras específicas pueden comprender mejor los verdaderos "puntos débiles", así como en qué países aparentemente se abordan con éxito.

Normas mutuamente acordadas para la seguridad de enrutamiento (MANRS)

Nayreth González (Embajadora de MANRS) presentó las medidas que los operadores de red pueden tomar de forma voluntaria según lo descrito en las Normas Mutuamente Acordadas para la Seguridad de Enrutamiento (MANRS), que es una campaña originada por ISOC dirigida a la adopción de mejores prácticas para la prevención de incidentes de enrutamiento. Como responsable de un Punto de Intercambio de Tráfico de Internet, Nayreth adoptó MANRS como forma de trabajar y, como embajadora de MANRS, da un paso adelante para ayudar a mejorar MANRS y ayudar a estimular una adopción más amplia de MANRS.

El enrutamiento es un elemento clave para que Internet funcione. Hay más de 70,000 redes centrales (sistemas autónomos) en Internet, cada una de las cuales utiliza un número de sistema autónomo (ASN) único para identificarse ante otras redes. Los enrutadores utilizan el protocolo Border Gateway Protocol (BGP) para intercambiar "información de accesibilidad", es decir, sobre las redes a las que saben cómo llegar. Los enrutadores crean una "tabla de enrutamiento" y eligen la mejor ruta al enviar un paquete, generalmente basándose en la ruta más corta.

Border Gateway Protocol (BGP) se basa enteramente en la confianza entre redes. Se creó antes de que la seguridad fuera una preocupación y asume que todas las redes son confiables. No existe una validación incorporada de que las actualizaciones sean legítimas. Esta cadena de confianza se extiende por continentes y existe una clara falta de datos confiables sobre recursos.

Sólo en 2019, más de 10,000 interrupciones de enrutamiento o ataques (como secuestros, filtraciones y suplantaciones de identidad) provocaron una variedad de problemas que incluyeron datos robados, pérdida de ingresos, daños a la reputación y más. Alrededor del 40% de todos los incidentes de red son ataques; El 3.8% del total de Sistemas Autónomos en Internet se vieron afectados. Los incidentes son de

escala global, y los problemas de ruta de un operador se multiplican y afectan a otros. Por eso, el enrutamiento inseguro es una de las rutas más comunes para las amenazas maliciosas. Los ataques pueden tardar desde horas hasta meses en reconocerse, y los errores involuntarios pueden desconectar a países enteros, mientras que los atacantes pueden robar los datos de un individuo o mantener como rehén la red de una organización. Por lo tanto, es de vital importancia estar atentos y disponer de procedimientos. MANRS mejora la seguridad y confiabilidad del sistema global de enrutamiento de Internet, basándose en la colaboración entre los participantes y la responsabilidad compartida de la infraestructura de Internet. MANRS recomienda cuatro acciones simples pero concretas que los operadores de red deben implementar para mejorar la seguridad y confiabilidad de Internet.

Los operadores de red tienen la responsabilidad de garantizar una infraestructura de enrutamiento segura y sólida a nivel mundial. La seguridad de la red depende de una infraestructura de enrutamiento que erradique los actores dañinos y las configuraciones erróneas accidentales que causan estragos en Internet. Cuanto más trabajen juntos los operadores de red, menos incidentes habrá y menos daños podrán causar.

Además de los operadores de red, MANRS también aborda posibles acciones para los Puntos de Intercambio de Internet y les pide que adopten MANRS como práctica de trabajo. Desde 2020, MANRS también incluye un programa para CDNs y proveedores de nube que ayuda al requerir controles de enrutamiento de salida para que las redes puedan evitar que ocurran incidentes. Aprovechar el poder de interconexión de las CDN y los proveedores de nube puede tener un importante efecto indirecto positivo en la higiene del enrutamiento de las redes con las que interconectan, y sirven a muchos usuarios finales.

