Seguridad y resiliencia de Internet

Ciberseguridad es un término amplio y algo impreciso que diferentes actores utilizan con diferentes significados, entre ellos "seguridad informática y seguridad de la información", seguridad de la infraestructura de Internet, seguridad de todo lo que esté conectado a Internet (incluidos los "servicios esenciales" como la distribución eléctrica), seguridad de los datos, aplicaciones y comunicaciones, seguridad de los usuarios de Internet (particularmente de los niños), y con frecuencia abarca nociones tanto de seguridad "nacional" como de seguridad "privada". De hecho, no hay un consenso generalizado con respecto al significado de este término.

Sin tratar de definir mejor el término ni proponer soluciones para todos los aspectos que pudieran recaer dentro de su ámbito, este trabajo explora los componentes fundamentales para la seguridad y la resiliencia del ecosistema de Internet: las soluciones técnicas y de políticas alineadas con las invariantes de Internet, la responsabilidad individual y colectiva del riesgo, y la colaboración.

Las invariantes de Internet

Internet ha experimentado cambios desde su creación y continúa evolucionando. Es importante comprender qué es lo que realmente permanece constante – las propiedades clave o invariantes "que han permitido que Internet sirva como una plataforma para la innovación aparentemente ilimitada, que resuman no solo su tecnología sino también su forma en términos de su impacto global y estructuras sociales" .[1]

Cualquier marco para abordar la ciberseguridad debe comenzar con una comprensión de las propiedades fundamentales de Internet que realmente hacen que este medio de comunicación global sea lo que es. A estas propiedades fundamentales las describimos como las "**invariantes de Internet**", ya que el éxito generalizado y continuo de Internet depende de que estas propiedades perduren.

Las dos primeras propiedades son el **alcance global y la integridad**.

La Internet es global porque cualquier punto extremo conectado a la red puede enviar paquetes a cualquier otro punto extremo. Un punto extremo podría ser una computadora portátil, un teléfono móvil, un sistema de navegación satelital con conexión a Internet, etc.

La integridad de Internet significa que la información recibida en un punto extremo es la que pretendía el remitente, sin importar dónde el receptor se conecte a Internet. Por ejemplo, independientemente de dónde se encuentre el usuario, dicho usuario debe recibir el mismo contenido al acceder a la página principal de la Internet Society en www.internetsociety.org. Un usuario podría decidir limitar el contenido que recibe en su dispositivo (por ejemplo, utilizando en su navegador el plug-in Ghostery para bloquear Google Analytics). Esto no afectaría la integridad de la comunicación. Sin embargo, si un ISP bloqueara el acceso de un usuario a www.internetsociety.org, eso sí interferiría con la integridad de Internet, dado que el ISP estaría desviando o eliminando la información antes que ésta llegara a su destino final. Lo significativo es que la acción no es tomada por un extremo de la red, sino más bien por un intermediario.

La tercera propiedad clave es **servir de apoyo para la innovación sin necesidad de pedir permiso.** Dicho de otra manera, se trata de la posibilidad de que cualquier persona pueda crear una nueva aplicación en Internet sin tener que obtener la aprobación de un órgano de gobierno. La historia de Internet está repleta de ejemplos de tecnologías y servicios asombrosos que fueron posible gracias a la libertad de introducir nuevas aplicaciones o servicios sin tener que pedir permiso al gobierno, al ISP ni a cualquier otra persona. Quizás el ejemplo mejor conocido sea el del HTML (HyperText Markup Language), que dio origen a la red de redes. Este lenguaje fue desarrollado por un investigador del CERN en Suiza, quien lo puso a disposición para que otros lo utilizaran. Si Tim Berners-Lee hubiera tenido que pedir permiso, ¿existiría Internet? ¿La idea de proveer enlaces a datos hubiera sido rechazada, acabando con el desarrollo de los servicios de búsqueda como Google? ¿Facebook tendría mil millones de usuarios activos al mes ? ¿Existirían servicios de recolección y visualización de datos colaborativos (crowd-sourced) como Ushahidi ? ¿Y Wikipedia, Twitter, YouTube, las aplicaciones para dispositivos móviles, el software de mapas, la música vía streaming y cientos de otras cosas que usamos todos los días y damos por sentadas?

La cuarta propiedad es la **apertura** – una Internet desarrollada abiertamente y abierta para que cualquiera la utilice. Internet se basa en normas técnicas que se desarrollan de manera abierta y por consenso y luego se ponen a disposición de todos [por ejemplo, HTTP (para acceder al contenido web), SMTP (para el correo electrónico), SIP y RTP (para comunicaciones de voz y audio), etc.].

Una quinta propiedad de que debemos preservar es la **accesibilidad de Internet**. Esto va más allá de que las personas puedan acceder a información y servicios en línea – se extiende a la capacidad de contribuir contenido, interactuar con otras personas de todo el mundo, instalar una “app” o servicio, agregar un servidor o una nueva red, siempre y cuando se satisfagan las normas técnicas de Internet.

La sexta propiedad clave que debemos salvaguardar es el **espíritu de colaboración** de Internet. Al abordar los temas de seguridad en Internet, tenemos que encontrar una manera de involucrar a todas las partes interesadas, desde los usuarios hasta la comunidad de investigadores, las empresas privadas, los formuladores de políticas y más. Las soluciones desarrolladas de manera aislada o bien no resuelven el problema o bien el daño que provocan es mayor que los beneficios que aportan. En algunos casos, incluso pueden llegar a crear importantes problemas que socavan la estabilidad de Internet.

La complejidad del panorama de la seguridad

> *Satisfacer los objetivos de seguridad y a la vez preservar las propiedades clave de Internet es un delicado equilibrio y constituye el verdadero desafío para una estrategia de ciberseguridad. Es fundamental que las soluciones sean compatibles con las invariantes de Internet*

Satisfacer los requisitos de seguridad en un sistema cerrado que opera en un entorno limitado es relativamente fácil y, en muchos casos, una simple estrategia de “seguridad por oscuridad” puede resultar satisfactoria. Asegurar un sistema abierto como Internet presenta diferentes desafíos.

En primer lugar, las mismas propiedades en las cuales se fundamentan el éxito de Internet y su valor para los usuarios generan nuevas oportunidades para diversos tipos de actividades maliciosas. Por ejemplo:

- Internet es accesible.
    - Pero esto significa que también es accesible para los ataques y las intrusiones.
- Internet está floreciendo gracias a la posibilidad de innovar sin necesidad de pedir permiso.
    - Pero esto también permite el desarrollo y despliegue de diversos tipos de *malware*.
- Valoramos el alcance global de Internet.
    - Pero, en términos de ciberseguridad, significa que posiblemente sea más fácil cometer un ciberdelito y que los efectos de un ataque tengan mayor alcance.
- Los estándares de Internet son de carácter voluntario, al igual que su adopción. Son el resultado de la colaboración – la colaboración que es una parte integral del funcionamiento de Internet.
- Pero al mismo tiempo se hace más difícil asignar las responsabilidades y prescribir soluciones.

Al abordar los diferentes aspectos de la ciberseguridad, es importante tener en cuenta que, aunque hay quienes maliciosamente explotarán cualquier oportunidad, las invariantes de Internet no son ni el origen ni la causa de las actividades maliciosas. Satisfacer los objetivos de seguridad y a la vez preservar estas propiedades representa un delicado equilibrio y el verdadero desafío para una estrategia de ciberseguridad. Esto significa que el diseño y la implementación de soluciones de seguridad deben considerar

su potencial efecto sobre las propiedades fundamentales de Internet. Como se señaló anteriormente, para asegurar el éxito continuado de Internet como motor de prosperidad económica y social, es importante que las soluciones de seguridad se basen en las invariantes de Internet, o que al menos sean coherentes con las mismas.