La seguridad es un proceso, no un estado. MANRS proporciona una estructura y un enfoque consistente para resolver los problemas de seguridad que enfrenta Internet. La adopción de MANRS mejora la seguridad y confiabilidad del sistema global de enrutamiento de Internet, basado en la colaboración entre los participantes y la responsabilidad compartida de la infraestructura de Internet. MANRS establece una nueva norma para la seguridad del enrutamiento: unirse a una comunidad de organizaciones preocupadas por la seguridad y comprometidas a hacer que la infraestructura de enrutamiento global sea más sólida y segura. El compromiso de adoptar MANRS realmente está creciendo en toda la industria. Y el observatorio MANRS realmente ayuda a comprender la preparación de una región hacia la ciberhigiene y la resiliencia; de ahí el llamado a la industria para que adopte MANRS, y a los gobiernos y los usuarios finales para que soliciten MANRS a sus proveedores de servicios.

Normas de intercambio de conocimientos y creación de instancias para DNS y seguridad de nombres (KINDNS)

Nicolás Antoniello, de ICANN (región OCTO LAC), presentó la iniciativa de ICANN KINDNS (Knowledge Sharing and Instantiating Norms for DNS and Naming Security), enfatizando la importancia de la configuración en la prestación de servicios de Internet y cómo este programa ayudaría a hacerlo de la mejor manera. Una salida posible. Al igual que la iniciativa MANRS, se trata de buenas prácticas que pueden implementarse en el contexto y uso del Sistema de Nombres de Dominio. Pidió una mayor colaboración entre los operadores para mejorar la resiliencia de Internet, así como la seguridad de la infraestructura. KINDNS es un marco simple que puede ayudar a una amplia variedad de operadores de DNS, desde pequeños a grandes, a seguir tanto la evolución del protocolo DNS como las mejores prácticas que la industria identifica para una mayor seguridad y operaciones de DNS más efectivas. Los operadores de cada categoría pueden autoevaluar sus prácticas operativas según KINDNS y utilizar el informe para corregir/ajustar prácticas no alineadas:

– la autoevaluación es anónima
– los informes se pueden descargar directamente desde el sitio web

Los participantes en la iniciativa KINDNS se convierten en una comunidad de operadores que se comprometen voluntariamente a implementar/adherirse a las prácticas acordadas. También se convierten en embajadores de buena voluntad y promueven las mejores prácticas, ya que cuanto más se difundan las mejores prácticas, más saludable será Internet.

ICANN está en el proceso de promover esta iniciativa en múltiples idiomas y continúa mejorando las herramientas, basándose en la experiencia de interacción con quienes participan y contribuyen. Se organizan talleres y seminarios web para aumentar la concientización sobre las prácticas de KINDNS como parte del programa general de concientización sobre la seguridad del ecosistema DNS de la ICANN. Se anima a todos los operadores a registrarse, seguir las prácticas y contribuir a la mejora continua de la plataforma.

Programa Brasil de Internet más seguro

Gilberto Zorello (NIC.br) presentó el Programa Internet más Seguro de Brasil, una iniciativa desarrollada por el Comité Gestor de Internet de Brasil (CGI). Este programa es un enfoque integral para introducir una serie de medidas que pueden implementarse en Brasil, dirigidas a la comunidad técnica de Internet en Brasil. Sus principales objetivos son:

1. Reducción de los ataques de Denegación de Servicio (CERT.br)
2. Mejora de la seguridad del enrutamiento de la red (MANRS)
3. Difundir las mejores prácticas de seguridad de DNS (KINDNS & TOP)

4. Difundir las mejores prácticas de seguridad para la configuración de sitios web y servicios de correo electrónico (TOP)
5. Fomentar la implementación de IPv6 en los usuarios finales y servicios de Internet (TOP).

Con esto, vemos un programa verdaderamente integral que aborda las prioridades también indicadas en el Manual Triple-I de GFCE, y es ejemplar como tal, para que otros países y regiones vean cómo el liderazgo y dar un paso adelante pueden ayudar a mejorar la confianza justificada en el uso de Internet y del correo electrónico.

El proyecto TOP mencionado anteriormente significa Teste Os Padrões, un sitio web de prueba para comprobar qué tan bien se han implementado los estándares modernos de Internet. Utiliza el código abierto proporcionado por la implementación holandesa Internet.nl con una interfaz web en portugués para atender a los usuarios brasileños en el idioma local.