En la capa técnica, la comunidad técnica de Internet tiene un largo historial en cuanto al desarrollo de este tipo de soluciones (que incluyen protocolos y tecnologías, así como mejores prácticas operativas) y su puesta a disposición del mundo para ayudar a construir una Internet más segura y confiable. Estas soluciones se desarrollan en diferentes organizaciones y foros de normalización de manera abierta, en colaborativa y por consenso.

Algunos elementos tecnológicos básicos para la seguridad

Entre los ejemplos de estándares técnicos desarrollados por la IETF (Internet Engineering Task Force) con el objetivo de mejorar la seguridad de la infraestructura de Internet se pueden mencionar los siguientes:

- IPsec (seguridad del Protocolo de Internet) – proporciona seguridad de extremo a extremo en la capa de Internet
- TLS (seguridad de la capa de transporte) – proporciona seguridad a las comunicaciones a través de Internet y es muy utilizada, por ejemplo, para asegurar las comunicaciones web
- Protocolo de autenticación de redes Kerberos – ofrece una manera de verificar la identidad de las entidades en una red abierta (sin protección)
- DNSSEC (conjunto de extensiones de seguridad para el Sistema de Nombres de Dominio) – para asegurar la integridad y la autenticidad de las respuestas DNS
- DANE (autenticación basada en DNS de entidades nombradas) – aprovecha el DNSSEC para permitir que los administradores de los nombres de dominio especifiquen las claves que se utilizan en los servidores TLS de dicho dominio

Algunos ejemplos de los estándares técnicos que están en desarrollo y bajo consideración en W3C (World Wide Web Consortium) para mejorar la seguridad de la web y de Internet incluyen:

- Política de seguridad del contenido
- Acceso a recursos desde múltiples orígenes
- Firma XML, encriptación de XML y especificaciones relacionadas
- APIs criptográficas para JavaScript

Los ejemplos de estándares de seguridad de los datos de OASIS incluyen:

- DSS (Servicios de firma digital) – estándares para los servicios de firma digital para XML
- KMIP (Protocolo de interoperabilidad de administración de claves) – proporciona funcionalidad extendida a las tecnologías de clave encriptada asimétricas
- SAML (Security Assertion Markup Language) – marco basado en XML para la creación y el intercambio de información de seguridad entre asociados en línea
- XACML (eXtensible Access Control Markup Language) – representación y evaluación de las políticas de control de acceso

En segundo lugar, la seguridad absoluta no existe. Siempre habrá amenazas, por lo que "seguro" simplemente significa que los riesgos residuales son aceptables en un contexto específico. Es por ello que la "resiliencia" es una métrica importante a la hora de definir el objetivo de los esfuerzos de ciberseguridad. Al igual que un cuerpo humano que puede sufrir a causa de los virus pero que gracias a ellos se vuelve más fuerte y resistente, las nuevas tecnologías, soluciones y esfuerzos colaborativos hacen que Internet sea más resiliente ante las actividades maliciosas.

Cultura de responsabilidad compartida y colectiva frente al riesgo

> *El alto grado de interconexión e interdependencia del ecosistema de Internet traen aparejado un nuevo e importante requisito para lograr una seguridad eficaz: la gestión colaborativa de los riesgos "hacia adentro" y "hacia fuera".*

Los enfoques de seguridad tradicionales se ocupaban principalmente de las amenazas externas e internas y del impacto que éstas podían tener sobre nuestros propios activos. Sin embargo, cada vez más se reconoce que un paradigma de seguridad para el ecosistema de Internet debe tener como premisa la protección de las oportunidades de prosperidad económica y social, y no ser un modelo simplemente basado en la prevención del daño percibido. Por otra parte, la seguridad se debe abordar desde la perspectiva de la gestión del riesgo.

Con su alto grado de interconexión y dependencias, Internet aporta una nueva dimensión al riesgo. La seguridad y la resiliencia de Internet no solo dependen de lo bien que se gestionen los riesgos para la organización y sus activos, sino, sobre todo, del reconocimiento y la gestión de los riesgos que la propia organización (por su acción o inacción) introduce al ecosistema de Internet – los riesgos "hacia fuera". Por ejemplo: la existencia y el deficiente mantenimiento de los llamados "resolvedores de DNS abiertos" que habitualmente se utilizan para ataques DDoS basados en reflexión ; políticas y prácticas de seguridad deficientes que permiten que las computadoras comprometidas se unan a botnets existentes; una Autoridad de Certificación (CA) PKI con protección insuficiente y una capacidad inadecuada para la detección de violaciones compromete la seguridad y produce una demora en el anuncio de un incidente .

Este aspecto de la gestión del riesgo no es necesariamente evidente, sobre todo porque muchas veces no hay un daño inmediato y fácilmente identificable que afecte a la organización o a sus activos y, por lo tanto, no hay ningún caso de negocio que se pueda asociar directamente con la reducción de los riesgos "hacia fuera". A la vez, no considerarlos disminuye la seguridad global del ecosistema.

Por otra parte, algunos riesgos deben ser gestionados por más de un actor. Este es el concepto de gestión compartida del riesgo. Esto es particularmente importante en lo que concierne a la seguridad de la infraestructura global de Internet. Por ejemplo, mitigar el riesgo de los ataques DDoS basados en reflexión requiere una amplia adopción de prácticas de filtrado al ingreso para evitar el spoofing de direcciones IP . Otro ejemplo en que la responsabilidad colectiva desempeña un papel fundamental es la seguridad y

la resiliencia del sistema de enrutamiento global. Dado que las redes están interconectadas y son interdependientes, es poco lo que puede hacer una red, incluso a la hora de proteger los recursos propios. Volviendo a los ataques DDoS basados en reflexión, si las demás redes conectadas no despliegan filtrado al ingreso, un recurso (por ejemplo, un servidor web) puede ser atacado incluso si la red que lo aloja utiliza filtrado al ingreso. Sin embargo, el beneficio para Internet en general es que esta red no se podría utilizar como una plataforma para el lanzamiento de este tipo de ataques.

La cultura de responsabilidad compartida y colectiva está en consonancia con la naturaleza "por el interés público" de Internet. En el contexto de la ciberseguridad, esto significa que la implementación de soluciones de seguridad en el ecosistema de Internet es una inversión a largo plazo de la cual todos se benefician y que todas las partes interesadas tienen un interés común en la gestión de estos recursos.

La colaboración como un componente esencial de la seguridad efectiva

> *En definitiva, la gente es lo que mantiene la unidad de Internet. El desarrollo de Internet se ha basado en la cooperación y la colaboración voluntaria y creemos que este continúa siendo uno de los factores fundamentales para su prosperidad y potencial.*

Por lo general, resulta difícil identificar incentivos en el área de la seguridad. La seguridad de la infraestructura global de Internet, ya sea del DNS o del enrutamiento, implica nuevos desafíos: la utilidad de las medidas de seguridad depende en gran medida de las acciones de muchos otros actores.

Además, si quienes participan en el ecosistema de Internet actúan de forma independiente y motivados exclusivamente por sus propios intereses personales, esto no solo repercutirá en la seguridad del ecosistema sino que también disminuirá el potencial social y económico que ofrece Internet. Esta situación suele describirse como la "tragedia de los comunes", un término acuñado por Garrett Hardin en su trabajo del mismo nombre. La analogía de los recursos comunes se puede aplicar al ecosistema de Internet, donde destaca fuertemente algunos de sus desafíos, especialmente en el área de la ciberseguridad.

No es fácil superar la "tragedia de los comunes" en el ámbito de la seguridad y resiliencia de Internet, ya que la búsqueda de resultados que avancen nuestros intereses individuales forma parte de la naturaleza humana. Sin embargo, este enfoque es contraproducente y a la larga resulta perjudicial para los intereses de todos.

Las soluciones tecnológicas son un elemento esencial en este caso, aunque la tecnología por sí sola no es suficiente. Para lograr mejoras visibles en este ámbito, primero debe haber una mejor articulación del espacio del problema en términos de los riesgos, basado en métricas y tendencias, además de un cambio cultural que promueva la responsabilidad colectiva en todos los ámbitos: político, legal, técnico, económico, social, etc.