Varios equipos internos del NIC.br participan del Programa (CERT.br, CEPTRO.br, Registro.br, IX.br, Sistemas), y en interacción con la comunidad desarrollan materiales técnicos y buenas prácticas, y sensibilizan a la comunidad técnica organizando y participando en conferencias, cursos y capacitaciones. También hay interacción directa con los operadores de red mediante reuniones bilaterales para explicar cómo implementar las mejores prácticas recomendadas en cada situación, cuando sea necesario. Para medir el impacto, NIC.br prueba periódicamente los sitios web para detectar su mala configuración (ver imagen a continuación).

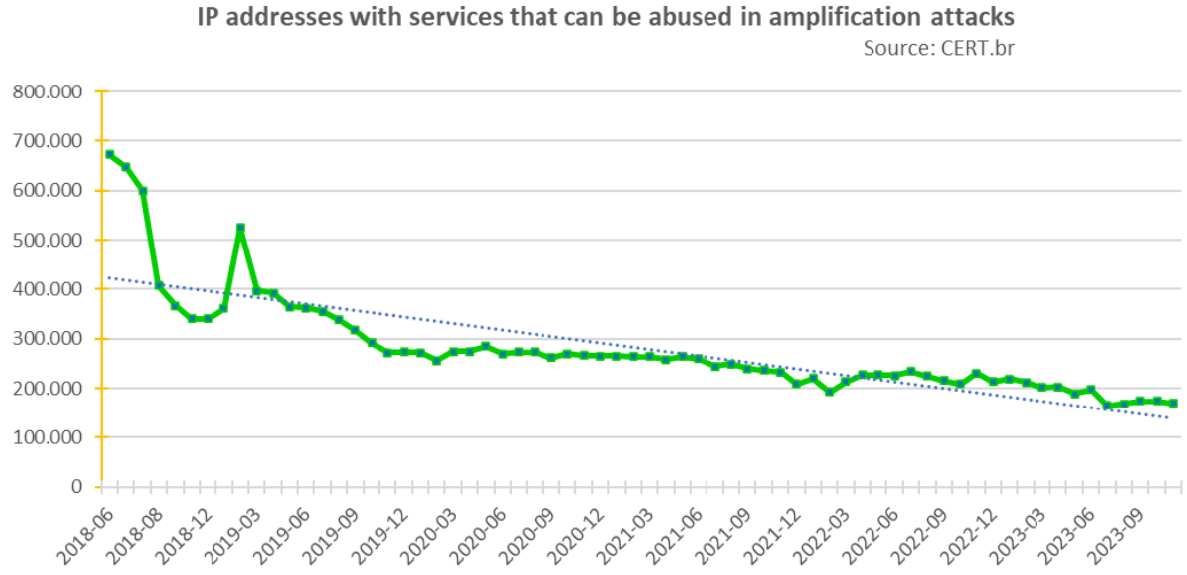

Fig. 2 – Cantidad de direcciones IP notificadas con servicios mal configurados (fuente: CERT.br)

La tendencia es clara: medir ayuda. Hay una reducción del 76% en direcciones IP mal configuradas desde el inicio del Programa. Gilberto ofreció su ayuda para el posterior establecimiento y desarrollo de tales actividades en toda América Latina.

Seguridad en IoT(Internet de las Cosas)

Posteriormente fue el turno de Ignacio (Nacho) Estrada de comentar sobre la seguridad en Internet de las Cosas (IoT), seguido de comentarios y contribuciones de Maarten y Lito.

Comenzó afirmando que los problemas de seguridad con IoT tienen que ver con la configuración y diseño de los dispositivos. Estos dispositivos se construyen a gran escala, y reutilizan otros componentes que puedan realizar varias funciones, no sólo las que el diseñador del dispositivo IoT busca ejecutar. Esto hace que el componente sea más barato. Este hecho supone un riesgo para la seguridad.

Por otro lado, la mayoría de estos dispositivos suelen venir con contraseñas preestablecidas que se obtienen en público fácilmente y la mayoría de los usuarios no los cambian cuando instalan el dispositivo, facilitando así la intrusión no autorizada del dispositivo.

Nacho ve tres tipos de problemas en torno a la seguridad de IoT: 1) Privacidad: si alguien tiene fácil acceso a una cámara, por ejemplo, puede ver la intimidad de mi casa u oficina, o tener acceso no autorizado a nuestros datos. 2) Manipulación de datos: los piratas informáticos pueden alterar la información en un dispositivo y causar problemas. 3) Secuestro de dispositivos IoT para realizar ataques de denegación de servicio y/u otros tipos de intrusión masiva.

Maarten comentó sobre los estándares, etiquetas y protocolos de seguridad para IoT que están siendo revisados o desarrollados por organizaciones internacionales, como IEEE. Los gobiernos pueden ser de gran ayuda al incluir en sus procesos de adquisiciones la demanda de estos estándares de seguridad para los proveedores. Etiquetado y certificación de seguridad y las características de privacidad serán un facilitador importante para que los usuarios finales realicen operaciones inteligentes y decisiones conscientes.

Finalmente, Lito mencionó que los temas propuestos para el Foro de Gobernanza de Internet este año, y seguramente en el futuro, han comenzado a incluir tecnologías emergentes, como la Inteligencia Artificial y el Internet de las Cosas, mostrando una creciente preocupación por su impacto para la humanidad.

Aceptación Universal

Lía Solís (Embajadora del Grupo de Estudio de Aceptación Universal UASG) explicó la importancia de mejorar la Aceptación Universal a nuevos Nombres de Dominio y scripts internacionalizados para nombres de Dominio y correo electrónico. Presentó el Llamado a la Acción para el próximo año, expresado por la UASG. El Plan de Acción pide:

Para las empresas:

- Organizar internamente y evaluar si los sistemas de su empresa cumplen con los estándares AU.
- Actualice sus propios sistemas de TI para que estén preparados para la AU. Consulte UASG026 UA-Readiness Framework, casos de prueba UASG004, ejemplos de código gratuitos y Guía de autocertificación EAI.

Para los gobiernos:

- Evaluar la posibilidad de incluir requisitos de AU en las licitaciones gubernamentales.
- Coordinar con sus administradores nacionales de ccTLD y los delegados del Comité Asesor Gubernamental (GAC) de ICANN para participar y fortalecer las acciones relacionadas con la AU.

Para la academia:

- Actualizar los sistemas de correo electrónico para admitir EAI.
- Actualizar los planes de estudio de TI para incluir la enseñanza y el aprendizaje de la UA y conceptos relacionados con la internacionalización del software.

El Plan de Acción también incluye un Día Mundial de la AU, que se celebrará el 28 de marzo, como se hizo en 2023 por primera vez. El objetivo es tener un evento global y una serie de eventos regionales y nacionales en el mismo período.

Bloque III: Planificación para una Internet más confiable: Mercado para la acción

Lito dio la introducción y Maarten presentó el resumen de los temas tratados en la mañana, entre ellos:

- "Confianza justificada en el uso de Internet y del correo electrónico", un tema importante que debe debatirse y avanzar de forma continua; hay recursos y herramientas de prueba disponibles en línea, usémoslos y contribuyamos a mejorar continuamente su utilidad;

Los comentarios recibidos son los siguientes:

- Esteban Lazcano comentó que es importante conocer los procesos, y por parte de los usuarios es importante tanto como de los actores que en muchos casos están

reunidos en diferentes organizaciones de las regiones, como LAC-ISP (Organización de Proveedores de Servicios de Internet de Latinoamérica y el Caribe), y otros. En particular, el interés es replicar iniciativas como éstas en los países a través de las cámaras de Proveedores de Servicios de Internet (ISP) existentes, u organizaciones similares;