El desarrollo de Internet siempre se ha basado en la cooperación y la colaboración voluntaria y la historia de Internet muestra muchos ejemplos de esta cooperación y su eficacia. Un excelente ejemplo es el Grupo de Trabajo sobre Conficker , creado para luchar contra el ataque realizado vía Internet por el software malicioso conocido como Conficker. Otros ejemplos son la multitud de grupos de operadores de redes regionales y nacionales (NOGs) y su papel en la resolución de problemas operativos (que suelen abarcar múltiples redes).

Los temas, desafíos asociados y oportunidades de colaboración y el cambio cultural necesario se pueden agrupar en cuatro áreas principales. En nuestra opinión, avanzar en cada una de las siguientes áreas es un requisito previo para lograr un impacto positivo:

1. **Un entendimiento común del problema.** Cuanto más alineados estén los actores con respecto a cuáles son los problemas, su gravedad y la prioridad de su resolución, más enfocado será el diálogo y más coherentes serán los diversos esfuerzos destinados a mejorar la seguridad y la resiliencia.
2. **Un entendimiento común de las soluciones.** Aquí el desafío radica en que hay toda una gama de posibles soluciones (técnicas, políticas, económicas, sociales) y cada una de ellas resuelve apenas una parte del problema, o un conjunto de problemas en un momento determinado. Es importante comprender que no existe ninguna solución milagrosa, sino que para construir una solución de seguridad se pueden utilizar diferentes bloques en permanente evolución.
3. **Comprender los costos y beneficios comunes e individuales.** Los bloques de construcción tecnológicos varían en cuanto a los costos y beneficios que aportan para un participante de manera individual y para el bien común de la infraestructura global. Comprender estos factores y cómo se alinean con los objetivos de negocio de los operadores de red es fundamental para lograr mejoras sostenidas en términos de seguridad y resiliencia.
4. **Capacidad de evaluar los riesgos.** La correcta selección de las herramientas y los enfoques a utilizar depende de la capacidad de evaluar correctamente los riesgos, tanto “hacia adentro” como “hacia fuera”, tal como mencionamos anteriormente. Esto requiere ponerse de acuerdo sobre las métricas y los datos objetivos y tendencias asociados con los mismos. Estos datos también son importantes para medir los efectos de este tipo de herramientas una vez que se implementan y para monitorear la dinámica cambiante del entorno.

No es realista suponer que se llegará a un acuerdo universal sobre las cuestiones de fondo, ni que a nivel mundial se adoptará un plan de acción coherente en el futuro previsible. La competencia comercial, la política y la motivación personal son también factores que afectan el éxito de la colaboración. Sin embargo, tal como lo han demostrado diferentes esfuerzos de colaboración, las diferencias pueden ser superadas para cooperar y trabajar colaborativamente contra una amenaza. Esta colaboración voluntaria “en beneficio de todos” es notable por su escalabilidad y su capacidad de adaptarse a condiciones y amenazas cambiantes, y permite lograr una eficacia sin precedentes.

End Notes

[1] "Internet Invariants: What Really Matters", http://www.internetsociety.org/internet-invariants-what-really-matters

[2] http://news.cnet.com/8301-1023_3-57525797-93/facebook-hits-1-billion-active-user-milestone/

[3] Ushahidi es un proyecto de código abierto que permite que los usuarios, de forma colaborativa, aporten información sobre una crisis para su envío a través de la telefonía móvil, www.ushahidi.com

[4] https://en.wikipedia.org/wiki/Security_by_obscurity

[5] Por ejemplo, la técnica utilizada en el ataque contra www.spamhaus.org en marzo 2013.

[6] Por ejemplo, el compromiso de Diginotar, una Autoridad de Certificación Holandesa; informe completo: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

[7] Por más información, ver RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing* (http://tools.ietf.org/html/rfc2827)

[8] Hardin, G. "The Tragedy of the Commons". Science 162 (3859): 1243–1248, 1968.

[9] Conficker Working group, http://www.confickerworkinggroup.org/wiki/

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org

Internet Society™