- Maarten respondió que se pueden compartir documentos como el manual en el portal web. En particular, mencionó y ofreció los recursos de Triple-I (disponibles en línea) así como su propia experiencia;
- Rodrigo de la Parra comentó que es bueno organizar estos eventos, y que efectivamente cada actor de la comunidad técnica ha sido importante, y la ICANN cree que es bueno trabajar colaborativamente, sabiendo lo que estamos haciendo, pero también es importante medir, saber qué más debemos hacer, qué falta, o cómo podemos trabajar para mejorar lo que falta. Mencionó la importancia del índice ISOC y de la iniciativa brasileña.
- Maarten respondió que hay muchas cosas que se pueden hacer y Brasil es un ejemplo de lo que es posible. Y de hecho es tan sencillo que cualquiera puede hacerlo, colocando portales en un sitio web, para evaluarlo. La otra cosa importante es escuchar las ideas de los participantes en eventos similares en la región.
- Dominique Paz, de Argentina, mencionó su aporte es desde el aspecto legal. Y al respecto comentó las amenazas existentes en materia de seguridad, y un tema crítico tiene que ver con la capacitación, por lo que las experiencias presentadas son cruciales para las personas involucradas. Algo que tiene que ver con el derecho penal es que las empresas no reportan incidentes de seguridad, por lo que los usuarios que se ven afectados por estos incidentes no los conocen. Uno de los temas técnicos que comentó fue sobre la tecnología Network Address Translation (NAT), que no permite identificar los orígenes de la comunicación en Internet, y que probablemente esto debería resolverse mediante regulaciones que obliguen a la transición a IPv6;
- Gerardo comentó cómo iba avanzando la iniciativa brasileña, primero impulsada por el CGI, luego sumando MANRS y ahora sumando KINDNS. Busca mejorar constantemente su impacto, medirlo y el equipo está listo para ayudar a otros en la región de ALC a poner en marcha iniciativas similares;
- Luego tomó la palabra un participante de Honduras, mencionando que hay otras entidades que trabajan en estos temas, y que no debemos inventar la rueda, sino utilizar los recursos existentes. Esto fue reconocido y aceptado. Maarten expresó explícitamente que el objetivo es facilitar, acercar y cuando se encuentran brechas en lo que se necesita y lo que está disponible en una región, es importante buscar soluciones, en conjunto, con otras organizaciones de apoyo.
- Luego hubo un intercambio sobre la idea de regular protocolos. Honduras dice que prácticamente no es posible hacerlo. Sin embargo, Dominique cree que así debe ser. Nacho comentó que LACNIC no considera que forzar la transición a IPv6 por leyes nacionales sea un camino apropiado;

- Después, Raúl Echeverría comentó sobre la iniciativa del índice de resiliencia ISOC, y comentó que es un trabajo importante, que está en un proceso de maduración. También comentó la importancia de estos eventos. Habló sobre la falta de datos de seguridad, que nos impide ver la realidad de los incidentes de seguridad. Además, mencionó que hay que trabajar con las Pequeñas y Medianas Empresas (PyMES).
- Nicolás Antoniello comentó que todo lo que es Internet no es una construcción personal y en los últimos 20 años se ha dado cuenta de que es importante trabajar en equipo. No buscar soluciones parciales o fragmentadas. Es importante tener cuidado con las regulaciones que puedan afectar el ecosistema, y si acaso, desarrollarlas en conjunto.
- Lía Solís comentó que no es bueno trabajar bajo el enfoque de obligación. Pero también es importante escuchar y abordar otras demandas emergentes.
- Dina Santana Santos, de los Capítulos ISOC de Brasil y Colombia, comentó sobre la importancia del ambiente académico y su inclusión.
- Valeria Betancourt, de APC, preguntó sobre las iniciativas que existen para diseñar protocolos con enfoque de derechos humanos.

Tras estas interesantes aportaciones, Maarten cerró el evento agradeciendo a la organización y a los participantes su apoyo. Reiteró sobre la disponibilidad de documentación y soporte existente. También comentó cómo es posible trabajar en regiones, y en diferentes dimensiones. Parte de lo que hace GFCE es buscar con qué organizaciones y personas pueden trabajar en cada región y país.

Este informe se utilizará como base para el desarrollo de acciones futuras. No dude en enviarnos sugerencias e ideas para seguir adelante. Para obtener más información sobre GFCE Triple-I, incluidos los resultados de eventos anteriores, visite las páginas de GFCE Triple-I, si está interesado en mejorar la experiencia confiable de Internet en su región.

-=(fin del informe)=-